Algorithmic Information Theoretic Issues in Quantum Mechanics

Gavriel Segre - PHD thesis

October 20, 2001

Contents

Part I

Preliminaries

0.1 Warning

The project of this work, going beyond the possibility of realization (at least mine) during doctoral studies, has not been completed and has to be considered as **open**.

To underline the intellectual path I tried to pursue, I have conserved the title and mentioning to the unrealized sections instead of eliminating them, thinking that they add anyway some cbit of classical information.

0.2 Acknowledgments

First of all I would like to thank my PHD-tutor, prof. Rimini, for having believed I was worth to be allowed to follow my own way and for many encouragements and skills.

Then I would like to thank doct. Benatti for having read, analyzed and often constructively criticized many parts of this work, and for having taught me so many things that it is difficult to me to mention all of them.

In particular I am grateful to him for clarifying me the key point why some diagonalization-proofs don't generalize noncommutatively.

I then want strongly to thank prof. Jona-Lasinio for many invaluable remarks and teachings and, in particular, for having suggested me the idea of considering sequences of free coin tosses in view of Voiculescu's Central Limit Theorem.

Then I want to thank prof. Rasetti who introduced me to Word Problems, as well as to the Turing Barrier Problem of Quantum Mechanics and all the related issues.

I am very grateful to prof. Van Lambalgen for having given me a copy of his wonderful dissertation.

Then I would like to thank doct. Winter for having suggested me to partecipate to the Second Bielefeld Workshop on Quantum Information and Computation, giving me the motivations to pursue walking on my way.

Last but not least, I would like to thank prof. Odifreddi for many useful suggestions.

0.3 Notation

$\forall$	for all (universal quantificator)
$\exists$	exist (existential quantificator)
$\exists\,!$	exist and is unique
$x \;=\; y$	x is equal to y
$x \;:=\; y$	x is defined as y
2^S	power-set of the set S
S^0	interior of the topological space S
$\bar{S}$	closure of the topological space S
$\mathcal{D}(A_1\,,\,A_2)$	description methods of A_2 through A_1
$\mathcal{R}$	universe of description
Σ	binary alphabet $\{0,1\}$
Σ_n	n-letters' alphabet
$\Sigma^\star$	strings on the alphabet Σ
Σ^∞	sequences on the alphabet Σ
$\vec{x}$	string
λ	empty string
$\|\vec{x}\|$	length of the string $\vec{x}$
$string(n)$	n^{th} string in quasilexicographic order
$\|n\|$	length of the n^{th} string in quasilexicographic order
$\bar{x}$	sequence
$<_p$	prefix order relation
$\cdot$	concatenation operator
x_n	n^{th} digit of the string $\vec{x}$ or of the sequence $\bar{x}$
$\vec{x}(n)$	prefix of length n of the string $\vec{x}$ or of the sequence $\bar{x}$
$\vec{x}(n,m)$	substring of the sequence $\bar{x}$ obtained taking the digits from the n^{th} to the m^{th}
$\vec{x}^n$	string made of n repetitions of the string $\vec{x}$
$\vec{x}^\infty$	sequence made of infinite repetitions of the string $\vec{x}$
$S\,\Sigma^\infty$	sequences having the strings of S as prefixes
$\vec{x}\Sigma^\infty$	sequences having the string $\vec{x}$ as prefix
$N_i(\vec{y})$	number of occurence of the letter i in the string $\vec{y}$
$N_i^n(\bar{x})$	number of successive letters i ending in position n of the sequence $\bar{x}$
$\mathcal{I}(a,n,\vec{b})$	string obtained inserting the letter a at the n^{th} place of the string $\vec{b}$
$L_{D,P}$	average code-word length w.r.t. the code D and the distribution P
$H(P)$	Shannon's entropy of the distribution P
$K(\vec{x})$	simple algorithmic entropy of the string $\vec{x}$
$I(\vec{x})$	prefix algorithmic entropy of the string $\vec{x}$
$\Sigma(n)$	busy-beaver function
$P_U(\vec{x})$	universal probability of the string $\vec{x}$ w.r.t. the universal Chaitin computer U
Ω_U	halting probability of the universal Chaitin computer U

$CHAITIN-m-RANDOM(\Sigma^\star)$	Chaitin-m-random strings
$CHAITIN-RANDOM(\Sigma^\star)$	Chaitin-random strings
$\mathcal{N}(\bar{x})$	numeric representation of the sequence $\bar{x}$
$CHAITIN-RANDOM(\Sigma^\infty)$	Martin Löf- Solovay -Chaitin-random sequences
$BRUDNO-RANDOM(\Sigma^\infty)$	Brudno-random sequences
$q-PSEUDORANDOM(\Sigma^\star, V)$	pseudorandom strings of level q w.r.t. V
$MARTINL\ddot{O}F-q-RANDOM(\Sigma^\star)$	Martin Löf pseudorandom strings of level q
$\mu-RANDOM(\Sigma^\infty, \delta)$	Martin Löf μ-random sequences w.r.t. δ
$\mu-RANDOM(\Sigma^\infty)$	Martin Löf μ-random sequences
$\mathcal{P}(M)$	unary predicates over the set M
$\mathcal{P}_{TYPICAL}(CPS)$	typical properties of CPS
$\mathcal{L}_{RANDOMNESS}(CPS)$	laws of randomness of CPS
$P-CONF-RANDOM(\Sigma^\infty)$	conformistically-random sequences w.r.t. P
$CONF-RANDOM(\Sigma^\infty)$	conformistically-random sequences
$EXT[S]$	subsequence extraction function w.r.t. S
$CHURCH-RANDOM(\Sigma^\infty)$	Church-random sequences
$A \bigvee B$	coarsest refinement of the partitions A and B
h_{CDS}	Kolmogorov-Sinai entropy of CDS
$\mathbb{N}$	natural numbers
$\mathbb{Z}$	integers numbers
$\mathbb{A}_n$	algebraic numbers of order n
$\mathbb{A}$	algebraic numbers
$\mathbb{Q}$	rational numbers
$\mathbb{R}$	real numbers
$\mathbb{C}$	complex numbers
$\mathbb{C}P^n$	complex projective space of order n
$G_{k,n}(\mathbb{C})$	complex Grassmann manifold of order (k,n)
$\aleph_n$	$(n+1)^{th}$ infinite cardinal
$\Re(z)$	real part of the complex number z
$\Im(z)$	imaginary part of the complex number z
$f_1 \overset{+}{\leq} f_2$	f_1 is additively less or equal to f_2
$f_1 \overset{+}{=} f_2$	f_1 is additively equal to f_2
$f_1 \overset{\times}{\leq} f_2$	f_1 is multiplicatively less or equal to f_2
$f_1 \overset{\times}{=} f_2$	f_1 is multiplicatively equal to f_2
$a \mid b$	a divides b
$a \nmid b$	a does not divide b
gcd(a,b)	greatest common divisor of (a,b)
lcm(a,b)	least common multiple of (a,b)
$\lfloor x \rfloor$	floor of x: the greater integer less than or equal to x
$\lceil x \rceil$	ceiling of x: the least integer greater than or equal to x
$x \, mod \, n$	remainder: $x - n\lfloor \frac{x}{n} \rfloor$
$MAP(A,B)$	maps from A to B
$f : A \mapsto B$	map from A to B
$\overset{\circ}{MAP}(A,B)$	partial maps from A to B

$f : A \overset{\circ}{\mapsto} B$	partial map from A to B
C_M (NC_M)	mathematically-classical (mathematically-nonclassical)
C_Φ (NC_Φ)	physically-classical (physically-nonclassical)
REC	recursive
Δ_0^0	computable
$\varphi_e^{(n)}$	n-ary partial recursive function with Gödel number e
$\mathcal{W}_e^{(n)}$	halting set of $\varphi_e^{(n)}$
$\mathcal{L}(\mathcal{H})$	lattice of all the closed linear subspaces of the Hilbert space $\mathcal{H}$
$\mathcal{O}(\mathcal{H})$	linear operators on the Hilbert space $\mathcal{H}$
$\mathcal{B}(\mathcal{H})$	bounded linear operators on the Hilbert space $\mathcal{H}$
$\parallel \cdot \parallel_n$	n^{th} operatorial norm on $\mathcal{B}(\mathcal{H})$
$\|a\|$	modulus of the bounded operator a
$\mathcal{C}_n(\mathcal{H})$	n-class bounded operators on the Hilbert space $\mathcal{H}$
$\mathcal{C}_1(\mathcal{H})$	trace-class bounded operators on the Hilbert space $\mathcal{H}$
$\mathcal{C}_2(\mathcal{H})$	Hilbert-Schmidt bounded operators on the Hilbert space $\mathcal{H}$
$\mathcal{C}(\mathcal{H})$	noncommutative infinitesimals on the Hilbert space $\mathcal{H}$
$\mathcal{I}_\alpha(\mathcal{H})$	noncommutative infinitesimals of order α on the Hilbert space $\mathcal{H}$
$\mathcal{D}(M)$	classical probability distributions over M
$\mathcal{D}(\mathcal{H})$	density operators over the Hilbert space $\mathcal{H}$
$D_T(\vec{p}^{(A)}, \vec{p}^{(B)})$	classical trace distance among $\vec{p}^{(A)}$ and $\vec{p}^{(B)}$
$D_T(\rho^{(A)}, \rho^{(B)})$	quantum trace distance among $\rho^{(A)}$ and $\rho^{(B)}$
$F(\vec{p}^{(A)}, \vec{p}^{(B)})$	classical fidelity among $\vec{p}^{(A)}$ and $\vec{p}^{(B)}$
$F(\rho^{(A)}, \rho^{(B)})$	quantum fidelity among $\rho^{(A)}$ and $\rho^{(B)}$
$D_A(\vec{p}^{(A)}, \vec{p}^{(B)})$	classical angle distance among $\vec{p}^{(A)}$ and $\vec{p}^{(B)}$
$D_A(\rho^{(A)}, \rho^{(B)})$	quantum angle distance among $\rho^{(A)}$ and $\rho^{(B)}$
A_+	positive part of the $\star$-algebra A
$A_{p.s.d}$	part with discrete spectrum of the $C^\star$-algebra A
A_{sa}	self-adjoint part of the $\star$-algebra A
$PUR(\rho\, , \mathcal{H})$	purifications of the density operator ρ w.r.t. the Hilbert space $\mathcal{H}$
$\mathcal{U}(A)$	unitary group of the $\star$-algebra A
$\mathcal{P}(A)$	projections of the $\star$-algebra A
$QL(A)$	quantum logic of the $W^\star$-algebra A
$S(A)$	states on the $W^\star$-algebra A
$S(A)_n$	normal states on the $W^\star$-algebra A
ρ_ω	density operator of the normal state ω
ω_μ	state of the classical probability measure μ
$\Xi(A)$	pure states on the $W^\star$-algebra A
$POINTS(A)$	points on the $W^\star$-algebra A
$Sp(a)$	spectrum of a
$S_\tau(A)$	τ - invariant states on the $W^\star$-algebra A
$\Xi_\tau(A)$	τ - invariant pure states on the $W^\star$-algebra A
$\Delta_\omega(a)$	dispersion of the state ω on the element a of the $W^\star$-algebra A
$(\mathcal{H}_\omega\, , \pi_\omega\, , \|\Omega_\omega >)$	GNS-representation of the $C^\star$-algebra A w.r.t. the state ω
$AUT(A)$	automorphisms of the $W^\star$-algebra A
$INN(A)$	inner automorphisms of the $W^\star$-algebra A
$OUT(A)$	outer automorphisms of the $W^\star$-algebra A

$GR-AUT(G\,,\,A)$	automorphisms' groups of A representing G
$GR-INN(G\,,\,A)$	inner automorphisms' groups of A representing G
$GR-OUT(G\,,\,A)$	outer automorphisms' groups of A representing G
$CPU(A,B)$	channels from the $W^{\star}$-algebra A to the $W^{\star}$-algebra B
$CPU(A)$	channels on the $W^{\star}$-algebra A
$\alpha_{\star}$	dual of the channel α
$OPU(A)$	operational partition of unity over the $W^{\star}$-algebra A
$\{\alpha_i(\mathcal{V})\}$	channels' set of the operational partition of unity $\mathcal{V}$
$R(\mathcal{V})$	reduction channel of the operational partition of unity $\mathcal{V}$
A'	commutant of the Von Neumann algebra A
$\mathcal{Z}(A)$	centre of the Von Neumann algebra A
R	hyperfinite II_1-type factor
R_{λ}	hyperfinite III_{λ}-type factor $(0\,<\,\lambda\,<\,1)$
$cardinality_{NC}(A)$	noncommutative cardinality of the noncommutative set A
Σ_{NC}	noncommutative binary alphabet
$\Sigma_{NC}^{\star}$	noncommutative space of qubits' strings
Σ_{NC}^{∞}	noncommutative space of qubits' sequences
$M_n(a)$	n^{th} moment of the algebraic random variable a
$E(a)$	expectation value of the algebraic random variable a
$Var(a)$	variance of the algebraic random variable a
Z_a	characteristic function of the algebraic random variable a
μ_a	classical probability measure of the self-adjoint algebraic random variable a
v_a	result of the measurement of the self-adjoint algebraic random variable a
$ZQ_a(t)$	characteristic function of the noncommutative random variable a
$ZC_{Ap}(t)$	characteristic function of the classical approximation Ap
$END(\,A\,,\,\omega\,)$	endomorphisms of the algebraic probability space $(\,A\,,\,\omega\,)$
$AUT(\,A\,,\,\omega\,)$	automorphism of the algebraic probability space $(\,A\,,\,\omega\,)$
tr_{ω}	Dixmier trace
$O(n)$	n^{th} orthogonal group
$Spin(n)$	n^{th} spin group
∇	Levi-Civita connection of the (pseudo)riemannian manifold $(M\,,\,g)$
$\triangle_g$	Laplace-Beltrami operator on the (pseudo)riemannian manifold $(M\,,\,g)$
$d\mu(g)$	metric measure of the (pseudo)riemannian manifold $(M\,,\,g)$
$Is[(M\,,\,g)]$	isometries' group of the (pseudo)riemannian manifold $(M\,,\,g)$
$\Gamma(M,E)$	sections of the fibre bundle $E\,\stackrel{\pi}{\to}\,M$
$O(M)\,\stackrel{\pi}{\to}\,M$	orthonormal frame bundle of the riemannian manifold $(M\,,\,g)$
$S(M)\,\stackrel{\pi}{\to}\,M$	spin bundle on the spin manifold $(M\,,\,g)$
$C(M)\,\stackrel{\pi}{\to}\,M$	Clifford bundle on the spin manifold $(M\,,\,g)$
$\int_{NC}$	noncommutative integral on the spectral triple $(A\,,\,\mathcal{H}\,,\,D)$
d_{NC}	noncommutative differential on the spectral triple $(A\,,\,\mathcal{H}\,,\,D)$
$J[p(z)]$	Julia set of the polynomial p(z) on the complex field
$d\Lambda_D$	Hausdorff measure on a set with Hausdorff dimension D
$\mathcal{M}$	Mandelbrot's set
$d(\omega_1,\omega_2)$	noncommutative geodesic distance between two states
$(\,D\omega_1\,:\,D\omega_1\,)_t$	noncommutative Radon-Nikodym derivative between two states
σ_t^{ω}	modular group of the state ω
$<\chi\,\vert\,\mathcal{R}>$	presentation with generating system χ and defining relators $\mathcal{R}$

F_n	free group of rank n
$l^2(G)$	Hilbert space of the discrete group G
$\mathcal{L}(G)$	left group Von Neumann algebra of the discrete group G
$\mathcal{R}(G)$	right group Von Neumann algebra of the discrete group G
C_n	n^{th} Catalan number
$CSM(M,N)$	classical statistical model w.r.t M and N
$g_{CSM(M,N)}$	Fisher-Rao riemannian metric w.r.t. CSM (M , N)
$\hat{\Pi}_{random}$	Coleman-Lesniewski's operator
$I_Q(\|\psi>)$	Svozil's quantum algorithmic information of $\|\psi>$ w.r.t. Q
$\mathcal{P}_C(A)$	commutative predicates over the $W^{\star}$-algebra A
$\mathcal{P}_{NC}(A)$	noncommutative predicates over the $W^{\star}$-algebra A
$\mathcal{P}_C^{TYPICAL}(APS)$	typical commutative properties of APS
$\mathcal{P}_{NC}^{TYPICAL}(APS)$	typical noncommutative properties of APS
$KOLMOGOROV_C(APS)$	Kolmogorov commutatively-random elements of APS
$KOLMOGOROV_{NC}(APS)$	Kolmogorov noncommutatively-random elements of APS
$\mathcal{L}_{RANDOMNESS}^C(APS)$	commutative laws of randomness of APS
$\mathcal{L}_{RANDOMNESS}^C(APS)$	noncommutative laws of randomness of APS
$RANDOM(\Sigma_{NC}^{\infty})$	random sequences of qubits
$[G\, ,\, G]$	commutator subgroup of the group G
$G_1 \star G_2$	free product of the groups G_1 and G_2
$A_1 \star A_2$	free product of the algebraic spaces A_1 and A_2
$(A_1,\omega_1) \star (A_2,\omega_2)$	free product of (A_1,ω_1) and (A_2,ω_2)
ENSEMBLE[CPS , n]	ensemble of random matrices of order n w.r.t. CPS
$\mu_{emp}(a)$	empirical eigenvalue distribution of the random matrix a
$\mu_{mean}(a)$	mean eigenvalue distribution of the random matrix a
$S_{Araki}(\omega_1\, ,\, \omega_2)$	Araki's relative entropy of ω_1 w.r.t. ω_2
$S(\omega)$	entropy of the state ω
$H_{\omega}(A)$	entropy of the sub-$W^{\star}$-algebra A w.r.t. the state ω
$H_{\omega}(\alpha)$	entropy of the the channel α w.r.t. the state ω
$I(\omega\, ;\, \alpha)$	mutual entropy of the state ω and the channel α
$DEC(\omega)$	decompositions of the state ω
$DEC_{EXT}(\omega)$	extremal decompositions of the state ω
$DEC_{\perp}(\omega)$	orthogonal decompositions of the state ω
$DEC_{Schatten}(\omega)$	Schatten's decompositions of the normal state ω
$I_{acc}(\mathcal{E})$	classical accessible information information of the decomposition $\mathcal{E}$
$I_{Holevo}(\mathcal{E})$	Holevo's information of the decomposition $\mathcal{E}$
n-GOE	gaussian orthogonal ensemble of order n
n-GUE	gaussian unitary ensemble of order n
$gauss(D,\vec{m},\hat{C};\vec{x})$	D-dimensional gaussian measure of mean $\vec{m}$ and covariance $\hat{C}$
$gauss_{STANDARD}$	standard gaussian measure
$sc(m,r;x)$	semi-circle measure of mean m and variance $\frac{r^2}{4}$
$sc_{STANDARD}$	standard semi-circle measure

$S_{Bennett}(P)$	Bennett's entropy of the distribution P
$S_{Zurek}(\rho)$	Zurek's entropy of the density matrix ρ
$S_{therm}(\omega)$	thermodynamical entropy of the state ω
$S_{\text{double approach}}(\omega)$	double approach entropy of the state ω
$I_{skew}(\rho, a)$	skew information of the density matrix ρ w.r.t. the operator a
REC_O	recursivity in the oracle O
$f \ \leq_T \ g$	f is Turing reducible to g
$f \ \sim_T \ g$	f is Turing equivalent to g
$(\mathcal{D}_T \, , \leq_T)$	Turing degrees
$I^-(S)$	chronological past of the space-time's region's S
$I^+(S)$	chronological future of the space-time's region's S
$J^-(S)$	causal past of the space-time's region's S
$J^+(S)$	causal future of the space-time's region's S
$D^-(S)$	past domain of dependence of the space-time's region's S
$D^+(S)$	future domain of dependence of the space-time's region's S
$D(S)$	domain of dependence of the space-time's region's S
$\approx_{Dirac}$	weak equality
$[a \, , \, b]_{EFF}$	effective commutator of a and b
$I_{skew}^{(EFF)}(\rho \, , \, a)$	effective skew-information of ρ w.r.t. a
$r - \lim_{n \rightarrow \infty}$	recursive limit for $n \ \rightarrow \ \infty$
$REC_{Nielsen}(A)$	Nielsen-computable part of the $W^{\star}$-algebra A
$COMP - ST(B)$	computability structures on the Banach space B
$REC_{Pour \ El}(B, \mathcal{S})$	Pour-El computable vectors of B w.r.t. $\mathcal{S}$
$REC_{Pour \ El} - \mathcal{O}(\mathcal{H})$	effectively determined linear operators on $\mathcal{H}$ w.r.t. $\mathcal{S}$
$Bloch(\vec{r})$	one qubit density operator w.r.t. the Bloch-sphere's vector $\vec{r}$
L(G)	language generated by the Chomsky's grammar G
FIN	finite languages
REG	regular languages
LIN	linear languages
CF	context-free languages
CS	context-sensitive languages
RE	recursively enumerable languages
IGUS	information gathering and using system
PRG	pseudorandom number generator
r.e.	recursively enumerable
w.r.t.	with respect to
l.h.s.	left-hand side
r.h.s.	right-hand side
iff	if and only if
i.e.	id est
e.g.	exempli gratia

0.4 Introduction

The new exciting research field of Quantum Computation has opened a cross-fertilization area among Theoretical Physics and Theoretical Computer Science that, beside the intrinsic technological difficulties in the physical implementation essentially owed to a not-sufficient technological ability in contrasting decoherence, is expected to be a strategic point for developments in both fields [Pre98], [Chu00], [Jup01], [Gru01].

From the other side Quantum Computation Theory, concerning the algorithmic evolution of quantum information, may be seen as a sub-discipline of Quantum Information Theory, a research field that, in spite of its recent exciting developments, is a very older object of investigation in Mathematical Physics [Pet93], [Ohy97].

From a foundational perspective the first natural question is:

What is quantum information?

Such an innocent question is, surprisingly, still open.

The more reasonable way of proceeding to answer this question could consist in following the same footsteps Classical Information Theory undertook to become a well-established mathematical theory [Khi57], [Bil65], [Iha93],[Kak99] of common engeneering application [Tho91].

Though the invention of Information Theory must be tributed with no doubt to Claude E. Shannon's 1948 paper *"The Mathematical Theory of Communication"* [Wea71] the mathematical foundation of the concept of **classical information** was given, among the fifthies and the sixties, by the great mathematician Andrei Nicolaevich Kolmogorov [Shi93], [Soc00].

He observed that there exist three conceptually different ways of approaching the problem of defining the notion of **amount of information**:

1. the **combinatorial approach**
2. the **probabilistic approach**
3. the **algorithmic approach**

The **combinatorial approach** furnishes a definition of the information content of an object that is **contextual**, i.e. depends from the particular context (collection of objects) in which such an object is considered, but is **weight independent**, i.e. it doesn't depend on the specification of a way of weighting the contribution of different elements of such context.

So, given an object x belonging to a set X of N elements (the context) the **combinatorial approach**, invented by R. Hartley in 1928, defines the amount of information of x simply as:

$$I_{combinatorial}(x) := \log_2 N \tag{0.4.1}$$

Let us suppose, for example that x is a n-letter word in an alphabet of s letters containing m_i occurences of the i^{th} letter $(m_1 + \cdots + m_s = n)$.

Since there are:

$$C(m_1, \cdots, m_s) := \frac{n!}{m_1! \cdots m_s!} \tag{0.4.2}$$

words of this kind, one has that:

$$I_{combinatorial}(x) = \log_2 C(m_1, \cdots, m_s) \tag{0.4.3}$$

As $n, m_1, \cdots m_s$ tend to infinity, Stirling's asymptotic formula implies that:

$$I_{combinatorial}(x) \sim \sum_{i=1}^{s} \frac{m_i}{n} \log_2 \frac{m_i}{n} \tag{0.4.4}$$

The **probabilistic approach** furnishes a definition of the information content of an object that is both **contextual** and **weight dependent**.

So given an object x belonging to a set X of N elements (the context) such the the i^{th} element is considered with weight (probability) p_i , the **probabilistic approach**, that invented by Shannon in 1948 and often considered as Classical Information Theory tout court, defines the amount of information of x simply as:

$$I_{probabilistic}(x) := -\sum_{i=1}^{N} p_i \log_2 p_i \tag{0.4.5}$$

It must be noted, at this point, that the asymptotic formula eq.0.4.4 can be obtained, in the probabilistic approach by eq.0.4.5 applying the Law of Large Numbers.

Anyway, at this point, Kolmogorov underlines the importance that such a result can be obtained getting rid of the **weight dependence**, observing that it is precisely what he guaranteed for other two important notions he introduced time before, namely the **ϵ-entropy** $H_\epsilon(K)$ and the **ϵ-capacity** of compact classes of functions describing, respectively, the amount of information necessary for distinguishing some individual function in the class of functions K and the amount of information that can be coded by elements of K under the condition that elements of K no closer than ϵ to each other can be reliably distinguished.

In the same way Kolmogorov stressed the importance of getting-rid of the **context dependence**, i.e. to find an **intrinsic** notion of the amount of information of an object.

This led him to introduce the **algorithmic approach** that is, indeed, both **weight independent** and **context independent**:

in the **algorithmic approach** the amount of information of an object x with respect to a given computer C is defined as the length of the shortest program for C computing (i.e. algorithmically-describing) x:

$$I_{algorithmic}(C;x) \ := \ \begin{cases} \min\{length(p), C(p) = x\} & \text{if x is computable by the computer C,} \\ +\infty & \text{otherwise.} \end{cases} \tag{0.4.6}$$

The independence of this notion from the particular computer C is then established by Kolmogorov through the proof of the so called **Invariance Theorem** certifying the existence of **optimal computers**, i.e. of computers that, up to an object-independent constant, give algorithmic-descriptions always shorter of those given by any other computer.

Kolmogorov, the father of the usual, standard, measure-theoretic axiomatization, stressed from the beginning the conceptual importance of such an **intrinsic** definition of the informational-amount of an object for the same Foundation of Probability Theory, i.e. for the explanation why Probability Theory applies to reality.

The key point is that the **intrinsic nature** of the algorithmic definition of information allows to address the issue of giving an **intrinsic** characterization of randomness:

an algorithmically-random object x is, informally speaking, an **algorithmically-incompressible** object, i.e. an object whose more concise algorithmic-description is its same assignation.

So the grown up theory concerning the algorithmic approach to information, Algorithmic Information Theory from here and beyond, appeared from the beginning as the corner-stone for an alternative Algorithmic Foundation of Classical Probability Theory [Cha87], [Lam87], [Cal94], [Vit97].

Later, especially by the work of Cristian Calude, Gregory Chaitin and the Auckland's Center of Discrete Mathematics and Theoretical Computer Science, Algorithmic Information Theory revealed soon an even more fundamental rule in the Foundations of Mathematics, furnishing an extraordinarily clear information-theoretic explanation of the mathematical phenomenon of Incompleteness [Odi89] (Chaitin's First Undecidability Theorem states that a formal system can't decide statements involving an algorithmic-information's amount higher than its own algorithmic-informational content for more than a fixed constant, implying the recursive undecidability of algorithmic randomness), defining the notion of Halting Probability codifying in optimal way all the undecidabilities of Mathematics (the knowledge of the first n cbits in the binary expansion of Chaitin's Ω number would allow to decide all the n-cbit mathematical statements), stating precise bounds on its determination (Chaitin's Second Undecidability Theorem states that a formal system can't decide more than a finite number of digits in the binary expansion of Ω, such a result having been recentely streghtened by R.M. Solovay through the proof that, by a proper choice of the fixed Chaitin Universal Computer and considering as formal system the Zermelo-Fraenkel axiomatic system endowed with the Axiom of Choice, this finite number of digits reduces even to zero) and, last but not least, showing that Randomness is a pervasive phaenomenon in Pure Mathematics through a paradigmatical example, i.e. shelding new light on Jones and Matjasevic's proof that Hilbert's Tenth Problem (i.e. the problem of finding an algorithm deciding whether an arbitrary Diophantine equation has integer solutions) is undecidable by the proof of the existence of a one integer parameter, let's call it k, exponential diophantine equation such that to decide if it has a finite number of integer solutions is equivalent to decide the k^{th} cbit of the Halting Probability [Ben88] [Cha87], [Cha90], [Cha98], [Cha99], [Cha01], [Sol00].

Furthermore Algorithmic Information Theory appeared soon to play a key rule in the Theory of Chaotic Dynamical Systems:

in 1958 Kolmogorov introduced (only for K-systems, the generalization for arbitrary dynamical systems having being furnished later by Ya. Sinai) a notion that would have played a key rule for the solution of the problem of giving a metric classification of dynamical systems (that is the problem of finding a complete set of invariants that imply a metric isomorphism between dynamical systems): the metric entropy of a dynamical system, characterizing the maximal asymptotic rate of information obtained through a coarse-grained observation of dynamics;

a dynamical system is called chaotic if it has strictly positive metric entropy (or Kolmogorov-Sinai entropy as such notion is more often called).

For the link existing between probabilistic information and probabilistically expected algorithmic information it appeared, then, intuitive that the characterization of chaoticity in terms of the probabilistic approach to information should have a counterpart in terms of the algorithmic approach:

a first formalization of such a link was established by A.A. Brudno [Bru78], [Bru83], [Yak81] by the proof of a theorem (usually called Brudno's Theorem) stating that the Kolmogorov-Sinai entropy of a dynamical system is equal to the asympotic rate of **simple algorithmic information** of almost all its trajectories.

The importance of such a link was later stressed with particular emphasis by Joseph Ford who advocated strongly what he called an Algorithmic Approach to Chaos Theory [For92].

It must be said, anyway, that since the version of classical algorithmic information giving rise to the correct characterization of classical algorithmic randomness is not **simple algorithmic entropy** but **prefix algorithmic entropy**, the Algorithmic Approach to Chaos Theory is equivalent to the usual one only in a weak sense as we will extensively discuss.

The most important reason why Algorithmic Information Theory is of physical relevance lies, anyway, in Thermodynamics.

Many generations of physicists has been educated that the correct exorcism of Maxwell's demon [Max71] was the Leon's Brilloiun one [Bri90]: the **acquisition of information** on the velocity of the molecules by the demon is responsible of the fact that the Second Law of Thermodynamics is not violated.

The recent developments of the Thermodynamics of Computation [Fey96], [Ben90b], has shown, anyway, that Brillouin's exorcism doesn't work: by Landauer's Principle [Lan90] such an information's acquisition process may be realized in a thermodynamically reversible way.

The correct exorcism was, instead proposed by Charles Bennett [Ben90a]: it is the **erasure of information** by the demon that cannot e accomplished in a thermodynamically reversible way and is responsible of the preservation of the Second Law.

This has, anyway, dramatic conseguence concerning the same Foundations of Statistical Mechanics:

introducing the issue concerning the compatibility between the time-reversibility of motions'-equation and the phenomenological time-irreversibility of thermodynamics with Ludwig Boltzmann's own words:

> *"If therefore we conceive of the world as an enormously large mechanical system composed of an enormously large number of atoms, which starts from a completelly ordered initial state, and even at present is still in a substantially ordered state, then we obtain consequences which actually agree with the observed facts; although this conception involves, from a purely theoretical - I might say philosophical - standpoint, certain new aspects with contradicts general thermodynamics based on a purely phenomenological viewpoint. General thermodynamics proceeds from the fact that, as far as we can tell from our experience up to now, all natural processes are irreversible. Hence according to the principles of phenomenology, the general thermodynamics of the second law is formulated in such a way that the unconditional irreversibility of all natural process is asserted as a so-called axiom, just as general physics based on a purely phenomenological standpoint asserts the unconditional divisibility of matter without limits as an axiom". From the section 89 of [Bol95]*

let us observe that most of the answers it has received, such as the one authoritatively supported by Giovanni Gallavotti seeing in Lanford's Theorem a mathematical formalization and confirmation of Boltzmann's point of view that no inconsistency exists owing to the not observability of the time-scale on which reversibility manifests [Gal99], agree in a thing: the link between the thermodynamical entropy and the state of a dynamical system is given by the **probabilistic information** of that state.

As it has been strongly supported by Wojciech Zurek [Zur89], [Zur90b], [Zur90a], [Zur99] Bennett's exorcism ultimatively implies that in presence of a particular kind of information gathering and using systems (IGUS), also the **algorithmic information** of the state contribute to the thermodynamical entropy and has, conseguentially, to be taken into account.

As far as Quantum Information Theory is concerned, the whole Kolmogorovian analysis concerning the three possible approaches to Information Theory may be rephrased with no variation.

Anyway, nowadays, while the probabilistic approach has received a massive attention, resulting in a theory developed almost as much as the classical Shannon's theory, the situation is radically different for the combinatorial as well as for the algorithmic approach where all is available is not so much more than a plethora of attempts.

The algorithmic approach to Quantum Information Theory, for its context-independence as well as for its weight-independence, is of particular importance for the mathematical foundations of such a subject.

The organization of this thesis is the following:

- In partII we review the various equivalent characterizations of classical-algorithmic randomness
- In partIII the issue of formalizing the notion of quantum algorithmic randomness in the framework of Quantum Algorithmic Information Theory is analyzed
- In partIV the complementary issue of analyzing the classical algorithmic information status of quantum-measurements' results is discussed

Part II

Equivalent characterizations of classical algorithmic randomness

Chapter 1

Classical algorithmic randomness as classical algorithmic incompressibility

1.1 The distinction between mathematical-classicality and physical-classicality

The attribute **classicality** is used by two different scientific communities with different meanings:

- it is usually used by Theoretical Physicists to express that some physical system obeys the laws of Classical Mechanics; this is, for example the acception of the adjective **classical** intended in the title of the first two volumes *"Classical Dynamical Systems"* and *"Classical Field Theory"* [Thi97] of Walter Thirring's monography *"A Course in Mathematical Physics"*
- it is usually used by logico-mathematicians to express the part of a theory concerning only mathematical objects with cardinality less or equal to $\aleph_0$; this is, for example, the acception of the adjective **classical** intended in the title *"Classical Recursion Theory"* of Piergiorgio Odifreddi's monography [Odi89], [Odi99a]

Unfortunately such a double acception of the term **classical** have generated many confusions in the literature belonging to the intersection of the two disciplines.

At a foundational level the generated confusion may be seen as a confusion between the **subject** and the **object** of a computational process, i.e. between the **attributes of the computational device** and the **attributes of the computed mathematical objects**.

Hence some property (classicality/quantisticality i.e. commutativity/noncommutativity) is used in two undistinguished (and often interchanged) acceptions according to it refers:

- to the **subject of the computation**, i.e. to the computational device
- to the **object of the computation**, i.e. to the computed mathematical objects

An elegant way of avoiding this kind of mistakes is to pursue the following prescription:

any issue of Computability Theory must analyze separetely each cell of the following:

DIAGRAM 1.1.1

DIAGRAM OF COMPUTATION:

$\frac{OBJECT}{SUBJECT}$	C_M	NC_M
C_Φ	$\cdot_{11}$	$\cdot_{12}$
NC_Φ	$\cdot_{21}$	$\cdot_{22}$

with:

C_M **:** MATHEMATICALLY CLASSICAL

NC_M**:** MATHEMATICALLY NONCLASSICAL

C_Φ**:** PHYSICALLY CLASSICAL

NC_Φ**:** PHYSICALLY NONCLASSICAL

Let us consider, first of all, the following issue:
1^{th} ISSUE: WHAT IS COMPUTABLE ?

- $cell_{11}$: $C_M \cap C_\Phi$

  There is complete agreement in the scientific community that, as to the computation by **physically classical computers** of the following set of functions:

  DEFINITION 1.1.1

  MATHEMATICALLY CLASSICAL FUNCTIONS:

  (partial) functions on sets $S : card(S) \leq \aleph_0$

  Church-Turing's Thesis holds leading to the identification of the computable (partial) functions with the (partial) recursive functions [Odi89], [Odi96] that we will now define.

Introducing a notation we will adopt from here and beyond, we will denote the computability attribute relative to the cell $cell_{ij}$ of the diagram1.1.1 by the symbol $cell_{ij} - \Delta_0^0$.

For example the above statement may be rephrased saying that the set $C_M - C_\Phi - \Delta_0^0 - \overset{\circ}{MAP}(S,S)$ is the set of all the partial recursive functions over S.

Let, clarify, first of all, what we mean by a partial function:

a **total** (i.e. ordinary) $f : A \rightarrow B$ is a rule associating to every element x of the set A an element f(x) of the set B:

$$x \in A \overset{f}{\rightarrow} f(x) \in B$$

We will indicate the set of all the total functions from a set A to a set B by MAP(A,B).

A **partial function** $f : A \overset{\circ}{\rightarrow} B$ is a rule associating to each element x of a certain subset $HALTING(f) \subseteq A$ of A, said the **halting set of f**, an element f(x) of the set B:

$$x \in HALTING(f) \overset{f}{\rightarrow} f(x) \in B$$

We will say that:

DEFINITION 1.1.2

f HALTS ON $x \in A$ $(f(x) \downarrow)$:

$$x \in HALTING(f) \tag{1.1.1.1}$$

DEFINITION 1.1.3

f DOESN'T HALT ON $x \in A$ $(f(x) \uparrow)$:

$$x \notin HALTING(f) \tag{1.1.1.2}$$

We will indicate the set of all the partial functions from a set A to a set B by $\overset{\circ}{MAP}(A,B)$. Given two partial functions $f_1, f_2 \in \overset{\circ}{MAP}(A,B)$:

DEFINITION 1.1.4

f_1 IS EQUAL TO f_2 $(f_1 = f_2)$:

$$(HALTING(f_1) = HALTING(f_2)) \; and \; (f_1(x) = f_2(x) \;\; \forall x \in HALTING(f_1)) \tag{1.1.1.3}$$

The language of **partial functions** is of common use in Mathematical-Logic; we adopt it, anyway, also in unusual environments: from Classical (i.e. commutative) Measure Theory (in which measures' halting sets will be suitable σ-algebras) to Operator Theory on Hilbert spaces (in which unbounded operators' halting sets will be dense subspaces)

Denoted by $\mathbb{N}^{\star} := \bigcup_{n \in \mathbb{N}} \mathbb{N}^{n}$ the set of all the n-ples of natural numbers:

DEFINITION 1.1.5

CLASS OF PARTIAL RECURSIVE FUNCTIONS (ON NUMBERS) ($REC- \overset{\circ}{MAP}$ $(\mathbb{N}^{n} , \mathbb{N})$)

the smallest class of partial functions:

1. containing the initial functions:

$$\begin{aligned} \mathcal{O}(x) &:= 0 && (1.1.1.4) \\ \mathcal{S}(x) &:= x+1 && (1.1.1.5) \\ \mathcal{I}_{i}^{n}(x_{1}, \cdots , x_{n}) &:= x_{i} \;\; i = 1, \cdots , n \, , \, n \in \mathbb{N} && (1.1.1.6) \end{aligned}$$

2. closed under **composition**, i.e. the schema that given $\gamma_{1}, \cdots , \gamma_{m}, \psi$ produces:

$$\varphi(\vec{x}) := \psi(\gamma_{1}(\vec{x}), \cdots , \gamma_{m}(\vec{x})) \qquad (1.1.1.7)$$

3. closed under **primitive recursion**, i.e. the schema that given ψ , γ produces:

$$\begin{aligned} \varphi(\vec{x}, 0) &:= \psi(\vec{x}) && (1.1.1.8) \\ \varphi(\vec{x}, y+1) &:= \gamma(\vec{x}, y, \phi(\vec{x}, y)) && (1.1.1.9) \end{aligned}$$

4. closed under **unrestricted μ-recursion**, i.e. the schema that given ψ produces:

$$\varphi(\vec{x}) := \min\{ y : (\psi(\vec{x}, z) \downarrow \; \forall z \leq y) \, and \, (\psi(\vec{x}, y) = 0) \} \quad (1.1.1.10)$$

   where $\varphi(\vec{x}) := \uparrow$ if there is no such function

The more fundamental properties of partial recursive functions may be collected in the following:

Theorem 1.1.1

GÖDEL'S NUMBERING OF PARTIAL RECURSIVE FUNCTIONS:

It is possible to enumerate all partial recursive functions:

$$\varphi_{e}^{(n)} : \mathbb{N}^{n} \overset{\circ}{\rightarrow} \mathbb{N}$$

(where the natural number **e** is called the **Gödel's number** of the e^{th} n-ary partial recursive function) in such a way that the following conditions are satisfied:

- **Universality:** there is a partial recursive function of two variables $\varphi_z^{(2)}(e,x)$ such that:

$$\varphi_z^{(2)}(e,x) \;=\; \varphi_e^{(1)}(e,x) \;\; \forall x \in \mathbb{N} \tag{1.1.1.11}$$

- **Uniform Composition:** there is a (total) recursive function of two variables *comp* such that:

$$\varphi_{comp(x,y)}^{(1)}(z) \;=\; \varphi_x^{(1)}(\varphi_y^{(1)}(z)) \;\; \forall x,y,z \in \mathbb{N} \tag{1.1.1.12}$$

- **Fixed Point:** For every $m \in \mathbb{N}_+$ and every recursive function f there effectively exists an x (called the fixed point of f) such that:

$$\varphi_x^{(m)} \;=\; \varphi_{f(x)}^{(m)} \tag{1.1.1.13}$$

It is useful to introduce the following notation concerning the domains of partial recursive functions:

DEFINITION 1.1.6

$$\mathcal{W}_e^n \;:=\; HALTING(\varphi_e^{(n)}) \;\; e,n \in \mathbb{N} \tag{1.1.1.14}$$

Given an n-ary relation $R(x_1, \cdots, x_n)$ on $\mathbb{N}$:

DEFINITION 1.1.7

R IS RECURSIVELY ENUMERABLE (R.E.):

$$\exists e \in \mathbb{N} \;:\; R \;=\; \mathcal{W}_e^n \tag{1.1.1.15}$$

We will identify, from here and beyond, **sets** and **unary relations** by posing:

$$\mathcal{W}_e \;:=\; \mathcal{W}_e^1 \tag{1.1.1.16}$$

Given a set $S \subset \mathbb{N}^\star$:

DEFINITION 1.1.8

S IS RECURSIVE:

the characteristic function χ_S:

$$\chi_S(x) \;:=\; \begin{cases} 1 & \text{if } x \in S, \\ 0 & \text{otherwise.} \end{cases} \tag{1.1.1.17}$$

is a total recursive function

Clearly one has that:

Theorem 1.1.2

RECURSIVITY IS STRONGER THAN RECURSIVE ENUMERABILITY:

$$\begin{aligned} \textit{recursivity} &\Rightarrow \text{ recursive enumerability} \\ \text{recursive enumerability} &\nRightarrow \textit{recursivity} \end{aligned}$$

Remark 1.1.1

GÖDEL NUMBERING AND SELF-REFERENCE

Gödel's numbering, introduced by Kurt Gödel in his his famous 1931's paper *"On Formally Undecidable Propositions of the Principia Mathematica and Related Systems"* [Dav65], is a deep concept since it creates that link between **language** and **meta-language** giving rise to self-reference and all the consequences it generates through Cantor's Diagonalization.

Since recursivity is equivalent to representability in an arbitary consistent formal system extending Tarski-Montowski-Robinson Arithmetics Gödel's numbering may be equivalentely seen as a way of enumerating all the logical propositions concerning natural numbers.

So one has a hierarchy of levels:

1. the **objects** of investigation, i.e. natural numbers
2. the **language** by which properties of the objects are described, i.e. the logical propositions concerning the objects
3. the **meta-language** by which properties of the **meta-objects**, i.e the logical propositions of the language (by which properties of the objects are described) are described; we will denote by **meta-proposition** a proposition of the **meta-language**

Owing to Gödel numbering, a **number** plays a double rule:

– as an **object**
– as the Gödel number identifying a proposition of the language, i.e. as a **meta-object**

This can be used to pass from **meta-language** to the **language**, simply associating to the **meta-proposition** $\varphi_e(x)$ concerning the **meta-object** x, i.e. the proposition of the language with Gödel number x, the **proposition** $\varphi_e(x)$ concerning the **object**, i.e. the number, x and, viceversa, to pass from **language** to **meta-language**, associating to the **proposition** $\varphi_e(x)$ concerning the **object**, i.e. the number, x the **meta-proposition** $\varphi_e(x)$ concerning the **meta-object** x, i.e. the proposition of the language with Gödel number x.

But then self-reference immediately appears since $\varphi_e(e)$ happens to speak about itself.

- $cell_{21}$: $C_M \cap NC_\Phi$

  There is no universally accepted answer in the scientific community to the question if a **physically nonclassical computer** can violate Church-Turing's Thesis, i.e. can compute non-recursive **mathematically classical functions**.

  In particular, as far as the computation by **physically quantistical computers** of **mathematically classical functions** is concerned, the common opinion among the researchers in Quantum Computation [Fey99], [Deu85], [Joz98] is that **Nonrelativistic Quantum Mechanics** and **Special-relativistic Quantum Mechanics (Local Quantum Field Theories)** don't violate Church-Turing's Thesis.

  It must be cited, anyway, that the opposite thesis has been asserted by various authors (cfr. [Vin92], [Joz99], [Svo00] and the paragraphs 4.12 and 4.23 of [Pau01])

  Furthermore it must be observed that in the Masanao Ozawa's final formalization of Quantum Turing Machines [Oza98c] (saying according, to us, the last word on the consistence's problem of Deutsch's Halting Protocol) the satisfaction of the Church-Turing's Thesis is posed by hand restricting the range of the local transition function to recursive complex numbers.

  We will, anyway, extensively return on this point in section8.1

  Finally, when **Generally-relativistic Quantum Mechanics** (both in the form of **Quantum Gravity** and in the form of some suggested **gravitationally-modificated Quantum Mechanics**) is considered, the whole story touches the strongly debated ideas of Roger Penrose about a non-computable alteration of the quantum unitary dynamics induced by gravity [Pen89], [Pen96], [Ana98], [Pen00].

- $cell_{12}$: $NC_M \cap C_\Phi$

  As soon as one goes out from the boundaries of C_M-Classical Recursion Theory the almost miracolous equivalence of all the different approaches (recursivity, finitely definability, Herbrand-Gödel Computability, representability in consistent formal system extending Tarski-Montowski-Robinson Arithmetics, λ-definability in Church's λ- Calculus, flowchart computability, computability by Classical Turing Machines, by cellular automata [Odi89], by Shepherdson-Sturgis register machines [Cut80], LISP computability [Car60], $\cdots$) that in such a theory manifests the strong experimental verification of Church's Thesis, dramatically disappears.

  Just as to Computability Theory by **physically classical computers** of (partial) functions on sets $S : cardinality(S) = \aleph_1$ while many different inequivalent candidate theories have been proposed:

  1. the well extablished and almost always accepted theory named Computable Analysis, generated by the studies of Grzegorczyck - Lacombe [Ric89]

2. the theory developed by the so called Markov School in the framework of Constructive Mathematics [Odi89]
3. the Blum - Shub - Smale 's Theory [Sma92], [S.S98]

The relative popularity of the issue about the concurrence of such candidate theories is owed to Penrose's question if Mandelbrot's set is recursive [Pen89]. We will partially analyze it in section1.6

- $cell_{22} \; : \; NC_M \cap NC_\Phi$

  It's important to realize that, contrary to what is often claimed, Church-Turing's Thesis doesn't imply that the answer to the $1^{th} ISSUE$ contained in the cells $cell_{12}$ and $cell_{22}$ must be equal.

  For example Church-Turing's Thesis is not incompatible with an hypothetical situation in which Mandelbrot's set would be C_Φ - incomputable but NC_Φ - computable.

  Though some undecidability theorems and conjectures still exist (cfr. e.g. Lloyd's arguments concerning uncomputable diagonalizations in Quantum Computation [Llo89] as well as his general consideration about the physical limits of Computation [Loy01], or Geroch and Hartle's speculations concerning the eventuality that the recursive undecidability of the Homeomorphism-problem for four-manifolds [Zie98] may lead to the recursive undecidability of quantizing Gravity) no general mathematically formalization has been realized yet.

  Particular importance has, according to us, Karl Svozil's suggestion that in Quantum Algorirhmic Information Theory there should exist undecidability theorems analogues to the classical Chaitin's ones (cfr. the problem17 of [Cal96]).

1.2 Uspensky's abstract definition of algorithmic information

The last contribution Andrei Nikolaevich Kolmogorov left us before dying was his forum report *Algorithms and Randomness*, made with and exposed by his student Vladimir Uspensky, at the First World Congress of the Bernoulli Society (September 8-14, 1986) [Soc00].

Later Unspensky formalized the Kolmogorovian approach to Algorithmic Information Theory in a very general and elegant way we will start from [Usp92], [Sem93].

DEFINITION 1.2.1

AGGREGATE:
a couple (X , R) such that:

- X is a set
- R, called a **concordance relation**, is a computable binary relation on X

Remark 1.2.1

CONTEXT-DEPENDENCE OF THE COMPUTABILITY CONSTRAINT
Let us observe that, in the definition def.1.2.1 we have imposed a **computability constraint** without specifying its precise mathematical meaning.

This has been done in order of guaranteeing the maximal generality: in the different contextes corresponding to the different cells $cell_{ij}$ of the diagram1.1.1 such a constraint is formalized by the proper $cell_{ij} - \Delta_0^0$ condition

Given two aggregates $A_1 := (X_1 , R_1)$ and $A_2 := (X_2 , R_2)$ it is natural to ask under which conditions we can think to elements of A_2 as descriptions of elements of A_1 with respect to a proper description mode;

the answer is given by the following definition:

DEFINITION 1.2.2

MODE OF DESCRIPTION (OF A_2-ELEMENTS THROUGH A_1-ELEMENTS):
a relation R between elements of X_1 and elements of X_2 such that:

$$R_1(x_1, y_1) \, and \, R_2(x_2, y_2) \, and \, R(x_1, x_2) \;\Rightarrow\; R(y_1, y_2) \;\; \forall x_1, x_2 \in X_1, \forall y_1, y_2 \in X_2 \tag{1.2.1.1}$$

We will denote the set of all the mode of description of A_2-elements through A_1-elements by $\mathcal{D}(A_1, A_2)$.

Given a mode of description R among the aggregates A_1 and A_2:

DEFINITION 1.2.3

$x_2 \in X_2$ IS A DESCRIPTION OF $x_1 \in X_1$ THROUGH THE MODE R:

$$R(x_1, x_2) \tag{1.2.1.2}$$

All the ingredients introduced up to this point are of pure set-theoretic nature (with some constructibility constraint).

The introduction of a notion characterizing the amount of not-redundant, i.e. algorithmically incompressible, information of an object $x_1 \in X_1$ with respect to the description mode R requires the introduction of some point measure quantifying the extension of the descriptions.

Let us, then, define, the following notion:

DEFINITION 1.2.4

METRIC AGGREGATE:

a couple $(A\,,\mu)$ such that:

- $A \,:=\, (X\,,R)$ is an aggregate
- μ is a point measure on A

Given a metric aggregate $A_1 \,:=\, (X_1\,,\,R_1\,,\,\mu)$, an aggregate $A_2 \,:=\, (X_2\,,\,R_2\,)$ and a mode of description R among the aggregates A_1 and A_2 we can finally introduce the following basic notion:

DEFINITION 1.2.5

ALGORITHMIC INFORMATION OF $x_2 \in X_2$ W.R.T. THE DESCRIPTION MODE R:

$$I_R(x_2) \,:=\, \begin{cases} \min\{\mu(x_1) \,:\, R(x_1, x_2)\} & \text{if } \exists\, x_1 \in X_1 \,:\, R(x_1, x_2), \\ +\infty & \text{otherwise.} \end{cases} \tag{1.2.1.3}$$

Clearly the definition def.1.2.5 depends on the particular chosen description mode R.

It is clear, anyway, that the whole consistence of Algorithmic Information Theory lies on the possibility of getting-rid of such a dependence.

The formalization of this issue is given by the following notions:

DEFINITION 1.2.6

UNIVERSE OF DESCRIPTION OF A_2 THROUGH A_1:

a set $\mathcal{R}$ of description modes of the aggregate A_2 through the metric aggregate A_1:

$$\mathcal{R} \,\subseteq\, \mathcal{D}(A_1, A_2) \tag{1.2.1.4}$$

The intuitive idea we are going to formalize is that Algorithmic Information Theory is meaningful provided the involved universes of descriptions admit optimal mode of descriptions, i.e. mode of descriptions that are always more concise of all the others, up to an object-independent additive constant.

This requires the introduction of two ordering relation we will use extensively in the whole dissertation.

Given two real-valued partial function $f_1 : A \overset{\circ}{\to} \mathbb{R}$, $f_2 : A \overset{\circ}{\to} \mathbb{R}$ we will say that:

DEFINITION 1.2.7

f_1 IS ADDITIVELY LESS OR EQUAL TO f_2 ($f_1 \overset{+}{\leq} f_2$)

$$\exists c \in \mathbb{R}_+ \ : \ f_1(x) \ \leq \ f_2(x) + c \ \ \forall x \in HALTING(f_1) \bigcap HALTING(f_2) \tag{1.2.1.5}$$

DEFINITION 1.2.8

f_1 IS ADDITIVELY EQUAL TO f_2 ($f_1 \overset{=}{\leq} f_2$)

$$f_1 \overset{+}{\leq} f_2 \ and \ f_2 \overset{+}{\leq} f_1 \tag{1.2.1.6}$$

DEFINITION 1.2.9

f_1 IS MULTIPLICATIVELY LESS OR EQUAL TO f_2 ($f_1 \overset{\times}{\leq} f_2$)

$$\exists c \in \mathbb{R}_+ \ : \ f_1(x) \ \leq \ f_2(x) \times c \ \ \forall x \in HALTING(f_1) \bigcap HALTING(f_2) \tag{1.2.1.7}$$

DEFINITION 1.2.10

f_1 IS MULTIPLICATIVELY EQUAL TO f_2 ($f_1 \overset{\times}{=} f_2$)

$$f_1 \overset{\times}{\leq} f_2 \ and \ f_2 \overset{\times}{\leq} f_1 \tag{1.2.1.8}$$

Let us now consider an aggregate A_1, a metric aggregate A_2, a universe of description $\mathcal{R}$ of A_1 through A_2 and a particular mode of description belonging to such a universe $U \in \mathcal{R}$.

We will say that:

DEFINITION 1.2.11

U IS OPTIMAL W.R.T. $\mathcal{R}$:

$$U \ \overset{+}{\leq} \ f \ \ \forall f \in \mathcal{R} \tag{1.2.1.9}$$

We can then introduce the following notion:

DEFINITION 1.2.12

ALGORITHMIC INFORMATION THEORY IS MEANINGFUL W.R.T. $\mathcal{R}$:

$$\exists\, U \in \mathcal{R} \ optimal \tag{1.2.1.10}$$

Adhering to Uspensky's terminology let us introduce the following notion:

DEFINITION 1.2.13

ALGORITHMIC ENTROPY:
a function I equal to the algorithmic information w.r.t. a description mode that is optimal w.r.t to some universe of description modes.

In order to discuss the first fundamental examples, let us introduce some basic notions.
Given a set Σ:

DEFINITION 1.2.14

SET OF THE STRINGS ON Σ :

$$\Sigma^{\star} \ \equiv \ \{\lambda\} \bigcup \cup_{k \in \mathbb{N}} \Sigma^{k} \tag{1.2.1.11}$$

DEFINITION 1.2.15

SET OF THE SEQUENCES ON Σ:

$$\Sigma^{\infty} \ \equiv \ \{\lambda\} \bigcup \{\bar{x} : \mathbb{N}_{+} \ \rightarrow \ \Sigma\} \tag{1.2.1.12}$$

where λ denotes the *empty string*.
Given $\vec{x} \in \Sigma^{\star}$ let us denote by $\vec{x}^{n} \in \Sigma^{\star}$ the string made of n repetitions of $\vec{x}$ and by $\vec{x}^{\infty} \in \Sigma^{\infty}$ the sequence made of infinite repetitions of $\vec{x}$.
It is important to remark that [Cal94]:

Theorem 1.2.1

ON THE CARDINALITIES OF STRINGS AND SEQUENCES OVER A FINITE ALPHABET
HP:

$$cardinality(\Sigma) \ \in \ \mathbb{N}$$

TH:

$$\begin{aligned} cardinality(\Sigma^{\star}) \ &= \ \aleph_{0} \\ cardinality(\Sigma^{\infty}) \ &= \ \aleph_{1} \end{aligned}$$

We will assume from here and beyond that $\Sigma \ := \ \{0, 1\}$.
The total-ordering $0 \ < \ 1$ induces the following:

DEFINITION 1.2.16

QUASI-LEXICOGRAPHIC ORDERING ON $\Sigma^\star$

$$\lambda < 0 < 1 < 00 < 01 < \\ 10 < 11 < 000 < 001 < \cdots 111 < \cdots \tag{1.2.1.13}$$

We can then introduce the following bijection:

DEFINITION 1.2.17

QUASI-LEXICOGRAPHIC MAP:

$$\begin{aligned} &string : \mathbb{N} \to \Sigma^\star \\ &string(n) \; = \text{the } n^{th} \text{ string in quasi-lexicographic ordering} \end{aligned} \tag{1.2.1.14}$$

Let us now introduce the following ordering relation on $\Sigma^\star$

DEFINITION 1.2.18

PREFIX-ORDER RELATION $<_p$ ON $\Sigma^\star$:

$$\vec{x} <_p \vec{y} \; := \; \exists \vec{z} \in \Sigma^\star \; : \; \vec{y} = \vec{x} \cdot \vec{z} \tag{1.2.1.15}$$

Give a set $S \subset \Sigma^\star$ we will say that:

DEFINITION 1.2.19

S IS PREFIX-FREE:

$$(\vec{x} <_p \vec{y} \Rightarrow \vec{x} = \vec{y}) \, \forall \vec{x}, \vec{y} \in S \tag{1.2.1.16}$$

Example 1.2.1

SIMPLE ALGORITHMIC ENTROPY

Let us consider the case in which $A_1 \; = \; A_2 \; = \; (\mathbb{N}, =, |\cdot|)$ with:

$$|n| \; := \; |string^{-1}(n)| \; = \; \llcorner \log_2(n+1) \lrcorner \tag{1.2.1.17}$$

Kolmogorov started considering as universe of mode of descriptions the whole $\mathcal{D}(A_1, A_2)$.

But he immediately realized that:

Theorem 1.2.2

ALGORITHMIC INFORMATION THEORY W.R.T. $\mathcal{D}(A_1, A_2)$ IS NOT MEANINGFUL

PROOF:

Following [Vit97] let us us suppose by abdurdum that there exist a function $U \in \bigcap \mathcal{D}(A_1, A_2)$ such that:

$$U \overset{+}{\leq} f \;\; \forall f \in \mathcal{D}(A_1 \,,\, A_2) \tag{1.2.1.18}$$

Let us then consider an infinite sequence $X \,:=\, \{x_n \in \mathbb{N}\}_{n \in \mathbb{N}}$ such that:

$$i < j \;\Rightarrow\; x_i < x_j \;\; \forall i, j \in \mathbb{N} \tag{1.2.1.19}$$

Considered a subsequence $Y \,:=\, \{y_n \in \mathbb{N}\}_{n \in \mathbb{N}}$ of the sequence X such that:

$$\log y_n \;<\; \frac{\log x_n}{2} \;\; \forall n \in \mathbb{N} \tag{1.2.1.20}$$

let us introduce the function $f \in \mathcal{D}(A_1, A_2)$ conciding with U everywhere but for the points of the sequence X where it is defined as:

$$f(x_n) \;:=\; U(y_n) \;\; \forall n \in \mathbb{N} \tag{1.2.1.21}$$

We have clearly that:

$$cardinality(\{n \in \mathbb{N} : I_f(n) \leq \frac{I_U(n)}{2}\}) \;=\; \aleph_0 \tag{1.2.1.22}$$

that contradict the absurdum hypothesis ■

Theorem1.2.2 is the first of a set of theorems we will meet in this dissertation showing that certain quantities of Algorithmic Information Theory are meaningful only by effectivizing some notion.

Indeed, requiring that to describe objects must be an effective property, one is led by Church-Turing's thesis, for reasons that will be clarified in the next section, to restrict the universe of modes of descriptions to the set $C_M - C_\Phi - \Delta_0^0[\mathcal{D}(A_1, A_2)]$ of the **partial recursive ones**.

Kolmogorov realized that in this way the problem was overcome proving the following [Cal94]:

Theorem 1.2.3

INVARIANCE THEOREM FOR SIMPLE ALGORITHMIC ENTROPY:

Algorithmic Information Theory w.r.t. $C_M - C_\Phi - \Delta_0^0 - [\mathcal{D}(A_1, A_2)]$ is meaningful

As we have preannounced, the resulting algorithmic entropy, w.r.t. an optimal description mode that we will call from here and beyond a **simple universal computer**, is called the **simple algorithmic entropy** and is denoted by K.

Example 1.2.2

MONOTONE ALGORITHMIC ENTROPY

Let us consider the case in which $A_1 \;=\; A_2 \;=\; (\Sigma^\star \,,\, <_p \,,\, |\cdot|)$.

Exactly as in the example1.2.1 it may be proved that:

Theorem 1.2.4

ALGORITHMIC INFORMATION THEORY W.R.T. $\mathcal{D}(A_1, A_2)$ IS NOT MEANINGFUL

but:

Theorem 1.2.5

INVARIANCE THEOREM FOR MONOTONE ALGORITHMIC ENTROPY:

Algorithmic Information Theory w.r.t. $C_M - C_\Phi - \Delta_0^0 - [\mathcal{D}(A_1, A_2)]$ is meaningful

As we have preannounced, the resulting algorithmic entropy is called the **monotone algorithmic entropy**

Remark 1.2.2

FROM BINARY STRINGS TO NATURAL NUMBERS AND VICEVERSA

For pure simplicity reasons we have defined simple algorithmic entropy for natural numbers and monotone algorithmic information for binary strings.

By the quasi-lexicographic bijection the corrispondent notions, namely simple algorithmic entropy of strings and prefix algorithmic entropy of natural numbers are immediately obtained.

For the same reason from here and beyond everything stated for $\Sigma^\star$ may be immediately translated in terms of $\mathbb{N}$ and viceversa.

Up to now we have considered the case in which the two metric aggregates coincide.

Anyway one can clearly introduce also the following mixed notions:

Example 1.2.3

DECISION ALGORITHMIC ENTROPY:

Let us assume $A_1 = (\mathbb{N}, =, |\cdot|)$ while $A_2 = (\Sigma^\star, <_p, |\cdot|)$.

Exactly as in the example1.2.1 it may be proved that:

Theorem 1.2.6

ALGORITHMIC INFORMATION THEORY W.R.T. $\mathcal{D}(A_1, A_2)$ IS NOT MEANINGFUL

but:

Theorem 1.2.7

INVARIANCE THEOREM FOR DECISION ALGORITHMIC ENTROPY:

Algorithmic Information Theory w.r.t. $C_M - C_\Phi - \Delta_0^0 - [\mathcal{D}(A_1, A_2)]$ is meaningful

As we have preannounced, the resulting algorithmic entropy is called the **monotone algorithmic entropy**

Example 1.2.4

PREFIX ALGORITHMIC ENTROPY:

Let us assume $A_1 = (\Sigma^\star, <_p, |\cdot|)$ while $A_2 = (\mathbb{N}, =, |\cdot|)$.

Exactly as in the example1.2.1 it may be proved that:

Theorem 1.2.8

ALGORITHMIC INFORMATION THEORY W.R.T. $\mathcal{D}(A_1, A_2)$ IS NOT MEANINGFUL

but:

Theorem 1.2.9

INVARIANCE THEOREM FOR PREFIX ALGORITHMIC ENTROPY:

Algorithmic Information Theory w.r.t. $C_M - C_\Phi - \Delta_0^0 - [\mathcal{D}(A_1, A_2)]$ is meaningful

As we have preannounced, the resulting algorithmic entropy, w.r.t. an optimal description mode that we will call from here and beyond a **Chaitin universal computer**, is called the **prefix algorithmic entropy** and is denoted by I.

While the **decision entropy** and **monotone entropy** are of scarce utility, **simple entropy** and **prefix entropy** are of fundamental importance

1.3 Why prefix algorithmic entropy is better than simple algorithmic entropy

Let us now compare simple algorithmic entropy and prefix algorithmic entropy.

Though more intuitive, simple algorithmic entropy has a list of inconveniences that, after decades of debates among different attempts, led the scientific community to realize that the correct way of formulating Classical Algorithmic Information Theory involves prefix algorithmic entropy:

1. **classical probabilistic information**, namely **Shannon entropy**, satisfies the **subadditivity property**:

   $$I_{probabilistic}(X,Y) \leq I_{probabilistic}(X) + I_{probabilistic}(Y) \qquad (1.3.1.1)$$

   with the equality holding iff the classical random variables X and Y are independent, where the joint probabilistic information $I_{probabilistic}(X,Y)$ will be defined in section7.3.

   As we will see therein the subadditivity property remain preserved in the noncommutative generalization, i.e. eq.1.3.1.1 holds also in Quantum Probability Theory, where $I_{probabilistic}$ is the **quantum probabilistic information**, namely **Von Neumann entropy**, (X , Y) denotes a state over a tensor product Von Neumann algebra $A_1 \bigotimes A_2$ having X and Y as marginal states, the equality holding iff (X , Y) is not entangled.

   The intuitive meaning of eq.1.3.1.1 (the information of a compound system is less or equal to the information of its parts) lead to think that such a condition should hold also for **classical algorithmic information**.

   As to **simple algorithmic entropy**, anyway, the subadditivity condition is violated by a disturbing logarithmic addendum causing that:

   Theorem 1.3.1

   NOT SUBADDITIVITY OF SIMPLE ALGORITHMIC ENTROPY

   $$K((\vec{x},\vec{y})) \stackrel{+}{\not\leq} K(\vec{x}) + K(\vec{y}) \qquad (1.3.1.2)$$

   The subadditivity property is instead satisfied by **prefix algorithmic entropy**:

   Theorem 1.3.2

   SUBADDITIVITY OF PREFIX ALGORITHMIC ENTROPY

   $$I((\vec{x},\vec{y})) \stackrel{+}{\leq} I(\vec{x}) + I(\vec{y}) \qquad (1.3.1.3)$$

2. intuitive reasoning suggests that $C_M - C_\Phi$-algorithmic information should be **monotonic over prefixes**.

   Anyway one has that:

Theorem 1.3.3

NOT MONOTONICITY OVER PREFIXES OF SIMPLE ALGORITHMIC INFORMATION

$$\vec{x} <_p \vec{y} \not\Rightarrow K(\vec{x}) \stackrel{+}{\leq} K(\vec{y}) \qquad (1.3.1.4)$$

while:

Theorem 1.3.4

MONOTONICITY OVER PREFIXES OF PREFIX ALGORITHMIC INFORMATION

$$\vec{x} <_p \vec{y} \Rightarrow I(\vec{x}) \stackrel{+}{\leq} I(\vec{y}) \qquad (1.3.1.5)$$

3. since the **probabilistic approach** and the **algorithmic approach** to $C_M - C_\Phi$ - Information Theory are different ways of formalizing the same object of investigation, it is natural to suppose that $C_M - C_\Phi$-**probabilistic information** and $C_M - C_\Phi$-**algorithmic information** are strictly connected notions.

   While the link is very clear in term of **prefix algorithmic entropy**, anyway, it is much obscure in terms of **simple algorithmic entropy**.

   To show this it is necessary to introduce some notion of C_M - Coding Theory:

   DEFINITION 1.3.1

   C_M - CODE:

   a partial function $D : \Sigma^\star \stackrel{\circ}{\mapsto} \Sigma^\star$ of decoding associating to each word $\vec{x}$ belonging to the set HALTING(D) of **code words** its **source word** $D(\vec{x})$.

   Given a C_M - code D and a source word $\vec{x} \in \Sigma^\star$:

   DEFINITION 1.3.2

   SET OF THE D - CODE WORDS OF $\vec{x}$:

   the (eventually empty) set $D^{-1}(\vec{x})$.

   Let us observe that the definition1.3.1 doesn't require nor the surjectivity of a code (i.e. that each source word is codificable) neither the injectivity of a code (i.e. that each source word has only one code word).

   Let us now introduce a particular fundamental kind of code:

   DEFINITION 1.3.3

PREFIX-CODE:
a code $D : \Sigma^{\star} \overset{\circ}{\mapsto} \Sigma^{\star}$ such that HALTING(D) is prefix-free

The more fundamental property of prefix-codes is given by the following:

Theorem 1.3.5

KRAFT'S INEQUALITY
HP:

$$I \text{ index set} : cardinality(I) \leq \aleph_0$$
$$\{l_i \in \mathbb{N}\}_{i \in I}$$

TH:

$$\exists\, D : \Sigma^{\star} \overset{\circ}{\mapsto} \Sigma^{\star} \text{ prefix code} : \{|\vec{x}|, \vec{x} \in HALTING(D)\} = \{l_i \in \mathbb{N}\}_{i \in I} \Leftrightarrow \sum_{i \in I} 2^{-l_i} \leq 1 \tag{1.3.1.6}$$

We will appreciate the importance of Kraft Inequality as soon as we will introduce the **universal algorithmic probability** and the **Halting Probability**.

Let us now start the probabilistic analysis of C_M - Coding Theory.
Let us suppose that the generic source-word $\vec{x}$ occur with probability $P(\vec{x})$.
Given an injective prefix-code $D : \Sigma^{\star} \overset{\circ}{\mapsto} \Sigma^{\star}$ we can then introduce the:

DEFINITION 1.3.4

AVERAGE CODE WORD LENGTH OF THE CODE D W.R.T. THE SOURCE CODE DISTRIBUTION P:

$$L_{D,P} := \sum_{\vec{x} \in HALTING(D)} P(\vec{x})|D(\vec{x})| \tag{1.3.1.7}$$

It is clear that, in a communicational situation, the objective of a transmitter is to minimize the average code word length.
Clearly a coding strategy will be the more clever the more it will assign short code words to highly probable source words and viceversa, in order to minimize the average code word length.

DEFINITION 1.3.5

MINIMAL AVERAGE CODE WORD LENGTH ALLOWED BY THE DISTRIBUTION P:

$$L := \min\{L_{D,P} \, , \, D \, prefix - code\} \tag{1.3.1.8}$$

DEFINITION 1.3.6

OPTIMAL PREFIX-CODE W.R.T. THE SOURCE CODE DISTRIBUTION P:

a prefix-code D such that:

$$L_{D,P} = L \tag{1.3.1.9}$$

The probabilistic approach to $C_M - C_\Phi$ Information Theory is based on the following notion:

DEFINITION 1.3.7

SHANNON ENTROPY OF THE DISTRIBUTION P:

$$H(P) := - \sum_{\vec{x} \in \Sigma^\star} P(\vec{x}) \log_2 P(\vec{x}) \tag{1.3.1.10}$$

The corner stone of $C_M - C_\Phi$ Probabilistic Information Theory is the following:

Theorem 1.3.6

$C_M - C_\Phi$ NOISELESS CODING THEOREM

$$H(P) \leq L \leq H(P) + 1 \tag{1.3.1.11}$$

Let us now observe that **prefix algorithmic entropy** may be used to define a particular code:

by definition we have that:

$$I(\vec{x}) = |\vec{x}^\star| \tag{1.3.1.12}$$

where $\vec{x}^\star$ is the shortest input for the fixed universal Chaitin computer giving $\vec{x}$ as output (or the first one in quasi-lexicographic order if there are many).

The map $D_I : \Sigma^\star \overset{\circ}{\mapsto} \Sigma^\star$ defined by:

$$D_I(\vec{x}) := \vec{x}^\star \tag{1.3.1.13}$$

is by construction a prefix-code.

Since the code D_I is of pure algorithmic nature, it would be very reasonable to think that it may me optimal only for some ad hoc probability distribution, i.e. that for a generic probability distribution P the average code word length of D_I w.r.t. P:

$$L_{D_I,P} \; = \sum_{\vec{x} \in HALTING(D_I)} P(\vec{x}) I(\vec{x}) \qquad (1.3.1.14)$$

won't achieve the optimal bound of H(P) stated by Theorem1.3.6

But here the deep link between the **probabilistic-approach** and the **algorithmic-approach** makes the miracle: under mild assumptions about the distribution P the code D_I is optimal as is stated by the following:

Theorem 1.3.7

LINK BETWEEN $C_M - C_\Phi$ PROBABILISTIC INFORMATION AND $C_M - C_\Phi$ ALGORITHMIC INFORMATION

HP:

P $C_M - C_\Phi - \Delta_0^0$ probability distribution over $\Sigma^\star$

TH:

$$\exists c_P \in \mathbb{R}_+ \; : \; 0 \; \leq \; L_{D_I,P} - H(P) \; \leq \; c_P \qquad (1.3.1.15)$$

Such a result of a substantial equivalence between **Shannon entropy** and **average algorithmic prefix entropy** has a strongly weaker counterpart in terms of **algorithmic simple entropy**.

Indeed the two algorithmic entropies are linked by the following:

Theorem 1.3.8

FIRST SOLOVAY'S THEOREM:

$$I(\vec{x}) \; = \; K(\vec{x}) \, + \, K(string^{-1}(K(\vec{x})) \, + \, O(K(string^{-1}K(string^{-1}(K(\vec{x}))))) \qquad (1.3.1.16)$$

$$K(\vec{x}) \; = \; I(\vec{x}) \, - \, K(string^{-1}(K(\vec{x})) \, - \, O(I(string^{-1}I(string^{-1}(I(\vec{x}))))) \qquad (1.3.1.17)$$

that substituted in the Theorem1.3.7 gives:

$$-c_P \;\leq\; L_{D_K,P} - H(P) \;\leq\; \sum_{\vec{x}} P(\vec{x}) K(string^{-1}(C(string^{-1}(\vec{x})))) \tag{1.3.1.18}$$

which is bounded only if $\sum_{\vec{x}} P(\vec{x}) K(string^{-1}(C(string^{-1}(\vec{x}))))$ converges.

4. called U the fixed Chaitin universal computer let us introduce the main actors of some of the most fascinating developes of $C_M - C_\Phi$ Algorithmic Information Theory:

   DEFINITION 1.3.8

   UNIVERSAL ALGORITHMIC PROBABILITY OF $\vec{x} \in \Sigma^\star$:

   $$P_U(\vec{x}) \;:=\; \sum_{\vec{y} \in \Sigma^\star : U(\vec{y}) = \vec{x}} 2^{-|\vec{y}|} \tag{1.3.1.19}$$

   DEFINITION 1.3.9

   HALTING PROBABILITY:

   $$\Omega_U \;:=\; \sum_{\vec{x} \in \Sigma^\star} P_U(\vec{x}) \tag{1.3.1.20}$$

   These notion has a very intuitive meaning:

   - $P_U(\vec{x})$ is the probability that the computer U gives as output the string $\vec{x}$ under an uniformely random distributed input.
   - Ω_U gives the probability that the computer U halts under an uniformely random distributed input.

   Such a probabilistic meaning,anyway, lies on the fact that U is a **Chaitin computer** so that its halting set is prefix-free and hence Theorem1.3.5 implies that:

   $$0 \;\leq\; P_U(\vec{x}) \;\leq\; 1 \;\; \forall \vec{x} \in \Sigma^\star \tag{1.3.1.21}$$

   and that:

   $$0 \;\leq\; \Omega_U \;\leq\; 1 \tag{1.3.1.22}$$

   If we considered **simple algorithmic information** instead of **prefix algorithmic information** and hence we adopted a **non Chaitin computer**, anyway, the halting set of U wouldn't be prefix-free anymore, so that Theorem1.3.5 wouldn't imply eq.1.3.1.21 and eq.1.3.1.22.

5. Unlike **prefix algorithmic information**, **simple algorithmic information** is affected by oscillations that exclude the possibility of using it to define the notion of algorithmic randomness for sequences in an enough robust way as we will show in the next section

1.4 Chaitin random strings and sequences of cbits

Let us suppose to make 100 independent tosses of a coin.

If we obtained head all times we would certainly claim the the used coin is not fair.

But let us observe that, assuming that the coin is fair, the string of 100 heads have the same exact probability, i.e. 2^{-100}, of any other binary string of 100 cbits.

So, which foundation could we give at our claim that the coin is not fair?

The first to analyze this problem was Laplace that dedicated to this issue the Fifth Principle among the *"General Principles of the calculus of probabilities"* making the content of the third chapter of his pioneering work [dL51]; it is worth to report his own words:

> *"Sixth Principle: Each of the causes to which an observed event may be attributed is indicated with just as much likelihood as there is probability that the event will take place supposing the event to be constant. The probability of the existence of any one of these causes is then a fraction whose numerator is the probability of the event resulting from this cause and whose denominator is the sum of the similar probabilities relative to all the causes; if these various causes considerated à priori, are unequally probable, it is necessary in place of the probability of the event resulting from each cause, to employ the product of this probability by the possibility of the cause itself. This is the fundamental principle of this branch of the analysis of chances which consists in passing from events to causes. This principle gives the reason why we attribute regular events to a particular cause. Some philosophers have thought that these events are less possible than others and that at the play of heads and tails, for example, the combiantion in which heads occurs twenty successive times is less easy in its nature than those where head and tails are mixed in irregular manner. But this opinion suppose that past events have an influence on the possibility of future events which is not at all admissible. The regular combinations occur more rarely only because they are less numerous. $\cdots$ Thus at the play of head and tail the occurence of heads a hundred successive times appears to us extraordinary because of the almost infinite number of combinations which may occur in a hundred throws; and if divide the combinations in two regular series containing an order easy to comprehend, and into irregular series, the latter are incomparably more numerous"*

Laplace catchs the following basic points:

- what the string made of one hundred heads have of particular is to possess some kind of regularity
- this string has the same probability 2^{-100} of every other string
- the fact that if this string of results occurs we can claim the coin was unfair is founded by the observation that the fraction of the set of 100 cbit strings made by strings having some kind of regularity, i.e. the probability that

a string of this kind occurs, is enormously low and , conseguentially, the probability that a string of this kind occurs is extraordinarily low.

The only thing Laplace wasn't able to explain, as anyone else for little less than two centuries, was the exact meaning of the locution ***"to possess some regularity"***.

In this dissertation we will see how Classical Algorithmic Information Theory gives many equilavent mathematical characterization of this **absence of regularity** or, as we say it nowadays , of this **algorithmic randomness**.

Among these characterization the more important one is with no doubt that as **algorithmic incompressibility**.

As an **algorithmically incompressible** object we mean, informally speaking , an object whose more concise algorithmic description is substantially its own assignation.

So one could be to tempted to say that the string $\vec{x} \in \Sigma^{\star}$ is algorithmically random iff:

$$K(\vec{x}) \;=\; |\vec{x}| \tag{1.4.1.1}$$

or iff:

$$I(\vec{x}) \;=\; |\vec{x}| \tag{1.4.1.2}$$

The meaningness of these definitions, anyway, appear evident as soon as one keeps into account , as to eq.1.4.1.1, the issue of the additive constant involved in the passage from a **universal computer** to another **universal computer** and, as to eq.1.4.1.2, the issue of the additive constant involved in the passage from a **Chaitin universal computer** to another **Chaitin universal computer**.

The notion of random string originally introduced by Kolmogorov in 1965 was the following: given a constant $c \in \mathbb{R}_{+}$:

DEFINITION 1.4.1

$\vec{x} \in \Sigma^{\star}$ IS c-KOLMOGOROV-RANDOM:

$$K(\vec{x}) \;\geq\; |\vec{x}| \,-\, c \tag{1.4.1.3}$$

Before of analyzing the analogous notion involving **prefix algorithmic information** instead of **simple algorithmic information** let us introduce the following preliminary notion:

DEFINITION 1.4.2

BUSY BEAVER FUNCTION:

the function $\Sigma : \mathbb{N} \rightarrow \mathbb{N}$:

$$\Sigma(n) \;:=\; \max_{\vec{x} \in \Sigma^{n}} I(\vec{x}) \tag{1.4.1.4}$$

It obeys the following [Cal94]:

Theorem 1.4.1

$$\Sigma(n) \stackrel{\pm}{=} n + I(string(n)) \tag{1.4.1.5}$$

Chaitin's idea was that of defining the random strings of length n to be the strings with maximal prefix entropy among the strings of length n. So, given a natural number m:

DEFINITION 1.4.3

$\vec{x} \in \Sigma^{\star}$ IS CHAITIN m-RANDOM:

$$I(\vec{x}) \geq \Sigma(|\vec{x}|) - m \tag{1.4.1.6}$$

We will denote the set of al the Chaitin m-random binary strings by $CHAITIN-m-RANDOM(\Sigma^{\star}$.

a 0-Chatin random string is often called simply a **Chaitin random**. Following this terminology we will pone:

$$CHAITIN - RANDOM(\Sigma^{\star}) := CHAITIN - 0 - RANDOM(\Sigma^{\star}) \tag{1.4.1.7}$$

Remark 1.4.1

IMPOSSIBILITY OF A SHARP DISTINCTION BETWEEN REGULARITY AND RANDOMNESS FOR STRINGS

It is essential to observe that the introduction of additive constants in both definition1.4.1 and definition1.4.3 solves the problem of the inconsistence of, respectively, definition1.4.1.1 and definition1.4.1.2 only in a partial way: indeed definition1.4.1 and definition1.4.3 continue to depend upon, respectively, the fixed **universal computer** and the fixed **universal Chaitin computer**.

The improvement is that under these ansatzs one doesn't lose algorithmic randomness of strings but passes simply from algorithmic randomness relative to a certain constant to algorithmic randomness relative to a different constant.

But in this way one has to look at the transition from regular to random strings as a continuous, asymptotic one:

indeed the effective connotation of randomness given by the specification that a certain string $\vec{x} \in \Sigma^{\star}$ is m-Chaitin random is the more significative the more high is the difference $|\vec{x}| - m$.

A sharp distinction is possible only for sequences.

In chapter4 we will give a clear, intuitive explanation of this fact in terms of Classical Gambling Theory.

Unfortunately, as we will show in partIII, this point hasn't received the necessary consideration in most the attempts of defining quantum algorithmic randomness, that , erroneously to our opinion, concentrate the analysis to strings of qubits considering this case as simpler and only later, in a derivate mode, pass to analyze sequences of qubit.

We anticipate here that our point of view is opposite: since exactly as in the classical case a sharp distinction between regularity and randomness is possible only for sequences of qubits, the analysis of quantum algorithmic randomness has to start from sequences of qubit.

Let us now observe that there exist many reasons to prefer Chaitin-randomness to Kolmogorov-randomness:

1. the adoption of Chaitin randomness allows to give a clear quantitative foundation to the observation Laplace himself realized almost two centuries ago, namely that the strings not having any kind of regularity, the patternless ones, are the overwhelming majority:

   Theorem 1.4.2

   $$\exists c \in \mathbb{R}_{+} \ : \ cardinality(CHAITIN - RANDOM(\Sigma^{n})) \ > \ 2^{n-c} \ \ \forall n \in \mathbb{N} \tag{1.4.1.8}$$

2. Robert Solovay has proved that Chaitin randomness is stronger than Kolmogorov randomness

3. Chaitin randomness may be easily extended to binary sequences defining, informally speaking, an algorithmic random sequence as one whose prefixes are all Chaitin algorithmic random.

   As we will now show, the **phenomenon of the oscillations of simple algorithmic entropy** avoid this possibility for Kolmogorov randomness.

Let us introduce , first of all, a useful notation.

Given a sequence $\bar{x} \in \Sigma^{\infty}$ let us denote by x_n its n^{th} digit, by $\vec{x}(n)$ its prefix of length n and by $\vec{x}(n,m)$ $(n \leq m)$ the substring of $\bar{x}$ obtained taking its digits from the n^{th} to the m^{th}, namely:

$$\vec{x}(n,m) \ := \ x_n \cdots x_m \ \in \ \Sigma^{m-n} \tag{1.4.1.9}$$

Let us then observe that by identifying the generic string $\vec{x} \in \Sigma^{\infty}$ with the sequence $\vec{x}0^{\infty} \in$ we can look at $\Sigma^{\star}$ as a proper subset of Σ^{∞}.

Let us then introduce the following useful map:

DEFINITION 1.4.4

NUMERIC REPRESENTATION:

$\mathcal{N} : \Sigma^{\infty} \ \mapsto \ [0,1)$:

$$\mathcal{N}(\bar{x}) \ := \ \sum_{n=1}^{\infty} \frac{x_n}{2^n} \tag{1.4.1.10}$$

whose restriction $\mathcal{N}|_{\Sigma^{\infty}-\Sigma^{\star}}$ is a bijection and allows, conseguentially, to identify Σ^{∞} with the set $[0,1)$.

Let us then introduce the probability measure:

DEFINITION 1.4.5

UNBIASED PROBABILITY MEASURE ON Σ^{∞}:
$P_{unbiased} \,:\, 2^{\Sigma^{\infty}} \stackrel{\circ}{\rightarrow} [0,1]$:

$$HALTING(P_{unbiased}) \;=\; \mathcal{F}_{cylinder} \tag{1.4.1.11}$$

$$P_{unbiased}(\Gamma_{\vec{x}}) \;\equiv\; \frac{1}{2^{|\vec{x}|}} \;\; \forall \vec{x} \,\in\, \Sigma^{\star} \tag{1.4.1.12}$$

where:

DEFINITION 1.4.6

CYLINDER SET W.R.T. $\vec{x} \,=(x_1, \ldots ,x_n) \,\in\, \Sigma^{\star}$:

$$\Gamma_{\vec{x}} \;\equiv\; \{\bar{y} = (y_1, y_2, \ldots) \in \Sigma^{\infty} \;:\; y_1 = x_1, \ldots ,y_n = x_n\} \tag{1.4.1.13}$$

DEFINITION 1.4.7

CYLINDER - σ - ALGEBRA ON Σ^{∞}:

$$\mathcal{F}_{cylinder} \;\equiv\; \sigma - \text{algebra generated by} \{\Gamma_{\vec{x}} \,:\, \vec{x} \in \Sigma^{\star}\} \tag{1.4.1.14}$$

In the numeric representation of Σ^{∞} as the real interval $[0,1)$, $P_{unbiased}$ is, clearly, nothing but Lebesgue measure [Leb73].

Denoted by $N_i^n(\bar{x})$ the number of successive $i \in \Sigma$ ending in position n of the sequence $\bar{x}$ the First Borel-Cantelli's Lemma implies that (cfr. the fifth section of the fourth chapter of [Bil95]):

Theorem 1.4.3

$$P_{unbiased}(\{\bar{x} \in \Sigma^{\infty} \;:\; \limsup_{n \to \infty} N_0^n(\bar{x}) \;=\; 1\}) \;=\; 1 \tag{1.4.1.15}$$

$$P_{unbiased}(\{\bar{x} \in \Sigma^{\infty} \;:\; \limsup_{n \to \infty} N_1^n(\bar{x}) \;=\; 1\}) \;=\; 1 \tag{1.4.1.16}$$

Theorem1.4.3 tells us that for $P_{unbiased}$-almost all sequences $\bar{x} \in \Sigma^{\infty}$ there exist infinitely many n for which:

$$\vec{x}(n) \;\stackrel{+}{=}\; \vec{x}(1, n - \log_2 n)0^n \tag{1.4.1.17}$$

i.e.:

$$K(\vec{x}(n)) \stackrel{+}{=} \; n - \log_2 n \tag{1.4.1.18}$$

This suggest that if we adopted the following definition of algorithmic randomness for sequences:

DEFINITION 1.4.8

$\bar{x} \in \Sigma^{\infty}$ IS KOLMOGOROV RANDOM:

$$\exists c \in \mathbb{R}_{+} \ : \ K(\vec{x}(n)) \ > \ n - c \ \ \forall n \in \mathbb{N} \tag{1.4.1.19}$$

there wouldn't exist Kolmogorov random sequences.

That this is indeed the case may be rigorously proved observing that the existence of infinitely many n such that eq.1.4.1.18 holds may be proved to hold for all sequences (not only with $P_{unbiased}$- probability one).

This doesn't happen if we use prefix algorithmic entropy.

DEFINITION 1.4.9

$\bar{x} \in \Sigma^{\infty}$ IS CHAITIN RANDOM:

$$\exists c \in \mathbb{R}_{+} \ : \ I(\vec{x}(n)) \ > \ n - c \ \ \forall n \in \mathbb{N} \tag{1.4.1.20}$$

We will denote the set of all the Chaitin random sequences by $CHAITIN - RANDOM(\Sigma^{\infty})$.

By the numeric representation's map the notion of Chaitin randomness may be immediately extended to reals numbers in the following way:

DEFINITION 1.4.10

$x \in [0\,,\,1)$ IS CHAITIN RANDOM:

$$(\mathcal{N}|_{\Sigma^{\infty} \, - \, \Sigma^{\star}})^{-1}(\Omega) \tag{1.4.1.21}$$

We will denote the set of all the random real numbers by $CHAITIN - RANDOM([0,1))$

As we will prove later, *"almost all"* the numbers in the unitary interval are Chaitin-random.

In particular one has the following:

Theorem 1.4.4

CHAITIN RANDOMNESS OF THE HALTING PROBABILITY:

$$\Omega \ \in \ CHAITIN - RANDOM([0,1)) \tag{1.4.1.22}$$

Supposing now to let the fixed Chaitin universal computer to vary, Theodore A. Slaman has recentely proved the followin remarkable [Sla01]:

Theorem 1.4.5

SLAMAN'S THEOREM:

$$\{\,\Omega_{U}\,,\,:\,U \text{ Chaitin's universal computer } \} \ = \ CHAITIN - RANDOM([0\,,\,1)) \bigcap REC - EN(\mathbb{R}) \tag{1.4.1.23}$$

1.5 Brudno random sequences of cbits

As to the definition of algorithmically random binary sequences we have seen in the previous section that the phenomenon of oscillations of simple algorithmic entropy causes that, denoted by $KOLMOGOROV - RANDOM(\Sigma^{\infty})$ the set of all the Kolmogorov-random binary sequence, one has that:

Theorem 1.5.1

NOT EXISTENCE OF KOLMOGOROV RANDOM SEQUENCES:

$$KOLMOGOROV - RANDOM(\Sigma^{\infty}) \;=\; \emptyset \tag{1.5.1.1}$$

One could , at this point, argue that the existence of infinite islands of regularity in a generic sequence resulting in the logarithmic deficit of simple algorithmic entropy showed by an infinite number of its prefixes is a false problem since what is really relevant is the rate of plain algorithmic entropy for digit of the prefixes, i.e. the ratio $\frac{K(\vec{x}(n))}{n}$ for whose asymptotic behaviour the logarithmic deficits are irrilevant since obviuosly:

$$\lim_{n \rightarrow \infty} \frac{\log_2(n)}{n} \;=\; 0 \tag{1.5.1.2}$$

This way of reasoning led A.A. Brudno to introduce the following notions:

DEFINITION 1.5.1

BRUDNO ALGORITHMIC ENTROPY OF $\bar{x} \in \Sigma^{\infty}$:

$$B(\bar{x}) \;:=\; \lim_{n \rightarrow \infty} \frac{K(\vec{x}(n))}{n} \tag{1.5.1.3}$$

At this point one could think that considering the asympotic rate of prefix entropy instead of simple entropy would result in a different definition of the algorithmic entropy of a sequence.

That this is not the case is the claim of the following:

Theorem 1.5.2

$$B(\bar{x}) \;=\; \lim_{n \rightarrow \infty} \frac{I(\vec{x}(n))}{n} \tag{1.5.1.4}$$

PROOF:

It immediately follows by the fact that [Sta99]:

$$I(\vec{x}(n)) \;-\; K(\vec{x}(n)) \;=\; o(n) \tag{1.5.1.5}$$

■

DEFINITION 1.5.2

$\bar{x} \in \Sigma^{\infty}$ IS BRUDNO RANDOM:

$$B(\bar{x}) \ = \ 1 \tag{1.5.1.6}$$

We will denote the set of all the Brudno random binary sequences by $BRUDNO(\Sigma^{\infty})$.

Anyway one is here faced to a problem almost always misunderstood that is the main source of a sort of incomunicability between the scientific community of mathematical physicists studying Dynamical Systems Theory and the scientific community of the logico-mathematicians and Theoretical-Computer scientists studying Algorithmic Information Theory:

Theorem 1.5.3

BRUDNO RANDOMNESS IS WEAKER THAN CHAITIN RANDOMNESS:

$$BRUDNO - RANDOM(\Sigma^{\infty}) \ \subset \ CHAITIN - RANDOM(\Sigma^{\infty}) \tag{1.5.1.7}$$

Such a theorem was proven by Brudno himself in the last section of [Bru83] by the explicit presentation of a Brudno-random sequence doesn't passing a Martin-Löf test.

We postpone the presentation of such a proof to section2.2 where the involved properties of universal sequential Martin-Löf test are introduced.

1.6 Brudno algorithmic entropy versus the Uspensky abstract approach

In this section we will show that definition1.5.1 is not compatible with Uspensky's abstract approach of defining algorithmic information discussed in section1.2.

Uspensky's abstract approach would, indeed, require the specification of:

1. a **concordance relation** $\mathcal{R}$
2. a **point measure** μ

on Σ^{∞} such to constitute a **metric aggregate** $(\Sigma^{\infty}, \mathcal{R}, \mu)$.

Both these points are highly not-trivial.

Remembering remark1.2.1 we have to keep attention on the meaning of the computability constraint. Indeed, by theorem1.2.1, we see that the definition of the concordance relation $\mathcal{R}$ exit from the boundaries of C_M-Classical Recursion Theory.

As we have anticipated in section1.1, just as to Computability Theory by **physically classical computers** of (partial) functions on sets $S : card(S) = \aleph_1$ many different inequivalent candidate theories have been proposed:

1. the Orthodox Theory generated by the studies of Grzegorczyck - Lacombe [Ric89]
2. the theory developed by the so called Markov School in the framework of Constructive Mathematics [Odi89]
3. the Blum - Shub - Smale 's Theory [Sma92], [S.S98]

The basic notion of the Othodox Theory, namely the definition of a **recursive real number**, seems rather robust:

starting from the C_{Φ}-Computability of the whole $\mathbb{Q}$ the strategy of defining a **recursive real number** consists in effectivizing a method for constructing $\mathbb{R}$ from $\mathbb{Z}$; as shown by R.M. Robinson whichever of these methods one effective:

1. the construction of $\mathbb{R}$ from $\mathbb{Z}$ through Cauchy sequences
2. the construction of $\mathbb{R}$ from $\mathbb{Z}$ through nested intervals
3. the construction of $\mathbb{R}$ from $\mathbb{Z}$ through the Dedekind Cut
4. the construction of $\mathbb{R}$ from $\mathbb{Z}$ through the expansion to base b, where b is an integer > 1.

one results in the the same set $REC(\mathbb{R})$ [Ric89], [PE99].

Let us review the first of these strategies:

given a sequence $\{r_n\}_{n \in \mathbb{N}}$ of rational numbers:

DEFINITION 1.6.1

$\{r_n\}$ IS RECURSIVE:

$$\exists b, c, s \in C_M - C_\Phi - \Delta_0^0 - map(\mathbb{N}, \mathbb{N}) \ : \ r_n \ = \ (-1)^{s(n)} \frac{b(n)}{c(n)} \tag{1.6.1.1}$$

DEFINITION 1.6.2

$\{r_n\}$ CONVERGES EFFECTIVELY TO $x \in \mathbb{R}$:

$$\exists e \in C_M - C_\Phi - \Delta_0^0 - map(\mathbb{N}, \mathbb{N}) \ : \ m \geq e(n) \ \Rightarrow \ |r_m - x| < \frac{1}{2^n} \tag{1.6.1.2}$$

Given a real number $x \in \mathbb{R}$:

DEFINITION 1.6.3

RECURSIVELY ENUMERABLE REAL NUMBERS:

$$REC - EN(\mathbb{R}) \ := \ \{x \in \mathbb{R}) \ : \text{there is a increasing, computable sequence of rationals which converges to x}\} \tag{1.6.1.3}$$

DEFINITION 1.6.4

RECURSIVE REAL NUMBERS:

$$REC(\mathbb{R}) \ := \ \{x \in \mathbb{R}) \ : \text{there is a computable sequence of rationals which converges effectively to x }\} \tag{1.6.1.4}$$

Given a complex number $z \in \mathbb{C}$:

DEFINITION 1.6.5

z IS RECURSIVE:

$$\Re(z) \in REC(\mathbb{R}) \ and \ \Im(z) \in REC(\mathbb{R}) \tag{1.6.1.5}$$

We will denote the set of all the recursive complex numbers by $REC(\mathbb{R})$.
It may be proved that:

Theorem 1.6.1

BASIC PROPERTIES OF $REC(\mathbb{R})$

1. $REC(\mathbb{R})$ is a **closed field**
2. $$cardinality(REC(\mathbb{R})) \ = \ \aleph_0 \tag{1.6.1.6}$$

Obviously this immediately implies that:

Corollary 1.6.1

$$cardinality(REC(\mathbb{C})) \;=\; \aleph_0 \tag{1.6.1.7}$$

To understand in which sense Corollary1.6.1 may be seen highly unsatisfactory and even suggest the necessity of an Eterodox Theory, let us start from the analysis Roger Penrose dedicates to the issue:

Is Mandelbrot's set recursive?

in the seventh section of the fourth chapter of his book [Pen89] and its reformulation by Lenore Blum, Felipe Cucker, Michael Shub and Steve Smale in the first two chapters of their book [S.S98] significatively reporting a picture of Mandelbrot's set on its front cover.

Given a generic complex number $c \in \mathbb{C}$ let us introduce the polynomial $p_c(z) \;:=\; z^2 + c$ and let us denote by $p_c^{(n)}(z)$ its n^{th} iterate.

DEFINITION 1.6.6

MANDELBROT'S SET:

$$\mathcal{M} \;:=\; \mathbb{C} \,-\, \{c \in \mathbb{C} \,:\, \lim_{n \to \infty} p_c^{(n)}(0) = \infty\} \tag{1.6.1.8}$$

A key property of Mandelbrot's set is stated by the following [Fal90]:

Theorem 1.6.2

$\mathcal{M}$ is the halting set of the following algorithm:

Label[start] Input c
$x^2 + c \;\to\; x$
If $|x| \;\leq\; 2$ then Goto start
Output 1
Halt

To answer Penrose's query one needs an algorithm that, given the input $c \in \mathbb{C}$, will decide in a finite number of steps whether or not $c \in \mathcal{M}$.

Penrose appeals to the Orthodox Theory, but immediately refutes it:

"One implication of this is that even with such a simple set as the unit disc $\cdots$ there would be no algorithm for deciding for sure $\cdots$ whether the computable number $x^2 + y^2$ is actually equal to 1 or not, this being the criterion for deciding whether or not the computable complex number $x + iy$ lies on the unit circle $\cdots$ Clearly that is not what we want"

Then he tries to follow other approaches but at the end he concludes that:

"One is left with the strong feeling that the correct viewpoint has not yet been arrived at"

Blum, Cucker, Shub and Smale settle Penrose's question in the framework of their foundation of Computability Theory over a generic ring [Sma92] as a generalization of the Goldstine - Von Neumann axiomatization of Flowchart Theory (cfr. par.1.5 of [Odi89]). Introduced the following notion:

DEFINITION 1.6.7

$S \subset \mathbb{C}$ IS A SEMI-ALGEBRAIC SET:

it is a Boolean combination of sets defined by polynomial equalities and disequalities

Then they prove that a necessary condition for the decidability of a set $S \subset \mathbb{C}$ w.r.t. Computation Theory over the ring $\mathbb{R}$ is that it is the countable union of semi-algebraic sets over $\mathbb{R}$.

That this is not the case for the Mandelbrot's set follows by Shishikura's Theorem stating that the boundary of $\mathcal{M}$ has Hausdorff dimension two, resulting in the following:

Theorem 1.6.3

$\mathcal{M}$ is not Blum, Cucker, Shub and Smale computable

Following Uspensky abstract approach of defining algorithmic information, one would infer from Theorem1.6.3 that $\mathcal{M}$ has infinite algorithmic information, constrasting which what is claimed by another book reporting a picture of (part of) the Mandelbrot's set on its front cover, namely [Tho91], and stating that its information content is essentially zero.

That the applicability of the Uspensky abstract approach to this particular case might be problematic, anyway, results by the obsevation that it doesn't seem to exist some natural **point measure** to use in the the specification of the **metric aggregate** $(\Sigma^{\infty}, \mathcal{R}, \mu)$.

This throws a shadow on the same foundation of $NC_M - C_\Phi$ - Algorithmic Information that is, as has been recentely remarked by Chaitin in the first paragraph of the fourth chapter of [Cha01], mostly an unexplored field.

Chaitin discusses this subject in the usual concretelly LISP programming attitude he followed in his other two Springer books [Cha98], [Cha99], adding to his version of LISP a new primitive function **display** that allow to get the partial outputs of a non-halting computation, and hence considering the algorithmic information of (so produced) infinite sets of S-expressions: in this way he concretely shows that the infinite version of C_Φ - Algorithmic Information Theory differs for the finite version in many respects, an example being the violation of Theorem1.3.2.

1.7 The algorithmic approach to Classical Chaos Theory and Brudno's Theorem

Let us review the basic notions of Classical Ergodic Theory:
given a classical probability space (X, μ):

DEFINITION 1.7.1

ENDOMORPHISM OF (X, μ):
$T : HALTING(\mu) \rightarrow HALTING(\mu)$ surjective :

$$\mu(A) = \mu(T^{-1}A) \;\; \forall A \in HALTING(\mu) \quad (1.7.1.1)$$

DEFINITION 1.7.2

AUTOMORPHISM OF (X, μ):
$T : HALTING(\mu) \rightarrow HALTING(\mu)$ injective endomorphism of (X, μ)

DEFINITION 1.7.3

CLASSICAL DYNAMICAL SYSTEM:
a therne (X, μ, T) such that:

- (X, μ) is a classical probability space
- $T : HALTING(\mu) \rightarrow HALTING(\mu)$ is an endomorphism of (X, μ)

Given a classical dynamical system (X, μ, T):

DEFINITION 1.7.4

(X, μ, T) IS REVERSIBLE:
T is an automorphism

DEFINITION 1.7.5

(X, μ, T) IS ERGODIC:

$$lim_{n \rightarrow \infty} \frac{1}{n} \sum_{k=0}^{n-1} \mu(A \cap T^{k}(B)) = \mu(A)\, \mu(B) \; \forall A, B \in HALTING(\mu) \quad (1.7.1.2)$$

DEFINITION 1.7.6

(X, μ, T) IS MIXING:

$$lim_{n \rightarrow \infty} \mu(A \cap T^{n}(B)) = \mu(A)\, \mu(B) \; \forall A, B \in HALTING(\mu) \quad (1.7.1.3)$$

Example 1.7.1

CLASSICAL SHIFTS

DEFINITION 1.7.7

CLASSICAL SHIFT OVER Σ:
a classical dynamical system $(\Sigma^{\infty} , \sigma , \mu)$ such that:

$$\begin{aligned} \sigma : \Sigma^{\infty} \rightarrow \Sigma^{\infty} \\ (\sigma \bar{x})_{n} \; := \; x_{n+1} \end{aligned} \tag{1.7.1.4}$$

and:

$$HALTING(\mu) \; = \; \mathcal{F}_{cylinder} \tag{1.7.1.5}$$

Remark 1.7.1

CLASSICAL SHIFT IS SYNONIMOUS OF DISCRETE-TIME STATIONARY CLASSICAL STOCHASTIC PROCESS

The notion of a classical shift is nothing but a way of inglobing the Theory of Classical Stationary Stochastic Processes as a sub-discipline of Classical Ergodic Theory.

As we will see in section7.3 an analogous inglobation is possible in a quantum case.

That the notion of a classical shift over Σ is indeed equivalent to the notion of a classical stationary stochastic process over Σ follows immediately by the following two facts:

1. every classical probability measure μ on Σ^{∞} such that $HALTING(\mu) = \mathcal{F}_{cylinder}$ individuates the classical stationary stochastic process over Σ with **occurence probability of strings**:

$$p_{k}(i_{1}, \cdots , i_{k}) \; \equiv \; \mu(\Gamma_{(i_{1}, \cdots , i_{k})}) \;\; i_{1}, \cdots \; i_{k} \; \in \Sigma, k \in \mathbb{N} \tag{1.7.1.6}$$

satisfying the conditions:

$$p_{k}(i_{1} \, , \, \cdots \, i_{k} \,) \; \geq \; 0 \tag{1.7.1.7}$$

$$\sum_{i \in \Sigma} p_{k+1}(i_{1} \, , \, \cdots \, i_{k} \, i) \; = \; p_{k}(i_{1} \, , \, \cdots \, i_{k} \,) \tag{1.7.1.8}$$

$$\sum_{i \in \Sigma} p_{1}(\, i \,) \; = \; 1 \tag{1.7.1.9}$$

2. the collection of functions:

$$p_k(i_1\,,\cdots i_k\,)\;\; i_1\,,\cdots i_k\;\in\Sigma\,,\,k\in\mathbb{N}$$

expressing the **occurence probability of strings** of a classical stationary stochastic process (and, hence, satisfying the constraints eq.1.7.1.7, eq.1.7.1.8, eq.1.7.1.9) individuates the σ-invariant classical probability measure μ on Σ^{∞} such that $HALTING(\mu) \;=\; \mathcal{F}_{cylinder}$ and:

$$p_k(i_1,\cdots,i_k) \;=\; \mu(\Gamma_{(i_1,\cdots,i_k)})\;\; i_1,\cdots\; i_k\;\in\Sigma,k\in\mathbb{N} \tag{1.7.1.10}$$

Let us introduce some useful notion:

DEFINITION 1.7.8

STOCHASTIC VECTOR OVER Σ:
$\vec{P} \;=\; \begin{pmatrix} p_0 \\ p_1 \end{pmatrix}$ such that:

$$p_i \geq 0\;\; i=0,1 \tag{1.7.1.11}$$

$$\sum_{i\in\Sigma} p_i \;=\; 1 \tag{1.7.1.12}$$

i.e. a column vector specifying a probability distribution over Σ.

DEFINITION 1.7.9

STOCHASTIC MATRIX OVER Σ:
$2\,\times\,2$ matrix:
$\hat{P} = \begin{pmatrix} p_{0,0} & p_{0,1} \\ p_{1,0} & p_{1,1} \end{pmatrix}$ such that:

$$p_{i,j} \geq 0\;\; i,j=0,1 \tag{1.7.1.13}$$

$$\sum_{j\in\Sigma} p_{i,j} \;=\; 1\;\; i=0,1 \tag{1.7.1.14}$$

We can now introduce some basic classical shift:

DEFINITION 1.7.10

CLASSICAL BERNOULLI SHIFT OVER Σ W.R.T. THE STOCHASTIC VECTOR $\vec{P} \;=\; \begin{pmatrix} p_0 \\ p_1 \end{pmatrix}$:
the classical shift over Σ with measure μ :

$$p_k(\,i_1\,,\cdots\,i_k\,) \;=\; \prod_{l=1}^{k} p(\,i_l\,)\;\;\forall k\in\mathbb{N} \tag{1.7.1.15}$$

Given a stochastic vector $\vec{e} \ := \begin{pmatrix} e_0 \\ e_1 \end{pmatrix}$ and a stochastic matrix $\hat{P} \ := \begin{pmatrix} p_{00} & p_{01} \\ p_{10} & p_{11} \end{pmatrix}$ such that:

$$(\vec{P})^T \hat{P} \ = \ \hat{P} \tag{1.7.1.16}$$

DEFINITION 1.7.11

CLASSICAL MARKOV SHIFT OVER Σ W.R.T. THE STOCHASTIC VECTOR $\vec{e}$ AND THE STOCHASTIC MATRIX $\hat{P}$

the classical shift over Σ with measure μ :

$$p_k(i_1 \, , \cdots i_k) \ = \ e_{i_1} \, p_{i_1,i_2} \cdots p_{i_{k-1},i_k} \tag{1.7.1.17}$$

Remark 1.7.2

CLASSICAL SHIFT IS SYNONIMOUS OF STATIONARY CLASSICAL INFORMATION SOURCE

We have seen in remark1.7.1 that the notion of classical shift over Σ is equivalent to the notion of a stationary classical stochastic process over Σ.

But a classical stochastic process $\{x_n\}$ may be equivalentely seen as a classical information source, considering the random variable x_n as the letter trasmitted at time n by a sender (Alice) to a receiver (Bob) through a proper communicational channel.

The resulting equivalence between the notion of a classical shift and the notion of a stationary classical information source persists at the quantum level as we will see in the section6.7

Given a classical probability space $(X \, , \mu)$:

DEFINITION 1.7.12

FINITE MEASURABLE PARTITION OF $(X \, , \, \mu)$:

$$\begin{aligned} & A \ = \ \{ A_1 \, , \cdots A_n \} \ n \in \mathbb{N} \ : \\ & A_i \in HALTING(\mu) \ \ i \ = \ 1 \, , \cdots n \\ & A_i \cap A_j \ = \ \emptyset \ \forall i \neq j \\ & \mu(X \ - \ \cup_{i=1}^{n} A_i \,) \ = \ 0 \end{aligned} \tag{1.7.1.18}$$

We will denote the set of all the finite measurable partitions of $(X \, , \, \mu)$ by $\mathcal{P}(X \, , \, \mu \,)$.

DEFINITION 1.7.13

$A \in \mathcal{P}(X, \mu)$ IS FINER THAN $B \in \mathcal{P}(X, \mu)$:

every atom of B is the union of atoms by A

DEFINITION 1.7.14

COARSEST REFINEMENT OF $A = \{A_i\}_{i=1}^{n}$ AND $B = \{B_j\}_{j=1}^{m} \in \mathcal{P}(X , \mu)$:

$$\begin{aligned} & A \vee B \ \in \mathcal{P}(X,\mu) \\ & A \vee B \ \equiv \ \{ A_i \cap B_j \ i = 1, \cdots , n \ j = 1, \cdots , m\} \end{aligned} \tag{1.7.1.19}$$

Clearly $\mathcal{P}(X,\mu)$ is closed both under coarsest refinements and under endomorphisms of (X,μ).

Remark 1.7.3

COARSE-GRAINED MEASUREMENTS ON A CLASSICAL PROBABILITY SPACE: THE OPERATIONAL MEANING OF A CLASSICAL PARTITION

Beside its abstract, mathematical formalization, the definition 1.7.12 has a precise operational meaning.

Given the classical probability space (X,μ) let us suppose to make an experiment on the probabilistic universe it describes using an instrument whose resolutive power is limited in that it is not able to distinguigh events belonging to the same atom of a partition $A = \{A_i\}_{i=1}^{n} \in \mathcal{P}(X,\mu)$.

Conseguentially the outcome of such an experiment will be a number

$$r \in \{1, \cdots , n\} \tag{1.7.1.20}$$

specifying the observed atom A_r in our coarse-grained observation of (X,μ).

We will call such an experiment an **operational observation of** (X,μ) **through the partition A**.

Considered another partition $B = \{B_j\}_{i=1}^{n} \in \mathcal{P}(X,\mu)$ we have obviously that the operational observation of (X,μ) through the partition $A \vee B$ is the conjuction of the two experiments consisting in the operational observations of (X,μ) through the partitions, respectively, A and B.

Conseguentially we may consistentely call an **operational observation of** (X,μ) **through the partition A** more simply an **A experiment**.

Remark 1.7.4

THE DOUBLE MEANING OF THE CLASSICAL PROBABILISTIC SHANNON ENTROPY OF AN EXPERIMENT

The experimental outcome of an operational observation of (X,μ) through the partition $A = \{A_i\}_{i=1}^{n} \in \mathcal{P}(X,\mu)$ is a classical random variable having as distribution the stochastic vector ($\begin{pmatrix} \mu(A_1) \\ \vdots \\ \mu(A_n) \end{pmatrix}$ whose Shannon entropy we will call the entropy of the partition A, according to the following:

DEFINITION 1.7.15

ENTROPY OF $A = \{A_i\}_{i=1}^{n} \in \mathcal{P}(X, \mu)$:

$$H(A) \equiv H(\begin{pmatrix} \mu(A_1) \\ \vdots \\ \mu(A_n) \end{pmatrix}) \tag{1.7.1.21}$$

with the right hand side expressed in terms of the definition1.3.7 we introduced in section1.3.

It is fundamental, at this point, to observe that, given an experiment, one has to distinguish between two conceptually different concepts:

1. the **uncertainty of the experiment**, i.e. the amount of uncertainty on the outcome of the experiment before of realizing it
2. the **information of the experiment**, i.e. amount of information gained by the outcome of the experiment

The fact that in Classical Probabilistic Information Theory both these concepts are quantified by the Shannon entropy of the experiment is a conseguence of the following (cfr. pag. 62 of [Bil65]):

Theorem 1.7.1

THE SOUL OF CLASSICAL INFORMATION THEORY

$$\text{information gained} \; = \; \text{uncertainty removed} \tag{1.7.1.22}$$

Theorem1.7.1 applies, in particular, as to the partition-experiments we are discussing.

Let us now consider a classical dynamical system $CDS := (X, \mu, T)$.

The T-invariance of μ implies the the partitions $A = \{A_i\}_{i=1}^{n} \in \mathcal{P}(X, \mu)$ and $T^{-1}A$ have equal probabilistic structure. Conseguentially the **A experiment** and the $T^{-1}A$**-experiment** are repliques , **not necessarily independent**, of the same experiment , made at succesive times.

In the same way the $\vee_{k=0}^{n-1} T^{-k}A$**-experiment** is the compound experiment consisting in n replications $A, T^{-1}A, , \cdots, T^{-(n-1)}A$ of the experiment corresponding to $A \in \mathcal{P}(X, \mu)$.

The amount of classical information per replication we obtain in this compound experiment is clearly:

$$\frac{1}{n} H(\vee_{k=0}^{n-1} T^{-k}A)$$

It may be proved (cfr. e.g. the second paragraph of the third chapter of [Sin00]) that when n grows this amount of classical information acquired for replication converges, so that the following quantity:

$$h(A, T) \; \equiv \; lim_{n \to \infty} \frac{1}{n} H(\vee_{k=0}^{n-1} T^{-k}A) \tag{1.7.1.23}$$

does exist.

In different words, we can say that $h(A,T)$ gives the asymptotic rate of production of classical information for replication of the A-experiment.

DEFINITION 1.7.16

$$h_{CDS} \equiv sup_{A \in \mathcal{P}(X,\mu)} h(A,T) \tag{1.7.1.24}$$

By definition we have clearly that:

$$h_{CDS} \geq 0 \tag{1.7.1.25}$$

DEFINITION 1.7.17

CDS IS CHAOTIC:

$$h_{CDS} > 0 \tag{1.7.1.26}$$

Remark 1.7.5

INFORMATION-THEORETIC NATURE OF THE CONCEPT OF CLASSICAL CHAOS

Definition1.7.17 shows explicitly that the concept of classical-chaos is an information-theoretic one:

a classical dynamical system is chaotic if there exist at least one experiment on the system that, no matter how many times we insist on repeating it, continue to give us classical information.

That such a meaning of classical chaoticity is equivalent to the more popular one as the sensible (i.e. exponential) dependence of dynamics from the initial conditions (the so called **butterfly effect** for which the little perturbation of the atmospheric flow produced here by a butterfly's flight may produce an hurricane in Alaska) is a conseguence of Pesin's Theorem stating (under mild assumptions) the equality of the Kolmogorov-Sinai entropy and the sum of the positive Lyapunov exponents.

This inter-relation may be caught observing that:

- if the system is chaotic we know that there exist an experiment whose repetition definitely continues to give information: such an information may be seen as the information on the initial condition that is necessary to furnish more and more with time if one want to keep the error on the prediction of the phase-point below a certain bound
- if the system is not chaotic the repetition of every experiment is useful only a finite number of times, after which every suppletive repetition doesn't furnish further information

Let us now consider the issue of symbolically translating the coarse-gained dynamics:

the traditional way of proceeding is that described in the second section of [Yak81]:

given a positive integer $n \in \mathbb{N}$ let us introduce the:

DEFINITION 1.7.18

n-LETTERS ALPHABET:

$$\Sigma_n := \{0, \cdots, n-1\} \tag{1.7.1.27}$$

Clearly:

$$\Sigma_2 = \Sigma \tag{1.7.1.28}$$

Considered a partition $A = \{A_i\}_{i=1}^{n} \in \mathcal{P}(X, \mu)$

DEFINITION 1.7.19

SYMBOLIC TRANSLATOR OF CDS W.R.T. A:

$\psi_A : X \to \Sigma_n$:

$$\psi_A(x) \equiv j : x \in A_j \tag{1.7.1.29}$$

In this way one associate to each point of X the letter, in the alphabet having as many letters as the number of atoms of the considered partition, labelling the atom to which the point belongs.

Concatenating the letters corresponding to the phase-point at different times one can then codify $k \in \mathbb{N}$ steps of the dynamics:

DEFINITION 1.7.20

k-POINT SYMBOLIC TRANSLATOR OF CDS W.R.T. A:

$\psi_A^{(k)} : X \to \Sigma_n^k$:

$$\psi_A^{(k)}(x) \equiv \cdot_{j=1}^{n} \psi(T^j x) \tag{1.7.1.30}$$

and whole orbits:

DEFINITION 1.7.21

$\psi_A^{(\infty)} : X \to \Sigma_n^{\infty}$:

$$\psi_A^{(\infty)}(x) \equiv \cdot_{j=1}^{\infty} \psi(T^j x) \tag{1.7.1.31}$$

The bug of this strategy of symbolic translation is the dependence of the used alphabet from the cardinality of the partition:

$$cardinality(A) \neq cardinality(B) \Rightarrow$$
$$Range[\psi_A(x)] \neq Range[\psi_B(x)] \;\; \forall x \in A \, , \forall A, B \in \mathcal{P}(X \, , \mu) \tag{1.7.1.32}$$

We will therefore adopt a different strategy of symbolic-coding using only the binary alphabet Σ based on the following:

DEFINITION 1.7.22

UNIVERSAL SYMBOLIC TRANSLATOR OF CDS:
$\Psi \, : \, X \, \times \, \mathcal{P}(\, X \, , \, \mu) \rightarrow \Sigma^{\star}$:

$$\Psi(x \, , \, \{A_i\}_{i=1}^{n}) \; \equiv \; string(j) \; \; , x \, \in \, A_j \tag{1.7.1.33}$$

that can be again used to codify $k \in \mathbb{N}$ steps of the dynamics:

DEFINITION 1.7.23

k-POINT UNIVERSAL SYMBOLIC TRANSLATOR OF CDS:
$\Psi^{(k)} \, : \, X \, \times \, \mathcal{P}(\, X \, , \, \mu) \rightarrow \Sigma^{\star}$:

$$\Psi^{(k)}(x \, , \, \{A_i\}_{i=1}^{n}) \; \equiv \; \cdot_{j=1}^{k} \psi(T^j x \, , \, \{A_i\}_{i=1}^{n}) \tag{1.7.1.34}$$

and whole orbits:

DEFINITION 1.7.24

ORBIT UNIVERSAL SYMBOLIC TRANSLATOR OF CDS:
$\Psi^{(\infty)} \, : \, X \, \times \, \mathcal{P}(\, X \, , \, \mu) \rightarrow \Sigma^{\infty}$:

$$\Psi^{(\infty)}(x \, , \, \{A_i\}_{i=1}^{n}) \; \equiv \; \cdot_{j=1}^{\infty} \psi(T^j x \, , \, \{A_i\}_{i=1}^{n}) \tag{1.7.1.35}$$

The asymptotic rate of of production of simple algorithmic entropy of the binary sequence obtained translating symbolically the orbit generated by $xinX$ through the partition $A \, \in \, \mathcal{P}(\, X \, , \, \mu)$ is clearly given by:

$$B(A,x) \; := \; B(\Psi^{(\infty)}(x,A)) \tag{1.7.1.36}$$

We saw in definition1.7.16 that the Kolmogorov-Sinai entropy was defined as $K(A,x)$ calculated on the more probabilistically-informative A-experiment; in the same way the Brudno algorithmic entropy of x is defined calculating $B(A,x)$ on the more algorithmically-informative A-experiment:

DEFINITION 1.7.25

$$B_{CDS}(x) \; \equiv \; sup_{A \in \mathcal{P}(X,\mu)} \, B(A,x) \tag{1.7.1.37}$$

We can now introduce the fundamental:

Theorem 1.7.2

BRUDNO'S THEOREM

$$h_{CDS} \; = \; B_{CDS}(x) \; \forall - \mu - a.e. \, x \in X \tag{1.7.1.38}$$

PROOF:

Conceptually if follows from Theorem1.3.7 and Theorem1.5.2.

Given it for granted, the complete proof given in [Bru83] adopting the traditional strategy of symbolic translation, let us observe that the passage to our strategy of symbolic translation simply involves the application of the quasi-lexicographic map whose bijectivity guarantees the equivalence ■

Let us now consider the **algorithmic approach to Classical Chaos Theory** strongly supported by Joseph Ford, whose objective is the characterization of the concept of chaoticity of a classical dynamical system as the algorithmic-randomness of its symbolically-translated trajectories.

To require such a condition for all the trajectories would be too restrictive since it is reasonable to allow a chaotic dynamical system to have a numerable number of periodic orbits.

Let us introduce then following two notions:

DEFINITION 1.7.26

CDS IS STRONGLY ALGORITHMICALLY-CHAOTIC:

$$\forall - \mu - a.e. x \in X \, , \, \exists A \in \mathcal{P}(X, \mu) \, : \, \Psi^{(\infty)}(x \, , \, A) \in CHAITIN - RANDOM(\Sigma^{\infty}) \tag{1.7.1.39}$$

DEFINITION 1.7.27

CDS IS WEAK ALGORITHMICALLY-CHAOTIC:

$$\forall - \mu - a.e. x \in X \, , \, \exists A \in \mathcal{P}(X, \mu) \, : \, \Psi^{(\infty)}(x \, , \, A) \in BRUDNO - RANDOM(\Sigma^{\infty}) \tag{1.7.1.40}$$

The difference between definition1.7.26 and definition1.7.27 follows by Theorem1.5.3.

Clearly Theorem1.7.2 implies the following:

Corollary 1.7.1

$$\begin{aligned} CHAOTICITY &= \text{WEAK ALGORITHMIC CHAOTICITY} \\ CHAOTICITY &< \text{STRONG ALGORITHMIC CHAOTICITY} \end{aligned}$$

that shows that the algorithmic approach to Classical Chaos Theory is equivalent to the usual one only in weak sense.

Chapter 2

Classical algorithmic randomness as passage of all the classical algorithmic statistical tests

2.1 Pseudorandom generators

We have seen in chapter1 how the notion of classical algorithmic randomness as classical algorithmic incompressibility may be properly formalized.

The deepest way of introducing the characterization of classical algorithmic randomness as passage of a certain battery of statistical tests is to analyze the issue of **random number generation**.

Such an expression is an oxymoron: the same fact that there exist an algorithm by which we generate an object on a classical deterministic computer means that such an object is algorithmically-compressible trough the adopted algorithm and, hence, is not algorithmically-random.

This observation was condensed by John Von Neumann in his famous sentence:

"Anyone who considers arithmetic methods of producing random digits is, of course, in a state of sin"

What a pseudorandom number generator (a PRG from here and beyond) outputs are **pseudorandom numbers**, i.e. numbers who mimic true algorithmic randomness up to a certain degree of accuracy, i.e pass a suffiencetely extended battery of randomness tests.

Before embarking in abstract mathematical definitions about what does it mean it is rather useful to make a previous breaf historical analysis of the concrete problem of pseudo-random number generation in Theoretical Computer Science.

Von Neumann himself introduced an arithmetic pseudorandom-generation method known as the **middle square method**:

supponing to want to generate m random integers of 10 digits starting from a certain 10' digits integer **seed** , such method is defined through the following algorithm:

1. set $i \leftarrow 0$
2. set $n_i \leftarrow seed$
3. square n_i to get an intermediate number M with 20 or less digits
4. set $i \leftarrow i + 1$
5. set $n_i \leftarrow$ the middle ten digits of M
6. if $i < m$ then goto step3, else halt

A serious problem with the middle-square method is that the orbit generated by many seeds is periodic with a very little period [Yan00].

In 1949 D.H. Lehmer proposed to use the **Theory of congruences**, i.e. the theory of the residue classes $\mathbb{Z}_n$ modulo n (a ring on integers being a field if and only if n is a prime number) to generate pseudorandom numbers.

Fixed the following numbers:

- n : the **modulus** , $n > 0$
- x_0 : the **seed**, $0 \leq x_0 \leq n$
- a : the **multiplier** $0 \leq a \leq n$
- b : the **increment** $0 \leq b \leq n$

the **linear congruential generator** generates the sequence of pseudorandom numbers defined recursively by:

$$x_j := ax_{j-1} + b \,(mod\, n)\, j > 0 \tag{2.1.2.1}$$

for $1 \leq j \leq l$ where $l \in \mathbb{N}$ is the least value such that $x_{l+1} \equiv x_j \,(mod\, n)$ i.e. is the **period** of the PRG.

Since the period is less or equal to the modulus $l \leq n$ to have a PRG of sufficient quality it is necessary to use high enough moduli.

For fixed n one would, then like to optimize the situation choosing the other parameters so that the period is equal to the modulus.

A necessary and sufficient condition for this to happen is given by the following [Knu98]:

Theorem 2.1.1

THEOREM OF GREENBERGER, HULL, DOBELL

$$l = n \Leftrightarrow (gcd(b,n) = 1\, and\, a \equiv 1 (mod\, p) \forall primes\, p|n,\, and\, a \equiv 1 (mod\, 4)\, if\, 4|n) \tag{2.1.2.2}$$

The **linear congruential generator** had (and continues to have) an immense application:

for example RANDU, the random number generator common on IBM mainframes computers in the sixties, was based on a linear congruential generator with parameters $a = 65539$, $b = 0$, $n = 2^{31}$.

However it was soon found that RANDU gave rise to insidious correlations: if successive triples of the numbers that RANDU generated were used as a set of coordinates in a three-dimensional space, the generated distribution of point seems random from most viewpoints but there exist a special orientation from wich one can see that they lie in a set of planes [Cle98].

The linear congruential method is still of great popularity: for example it is often used the **minimal standard 32-bit generator** obtained by the choice $a = 16807$, $b = 0$, $n = 2^{31} - 1$ adopted by many programming languages such as TURBO PASCAL even if its lack of randomness may be easily visualized [Woy98].

To avoid the bugs of linear congruential generators, a new kind of generators, the **shift-register-generator**, was then introduced.

In these generators each successive number depends upon many preceding values.

The basic operation may still be the **modular addition** or other functions such as the **exlusive or**.

For example a commonly used algorithm is the following:

$$x_j \; := \; x_{j-p}\, XOR\, x_{j-q} \tag{2.1.2.3}$$

The best choice of the pair of integers p and q happens when p and q are **Mersenne primes** such that [Bin00] :

$$p^2 + q^2 + 1 \text{ is prime} \tag{2.1.2.4}$$

A common choice of this kind is $p = 250$, $q = 103$.

Anyway it would be an error to think that this method (or their evolutions such as the **subtract with carry generators** or the **subtract with carry Weyl generators**) is, in absolute, better than the linear congruential method: there exist Monte-carlo simulations of the bidimensional Ising model for which the minimal standard 32-bit generator is not inficiated by systematic errors of younger algorithms producing deviations from Onsager's known solution.

Let us conclude this hystorical review mentioning Wolfram's suggestion of using some TYPE 3 elementary cellular automata as pseudo-random generators [Wol94] that he himself adopted for the integer-random number generator of

Mathematica (Rule[30] while for real numbers it is used a Marsaglia-Zaman subtract with borrow [Wol96]).

This panoramic on concrete pseudorandom number generators, hasn't, anyway, touched the basis question: what is a **pseudorandom generator**?

The answer that we have already anticipated, i.e. an algorithm producing binary strings passing an enough number of **randomness statistical tests**, may appear satisfying since anyone, eventually from his undergraduate χ^2 - test experiences, has an intuitive idea of what a randomness statistical test is: a well-defined procedure that allows to catch some kind of regularity of the statistical data.

For all practical purposes the definition of the notion of pseudo-random generator may indeed be accomplished concretely specifying a set of randomness statistical tests it has to pass: (e.g. the Kolmogorov-Smirnov test + the Frequency test + the Serial test + the Gap test + the Partition test + the Coupon collector's test + the Permutation test + the Run test + the Maximum-of t-test + the Collision test + the Birthday spacing test + Serial correlation test [Knu98]).

The higher is the number of elements of this list of randomness statistical tests, the higher is the quality of the generator.

From a conceptual point of view, anyway, such a definition is unsatisfactory since:

- it ultimately doesn't say what a **statistical randomness test** is
- it doesn't clarify the structure of the set of the **statistical randomness tests** and, conseguentially, the meaning of considering a subset of it.

A satisfactory answer to both these points may be given introducing Per Martin - Löf's Theory of Randomness Statistical tests.

The idea behind Martin - Löf's Theory is the following:

in statistical practice we are given an element x of some sample space (associated with some distribution that we will assume from here and beyond to be the unbiased one) and we want to test the hypothesis: **x is a typical outcome**.

Being **typical** means *"belonging to every reasonable majority"*.

An element will be **random** just in the case it lies in the intersections of all such majorities.

A level of a statistical test is a set of strings which are found to be relatively not-random (by the test).

Each level is a subset of the previous level, containing less and less strings, considered more and more not-random.

the number of strings decreases exponentially fast at each level.

So a test contains at level 0 all possible strings, at level 2 at most $\frac{1}{2}$ of the strings, at level three only $\frac{1}{4}$ of all strings and so on; accordingly at level m the test contains at most 2^{n-m} strings of length n.

DEFINITION 2.1.1

A recursively enumerable (r.e.) set $V \subset \Sigma^{\star} \times \mathbb{N}_{+}$ is a **Martin - Löf test** if:

1.

$$V_{m+1} \subset V_m \ \ \forall m \geq 1 \tag{2.1.2.5}$$

where:

$$V_m := \{\vec{x} \in \Sigma^{\star} : (\vec{x}, m) \in V\} \tag{2.1.2.6}$$

is called the **critical region of the test at level** $\frac{1}{2^m}$

2.

$$cardinality(\Sigma^n \cap V_m) < 2^{n-m} \ \ \forall n \geq m \geq 1 \tag{2.1.2.7}$$

Given a Martin - Löf test V and an integer number q:

DEFINITION 2.1.2

SET OF THE q-PSEUDORANDOM STRINGS FOR V:

$$q - PSEUDORANDOM(\Sigma^{\star}; V) := \{\vec{x} \in \Sigma^{\star} : \vec{x} \notin V_q \, and \, q < |\vec{x}|\} \tag{2.1.2.8}$$

Given a Martin - Löf test U:

DEFINITION 2.1.3

U IS UNIVERSAL:
for every Martin - Löf test V there exist a constant c (depending upon U and V) such that:

$$V_{m+c} \subset U_m \ \ m = 1, 2, \cdots \tag{2.1.2.9}$$

A universal Martin - Löf statistical test is a Martin - Löf statistical test that is as strong as any other Martin-Martin - Löf test.
So it is reasonable to fix once and for all a universal Martin - Löf test U and, given an integer number q, define:

DEFINITION 2.1.4

SET OF THE MARTIN LÖF - q - RANDOM STRINGS:

$$MARTINLÖF - q - RANDOM(\Sigma^{\star}) := q - PSEUDORANDOM(\Sigma^{\star}; U) \tag{2.1.2.10}$$

We can then introduce the following basic notion:

DEFINITION 2.1.5

MARTIN LÖF PRG OF QUALITY $q \in \mathbb{N}$:
a PRG whose outputs belongs to $MARTINLÖF - q - RANDOM(\Sigma^{\star})$

It must be remarked, any way, that this is not the only possible way one can follow in order of formalizing the concept of a PRG.

For example, following Oded Goldreich [Gol01], one can found the Theory of Pseudorandom Generation on Structural Complexity Theory [Odi99a] defining a PRG as an **efficient** algorithm that stretches short random strings into longer strings that are computationally indistinguishable from long random strings, in the sense that the difference can't be certified in an **efficient** way.

Let us shortly show how this can be formalized.

Adhering to Goldreich's terminology we will speak of **Classical Turing machines** instead of **partial recursive functions** remembering that by the **Church-Turing's Thesis** that is exactly the same.

Given a Turing machine M:

DEFINITION 2.1.6

M IS POLYNOMIAL-TIME:
there exist a polynomial p such that for every $\vec{x} \in \Sigma^{\star}$, when invoked on input x, M halts after at most $p(|\vec{x}|)$ steps

We will will consider the following particular kind of sequence of probability distributions:

DEFINITION 2.1.7

PROBABILITY ENSEMBLE OVER $\Sigma^{\star}$:
a sequence $\{P_n\}_{n \in \mathbb{N}}$ of probability distributions over $\Sigma^{\star}$ with the property that there exist a polynomial p such that:

$$P_n(\vec{x}) > 0 \Rightarrow |\vec{x}| = p(n) \tag{2.1.2.11}$$

Given two probability ensembles $\{P_n\}_{n \in \mathbb{N}}$ and $\{Q_n\}_{n \in \mathbb{N}}$:

DEFINITION 2.1.8

$\{P_n\}_{n \in \mathbb{N}}$ AND $\{Q_n\}_{n \in \mathbb{N}}$ ARE COMPUTATIONAL INDISTINGUISHABLE:
for every probabilistic polynomial-time Turing machine M, for every positive polynomial $p(\cdot)$ and for all sufficentely large n:

$$|Pr[M(1^n, P_n) = 1] - Pr[M(1^n, Q_n) = 1]| < \frac{1}{p(n)} \tag{2.1.2.12}$$

DEFINITION 2.1.9

GOLDREICH PRG:
a polynomial-time Turing machine G such that there exist a monotonically increasing function $l : \mathbb{N} \rightarrow \mathbb{N}$ such that the following two probability ensembles, denoted by $\{G_n\}_{n \in \mathbb{N}}$ and $\{R_n\}_{n \in \mathbb{N}}$, are computationally indistinguishable:

- G_n is defined as the output of G on a uniformely-selected n-bits string
- R_n is defined as the uniform probability distribution on $\Sigma^{l(n)}$

The link between definition2.1.9 and Structural Complexity Theory passes through **one-way functions**, i.e. functions easy to compute but hard to invert:

DEFINITION 2.1.10

ONE-WAY FUNCTION:
a function $f : \Sigma^{\star} \rightarrow \Sigma^{\star}$:

- easy to compute: f is computable in polynomial time
- hard to invert: for every probabilistic polynomial-time Turing machine M, for every positive polynomial $p(\cdot)$ and for all sufficentely large n and $\vec{x}$ uniformely distributed over Σ^{n}

$$Pr[M(1^{n}, f(\vec{x})) \in f^{-1}(f(\vec{x})) = 1] \; < \; \frac{1}{p(n)} \tag{2.1.2.13}$$

And here appears the following:

Conjecture 2.1.1

FUNDAMENTAL CONJECTURE OF STRUCTURAL COMPLEXITY THEORY:

$$P \neq NP \tag{2.1.2.14}$$

governing the following:

Theorem 2.1.2

$$\exists G \text{ Goldreich PRG } \; \Leftrightarrow \; \exists f \text{ one-way function } \; \Rightarrow \; \text{Conjecture2.1.1 holds} \tag{2.1.2.15}$$

The inter-relation between definition2.1.5 and definition2.1.9 has not been analyzed yet.

Ultimately it touches the issue of the link existing between Structural Complexity Theory and Algorithmic Information Theory that, though having been the subject of intensive investigation since the pioneristic Levin's analysis of the inter-relation among **perebor** (a russian term literally meaning *"brute force"* and adopted from the late fifthies by the sovietic operations research community to denote the necessity of an exhaustive search of all the alternatives in certain search problems) and Kolmogororov's ideas (cfr. the sixth paragraph of the second part of [Laz98], the 7^{th} chapter of), is still uncertain (cfr. [Lon92], the 7^{th} chapter of [Vit97] and the 10^{th} chapter of [Gab90])

2.2 Equivalence between passage of a Martin Löf universal sequential statistical test and Chaitin randomness

In the last paragraph we have introduced the notion of a Martin-Löf test on strings only for the uniform distribution, the only one necessary in order to define a PRG.

Since, anyway, we will front, in the next sections, also not-uniform distributions it may be appropriate to give a more general definition.

Given a recursive probability distribution P on $\Sigma^{\star}$:

DEFINITION 2.2.1

MARTIN LÖF TEST OF P-RANDOMNESS (P-TEST) :

a function $\delta : \Sigma^{\star} \rightarrow \mathbb{N}$:

1. the set $V := \{(m, \vec{x}) : \delta(\vec{x}) > m\}$ is recursively enumerable
2. $$\sum_{\vec{x} \in \Sigma^{n}} \{P(\vec{x}||\vec{x}| = n : \delta(\vec{x}) \geq m\} \leq \frac{1}{2^{m}} \quad \forall n \qquad (2.2.2.1)$$

Defined the **critical region of the test at level $\frac{1}{2^{m}}$**, for any integer $m \geq 1$, as:

$$V_{m} := \{\vec{x} \in \Sigma^{\star} : \delta(\vec{x}) \geq m\} \qquad (2.2.2.2)$$

it is immediate to see that for $P = P_{unbiased}$ the definition2.2.1 reduces to the definition2.1.1.

We would like, now, to extend this definition from $\Sigma^{\star}$ to Σ^{∞}.

Since an effective test can't be performed on an infinite sequence it is necessary to introduce an effective process of sequential approximations.

So, given a recursive probability measure μ on Σ^{∞}:

DEFINITION 2.2.2

SEQUENTIAL MARTIN LÖF TEST OF μ-RANDOMNESS (SEQUENTIAL μ-TEST) :

a function $\delta : \Sigma^{\infty} \rightarrow \mathbb{N} \bigcup \{\infty\}$:

1. $$\delta(\bar{x}) = \sup_{n \in \mathbb{N}} \{\gamma(\vec{x}(n))\} \qquad (2.2.2.3)$$

   where $\vec{x}(n) \in \Sigma^{n}$ denotes the prefix of length n of the sequence $\bar{x}$ while $\gamma : \Sigma^{\star} \rightarrow \mathbb{N}$ is a **total enumerable function** (i.e. $V := \{(m, \vec{y}) : \gamma(\vec{y}) \geq m\}$ is a **recursively enumerable set**

2.

$$\mu(\{\bar{x} \in \Sigma^{\infty} : \delta(\bar{x}) \geq m\} \leq \frac{1}{2^m} \ \forall m \geq 0 \tag{2.2.2.4}$$

Given a **sequential μ-test** δ we have that a sequence $\bar{x} \in \Sigma^{\infty}$ passes the test if $\delta(\bar{x}) < \infty$ while it doesn't passes the test if $\delta(\bar{x}) = \infty$.

The set of the sequences passing the test δ are those that it declares random:

DEFINITION 2.2.3

SET OF THE μ-RANDOM SEQUENCES W.R.T. δ:

$$\mu - RANDOM(\Sigma^{\infty}; \delta) := \{\bar{x} \in \Sigma^{\infty} : \delta(\bar{x}) < \infty\} \tag{2.2.2.5}$$

Clearly the definition2.2.3 depends on the particular sequential μ-test considered.

This relativization can be, anyway, eliminated by the usual strategy of Algorithmic Information Theory:

DEFINITION 2.2.4

UNIVERSAL SEQUENTIAL MARTIN LÖF TEST OF μ-RANDOMNESS (UNIVERSAL SEQUENTIAL μ-TEST) :

a sequential μ -test f such that for every other sequential μ -test δ there exist a constant $c \geq 0$ such that:

$$f(\bar{x}) \geq \delta(\bar{x}) - c \tag{2.2.2.6}$$

A universal sequential μ-test is a sequential μ-test that is as strong as any other sequential μ-test.

So it is reasonable to fix once and for all a universal sequential μ-test $\delta_0(\cdot|\mu)$ and define:

DEFINITION 2.2.5

SET OF THE μ-RANDOM SEQUENCES:

$$\mu - RANDOM(\Sigma^{\infty}) := \mu - RANDOM(\Sigma^{\infty}; \delta_0(\cdot|\mu)) \tag{2.2.2.7}$$

To be a μ-random sequence is the μ-rule in Σ^{∞} since:

Theorem 2.2.1

FOUNDATION OF THE APPLICABILITY OF PROBABILITY THEORY TO REALITY

$$\mu[\mu - RANDOM(\Sigma^{\infty})] = 1 \tag{2.2.2.8}$$

The most important case from which, in a certain proper sense, all the others cases may be derived is when the measure μ is the unbiased Lebesgue measure $P_{unbiased}$ on Σ^{∞}.

DEFINITION 2.2.6

MARTIN-LÖF RANDOM SEQUENCES:

$$MARTIN-L\ddot{O}F-RANDOM(\Sigma^{\infty}) \;:=\; P_{unbiased}-RANDOM(\Sigma^{\infty}) \tag{2.2.2.9}$$

We want now to present one of the more fundamental results of Algorithmic Information Theory: the Chaitin-Schnorr's Theorem.

This requires, anyway, the introduction of some technicalities.

Given a sequence $\bar{x} \in \Sigma^{\infty}$ and a set of strings $S \subset \Sigma^{\star}$ let us denote by $S\,\Sigma^{\infty}$ the set of all the sequences having the strings of S as prefixes, i.e.:

$$S\,\Sigma^{\infty} \;:=\; \{\bar{x} \in \Sigma^{\infty} \,:\, \vec{x}(n) \in S \text{ for some natural } n \geq 1\} \tag{2.2.2.10}$$

lightening the notation for singletons by poning:

$$\vec{x}\Sigma^{\infty} \;:= \{\vec{x}\}\Sigma^{\infty} \;\; \vec{x} \in \Sigma^{\infty} \tag{2.2.2.11}$$

We need the following:

Lemma 2.2.1

$$\begin{aligned} &\bar{x} \in MARTIN-L\ddot{O}F-RANDOM(\Sigma^{\infty}) \;\Leftrightarrow \\ &\quad \forall Covering \in \Sigma^{\star} \times \mathbb{N} \text{ r.e. } \;: (P_{unbiased}(Covering_{n}\Sigma^{\infty}) < \frac{1}{2^{n}}\,\forall n \geq 1) \\ &\qquad \exists m \in \mathbb{N} \,:\, \bar{x} \notin Covering_{m}\Sigma^{\infty} \end{aligned} \tag{2.2.2.12}$$

where, as with the same notation of eq.2.1.2.6 that we will understand from here and beyond:

$$Covering_{n} \;:=\; \{\vec{x} \in \Sigma^{\star} \,:\, (\vec{x}, n) \in Covering\} \tag{2.2.2.13}$$

Indeed Lemma2.2.1 is the starting point of a path leading to Solovay' s way of characterizing classical algorithmic randomness.

The first step it to observe that one can always effectively pass from an arbitrary covering to a prefix-free one, as is stated by the following:

Lemma 2.2.2

For every r.e. set $B \subset \Sigma^{\star} \times \mathbb{N}_{+}$, we can effectively find a r.e. set $C \subset \Sigma^{\star} \times \mathbb{N}_{+}$ such that:

$$C_{n} \;\text{ is prefix-free }\; \forall n \in \mathbb{N}_{+} \tag{2.2.2.14}$$

$$B_{n}\Sigma^{\infty} \;=\; C_{n}\Sigma^{\infty} \;\; \forall n \in \mathbb{N}_{+} \tag{2.2.2.15}$$

Lemma2.2.1 and Lemma2.2.2 immediately imply the following:

Lemma 2.2.3

$$\bar{x} \in MARTIN-L\ddot{O}F-RANDOM(\Sigma^{\infty}) \;\Leftrightarrow$$
$$\forall Covering \in \Sigma^{\star}\times\mathbb{N} \text{ r.e. } : (Covering_{n} \text{ is prefix-free} \, \forall n) \, and \, (P_{unbiased}(Covering_{n}\Sigma^{\infty}) < 2^{n} \, \forall n \geq 1)$$
$$\exists m \in \mathbb{N} \, : \, \bar{x} \notin Covering_{m}\Sigma^{\infty} \quad (2.2.2.16)$$

that allows to show the equivalence between the passage of a universal sequential Martin-Löf test and Solovay randomness defined as:

DEFINITION 2.2.7

$\bar{x} \in \Sigma^{\infty}$ IS SOLOVAY-RANDOM ($\bar{x} \in SOLOVAY-RANDOM(\Sigma^{\infty})$):

$$\forall X \subset \Sigma^{\star} \times \mathbb{N}_{+} \; r.e. \; : \sum_{n=1}^{\infty} P_{unbiased}(X_{n}\Sigma^{\infty}) \; < \; \infty$$
$$\exists N \in \mathbb{N} : \bar{x} \notin X_{n}\Sigma^{\infty} \; \forall n > N \quad (2.2.2.17)$$

as stated by the following:

Theorem 2.2.2

$$MARTIN-L\ddot{O}F-RANDOM(\Sigma^{\infty}) \; = \; SOLOVAY-RANDOM(\Sigma^{\infty}) \quad (2.2.2.18)$$

PROOF:

- $SOLOVAY-RANDOM(\Sigma^{\infty}) \subseteq MARTIN-L\ddot{O}F-RANDOM(\Sigma^{\infty})$

  Clearly to prove the thesis is equivalent to show that:

  $$\bar{x} \notin MARTIN-L\ddot{O}F-RANDOM(\Sigma^{\infty}) \; \Rightarrow \; \bar{x} \notin SOLOVAY-RANDOM(\Sigma^{\infty}) \quad (2.2.2.19)$$

  Let us then assume that $\bar{x} \notin MARTIN-L\ddot{O}F-RANDOM(\Sigma^{\infty})$.

  By Lemma2.2.3 it follows that there exist a r.e. set $X \subset \Sigma^{\star} \times \mathbb{N}_{+}$ such that:

  $$X_{n} \text{ is prefix-free } \; \forall n \in \mathbb{N}_{+} \quad (2.2.2.20)$$
  $$P_{unbiased}(X_{n}\Sigma^{\infty}) \; < \; \frac{1}{2^{n}} \quad (2.2.2.21)$$
  $$\bar{x} \; \notin \; \bigcap_{n=1}^{\infty} X_{n}\Sigma^{\infty} \quad (2.2.2.22)$$

  But then:

  $$\sum_{n=1}^{\infty} P_{unbiased}(X_{n}\Sigma^{\infty}) \; \leq \; \sum_{n=1}^{\infty} \frac{1}{2^{n}} \; = \; 1 \; < \; \infty \quad (2.2.2.23)$$

  and conseguentially $\bar{x} \notin SOLOVAY-RANDOM(\Sigma^{\infty})$

- $MARTIN-LÖF-RANDOM(\Sigma^{\infty}) \subseteq SOLOVAY-RANDOM(\Sigma^{\infty})$

  Clearly to prove the thesis is equivalent to show that:

  $$\bar{x} \notin SOLOVAY - RANDOM(\Sigma^{\infty}) \Rightarrow \bar{x} \notin MARTIN - LÖF - RANDOM(\Sigma^{\infty}) \tag{2.2.2.24}$$

  Let us then assume that $\bar{x} \notin MARTIN - LÖF - RANDOM(\Sigma^{\infty})$.
  Conseguentially there exist a r.e. set $X \subset \Sigma^{\star} \times \mathbb{N}_{+}$ such that:

  $$X_n \text{ is prefix-free } \forall n \in \mathbb{N}_{+} \tag{2.2.2.25}$$

  $$P_{unbiased}(X_n \Sigma^{\infty}) < \frac{1}{2^n} \tag{2.2.2.26}$$

  $$cardinality(\{n \in \mathbb{N}_{+} : \bar{x} \in X_n \Sigma^{\infty}\}) = \aleph_0 \tag{2.2.2.27}$$

  Given an arbitrary positive real number $c \in \mathbb{R}_{+}$ let us introduce the set:

  $$B := \{(\vec{y}, n) \in \Sigma^{\star} \times \mathbb{N} : cardinality(\{n \in \mathbb{N}_{+} : \vec{y} \in X_n \Sigma^{\star}\}) > 2^{n+c}\} \tag{2.2.2.28}$$

  By construction:

  $$P_{unbiased}(B_n \Sigma^{\infty}) < 2^{-n} \ \forall n \in \mathbb{N}_{+} \tag{2.2.2.29}$$

  Furthermore $\bar{x} \in \bigcap_{n=1}^{\infty} B_n \Sigma^{\infty}$, i.e. for every natural $n \geq 1$ there exist a natural $m \geq 1$ such that:

  $$cardinality(\{n \in \mathbb{N}_{+} : \vec{x}(m) \in X_n \Sigma^{\star}\} > 2^{n+c} \tag{2.2.2.30}$$

  Just take $m = \max\{i_1, i_2, \cdots, i_t\}$, where $t > 2^{n+c}$ and:

  $$\bar{x} \in \bigcap_{j=1}^{t} X_{i_t} \Sigma^{\infty} \tag{2.2.2.31}$$

■

An other ingredient required for proving Chaitin-Schnorr's Theorem is (a slighty streghtened form of the) Chaitin-Levin's Theorem expressing the deep link existing between **prefix algorithmic entropy** and the **universal algorithmic probability** introduced by definition1.3.8, namely the following:

Theorem 2.2.3

$$\exists c \in \mathbb{R}_{+} : 0 \leq I(\vec{x}) + \log_2 P_U(\vec{x}) \leq c \ \forall \vec{x} \in \Sigma^{\star} \tag{2.2.2.32}$$

Corollary 2.2.1

CHAITIN-LEVIN'S THEOREM

$$I(\vec{x}) \stackrel{\pm}{=} -\log_2 P_U(\vec{x}) \tag{2.2.2.33}$$

The last ingredient required for proving Chaitin-Schnorr's Theorem is the following generalization of Theorem1.3.5 to arbitrary r.e. sets.

Theorem 2.2.4

KRAFT-CHAITIN'S THEOREM
HP:

$\phi \in C_M - C_\Phi - \Delta_0^0 - \overset{\circ}{MAP}\ (\mathbb{N}, \mathbb{N})\ :\ HALTING(\phi)$ is an initial segment of $\mathbb{N}_+$

TH:

The following statements are equivalent:

1. We can effectively construct a function $\theta \in C_M - C_\Phi - \Delta_0^0 - \overset{\circ}{MAP}\ (\mathbb{N}_+, \Sigma^\star)$ such that:

$$HALTING(\theta) = HALTING(\phi) \tag{2.2.2.34}$$

$$|\theta(n)| = \phi(n)\ \ \forall n \in HALTING(\phi) \tag{2.2.2.35}$$

$$Range(\theta)\ \text{ is prefix-free} \tag{2.2.2.36}$$

2.

$$\sum_{n \in HALTING(\phi)} 2^{-\phi(n)} \leq 1 \tag{2.2.2.37}$$

Let us finally afford our objective:

Theorem 2.2.5

CHAITIN-SCHNORR'S THEOREM

$$MARTIN - L\ddot{O}F - RANDOM(\Sigma^\infty) = CHAITIN - RANDOM(\Sigma^\infty) \tag{2.2.2.38}$$

PROOF:

- $MARTIN-L\ddot{O}F-RANDOM(\Sigma^{\infty}) \subseteq CHAITIN-RANDOM(\Sigma^{\infty})$
  Clearly to prove the thesis is equivalent to show that:

$$\bar{x} \notin CHAITIN - RANDOM(\Sigma^{\infty}) \Rightarrow \bar{x} \notin MARTIN - L\ddot{O}F - RANDOM(\Sigma^{\infty}) \tag{2.2.2.39}$$

Let us assume that for every $m > 0$ there exists an n_m such that $I(\vec{x}(n_m)) < n_m$. By theorem2.2.3 we know we can choose a natural number $c > 0$ such that:

$$\exists c \in \mathbb{R}_{+} \ : \ 0 \ \leq \ I(\vec{x}) \ + \ \log_2 P_U(\vec{x}) \ \leq \ c \ \ \forall \vec{x} \in \Sigma^{\star} \tag{2.2.2.40}$$

Let us introduce the set:

$$Covering \ := \ \{(\vec{y},t) \in \Sigma^{\star} \times \mathbb{N}_{+} \ : \ I(\vec{y}) \ < \ |\vec{y}| - t - c - 1\} \tag{2.2.2.41}$$

Clearly the set Covering is r.e. and:

$$\begin{aligned} P_{unbiased}(Covering_t \Sigma^{\infty}) \ &\leq \ \sum_{\vec{y} \in Covering_t} 2^{-|\vec{y}|} \ = \\ &= \sum_{\{\vec{y} \in \Sigma^{\star} \, : \, I(\vec{y}) \, < \, |\vec{y}| - t - c - 1\}} 2^{-|\vec{y}|} \ \leq \\ &\leq \sum_{\{\vec{y} \in \Sigma^{\star} \, : \, I(\vec{y}) \, < \, |\vec{y}| - t - c - 1\}} 2^{-I(\vec{y}) - t - c - 1} \end{aligned} \tag{2.2.2.42}$$

so that:

$$\begin{aligned} P_{unbiased}(Covering_t \Sigma^{\infty}) \ &\leq \ \sum_{\vec{y} \in \Sigma^{\star}} 2^{-I(\vec{y}) - t - c - 1} \ = \\ &= \ 2^{t-c-1} \sum_{\vec{y} \in \Sigma^{\star}} 2^{-I(\vec{y})} \ \leq \ 2^{-t-1} \sum_{\vec{y} \in \Sigma^{\star}} P_U(|\vec{y}|) \ = \\ &= \ 2^{t-1} \ < \ 2^{-t} \end{aligned} \tag{2.2.2.43}$$

We prove now that $\bar{x} \in \bigcap_{t=1}^{\infty} Covering_t \Sigma^{\infty}$. Indeed, given $t > 0$, construct $m_t \ := \ n_{t+c+1}$ and use the hypothesis:

$$I(\vec{x}(m_t)) \ = \ I(\vec{x}(n_{t+c+1})) \ < \ n_{t+c+1} \ - \ (t + c + 1) \ = \ m_t - t - c - 1 \tag{2.2.2.44}$$

i.e. $\vec{x}(m_t) \ \in \ Covering_t$.
By Lemma2.2.1 $\bar{x} \notin MARTIN - L\ddot{O}F - RANDOM(\Sigma^{\infty})$

- $CHAITIN-RANDOM(\Sigma^{\infty}) \subseteq MARTIN-L\ddot{O}F-RANDOM(\Sigma^{\infty})$
  To prove the thesis is equivalent to show that:

$$\bar{x} \notin MARTIN - L\ddot{O}F - RANDOM(\Sigma^{\infty}) \Rightarrow \bar{x} \notin CHAITIN - RANDOM(\Sigma^{\infty}) \tag{2.2.2.45}$$

Let us assume that $\bar{x} \notin MARTIN - L\ddot{O}F - RANDOM(\Sigma^{\infty})$. By Lemma2.2.1 there exist a r.e. set $Covering \subset \Sigma^{\star} \times \mathbb{N}$ such that:

$$P_{unbiased}(Covering_n \Sigma^{\infty}) \; < 2^{-n} \;\; \forall n \in \mathbb{N}_{+} \tag{2.2.2.46}$$

$$\bar{x} \in \bigcap_{n=1}^{\infty} Covering_n \Sigma^{\infty} \tag{2.2.2.47}$$

Furthermore, by Lemma2.2.2, we may assume that $Covering_n$ is prefix-free for all $n\, geq\, 1$. Then:

$$\sum_{n=2}^{\infty} \sum_{\vec{y} \in Covering_{n^2}} 2^{-(|\vec{y}|-n)} \; = \; \sum_{n=2}^{\infty} 2^n \sum_{\vec{y} \in Covering_{n^2}} 2^{-|\vec{y}|} \; =$$

$$= \sum_{n=2}^{\infty} 2^n P_{unbiased}(Covering_{n^2} \Sigma^{\infty}) \; \leq \; \sum_{n=2}^{\infty} 2^{n-n^2} \; \leq \; 1 \tag{2.2.2.48}$$

By theorem2.2.4 we get a Chaitin computer C satisfying the following requirement:

$$\forall n \geq 2, \forall \vec{y} \in Covering_{n^2} \; \exists \vec{u} \in \Sigma^{|\vec{y}|-n} \; : \; C(\vec{u}, \lambda) \; = \; \vec{y} \tag{2.2.2.49}$$

By the Invariance Theorem for Prefix Algorithmic Entropy, namely theorem1.2.9, there exists a positive constant c such that:

$$I(\vec{y}) \; \leq \; |\vec{y}| - n + c \;\; \forall n \geq 2, \forall \vec{y} \in Covering_{n^2} \tag{2.2.2.50}$$

Next we prove that for all natural $n \geq 1$ there exist infinitely many m such that $\vec{x}(m) \in Covering_{n^2}$.

By hypothesis:

$$\vec{x} \; \in \; \bigcap_{k=1}^{\infty} Covering_k \Sigma^{\infty} \tag{2.2.2.51}$$

so for every n we can find a natural m_{n^2} with $\vec{x}(m_{n^2}) \in Covering_{n^2}$.

We have to prove that we can choose these numbers m_{n^2} as large as we wish.

Assume, for the sake of a contradiction, that $m_{n^2} \;\; \geq \;\; N$, for all n and some fixed N. This means the existence of a string $\vec{y}$ of length less than N such that $\vec{y}\, in\, Covering_{n^2}$, for all $n \geq 1$. Accordingly, for every $n \geq 1$ one has:

$$\vec{y}\Sigma^{\infty} \; \subset \; Covering_{n^2} \Sigma^{\infty} \tag{2.2.2.52}$$

and:

$$2^{-n^2} \; > \; P_{unbiased}(Covering_{n^2})\Sigma^{\infty} \; \geq \; P_{unbiased}(\vec{y}\Sigma^{\infty}) \; = \; 2^{-|\vec{y}|} \; \geq \; 2^{-N} \tag{2.2.2.53}$$

that is a contradiction.

In conclusion, given $d > 0$ we pick $i > d + c$ and $m \geq 2$ in order to get $\vec{x}(m) \in Covering_{n^2}$: by eq.2.2.2.50:

$$I(\vec{x}(m)) \; \leq \; m - n + c \; < \; m - d \tag{2.2.2.54}$$

■

Summing up, theorem2.2.2 and theorem2.2.5 show that Martin-Löf randomness, Solovay randomness and Chaitin randomness are equivalent notions, characterizing what is nowadays *almost* universally considered as the the correct characterization of the concept of **C_Φ-algorithmic randomness**.

The above *almost* is owed to to a problem we mentioned at the end of section1.5, almost always misunderstood and that is the main source of a sort of incomunicability between the scientific community of mathematical physicists studying Dynamical Systems Theory and the scientific community of the logico-mathematicians and Theoretical-Computer scientists studying Algorithmic Information Theory: Theorem1.5.3 stating that:

$$BRUDNO - RANDOM(\Sigma^{\infty}) \; \subset \; CHAITIN - RANDOM(\Sigma^{\infty}) \tag{2.2.2.55}$$

whose proof, as promized, we report here:

PROOF:

Given a universal computer C, let us introduce another computer C' defined in the following way:

$$C'(\vec{x}) \; := \; \begin{cases} \cdot_{i=1}^{|\vec{y}|} \mathcal{I}(y_i, 2^i, C(\vec{z})) & \text{if } \exists \vec{y}, \vec{z} \in \Sigma^{\star} : \vec{x} = \cdot_{i=1}^{|\vec{y}|} y_i^2 \cdot 01 \cdot \vec{z} \; , \\ C(\vec{x}) & \text{otherwise.} \end{cases} \tag{2.2.2.56}$$

where, generally, $\mathcal{I}(a, n, \vec{b})$ denotes the string obtained inserting the letter a at the n^{th} place of the string $\vec{b}$, i.e.:

$$\mathcal{I}(a, n, \vec{b}) \; := \; b_1 \ldots b_{n-1} \cdot a \cdot b_{n+1} \ldots b_{|\vec{b}|} \quad a \in \Sigma, \vec{b} \in \Sigma^{\star}, n \in \mathbb{N}_+ \; : n \leq |\vec{b}| \tag{2.2.2.57}$$

Clearly C' is a universal computer too.

Given $\bar{u} \in CHAITIN - RANDOM(\Sigma^{\infty})$ let us consider the sequence $\bar{u}'$ defined in the following way:

$$\bar{u}'_i \; := \; \begin{cases} 0 & \text{if } i = 2^k, k \in \mathbb{N} \; , \\ \bar{u}_i & \text{otherwise.} \end{cases} \tag{2.2.2.58}$$

Since:

$$K_{C'}(\vec{u}_n) \; \leq \; K_{C'}(\vec{u}'_n) + 2 + \log_2 n \tag{2.2.2.59}$$

It follows that:

$$\bar{u}' \in BRUDNO - RANDOM(\Sigma^{\infty}) \tag{2.2.2.60}$$

Let us now consider the Martin-Löf sequential test $V \subset \Sigma^{\star} \times \mathbb{N}_{+}$ whose n^{th} section is given by:

$$V_n := \{\vec{x} \in \Sigma^{\star} : x_{2^k} = 0 \ k = 0, \cdots, i-1\} \tag{2.2.2.61}$$

Since by construction one has that:

$$\bar{u}' \notin \bigcap_{n=1}^{\infty} V_n \tag{2.2.2.62}$$

it follows that:

$$\bar{u}' \notin CHAITIN - RANDOM(\Sigma^{\infty}) \tag{2.2.2.63}$$

■

Chapter 3

Classical algorithmic randomness as satisfaction of all the classical algorithmic typical properties

3.1 Typical properties of a classical probability space

We have seen in chapter2 that classical algorithmic randomness may be characterized as the passage of all the classical algorithmic statistical tests, i.e. of all the effectively implementable testes designed to catch some kind of regularity:

in this chapter we will show in which sense the absense of any kind of regularity may be interpreted as a condition of maximal conformism, i.e. as the ownership to all the overwhelming majorities.

Let us consider a collectivity S made of $N \in \mathbb{N}$ people.

Given a property $p(\cdot)$ will say that it is a **majoritary** property of S if the people in S having such a property are more than those not having it, i.e. iff:

$$cardinality(\{x \in S : p(x) \; holds\}) \; > \; \frac{N}{2} \tag{3.1.3.1}$$

We will say that $p(\cdot)$ is a **typical property** of S if the people in S having such a property are very more than those not having it, i.e. iff:

$$cardinality(\{x \in S : p(x) \; holds\}) \; \gg \; \frac{N}{2} \tag{3.1.3.2}$$

Of course this last notion is only an informal one, owing to the informal nature of the ordering relation **very greater than**.

Let us now consider the case in which the collectivity S is infinite but countable, i.e. $cardinality(S) = \aleph_0$; in this case the same notion of a majoritary property loses its meaning [1].

In the case of an infinite and uncountable community, i.e. $cardinality(S) \geq \aleph_1$, if S admits an unbaised probability measure $P_{unbiased}$ the notion of a **typical property** of S may be rigorously defined as a property holding $P_{unbiased}$ almost everywhere in S.

So the characterization of classical algorithmic randomness as **absolute conformism**, i.e. as the ownership of all the typical properties, would seem to be precisely formalized.

Such a formalization, anyway, results in an empty notion: asbolute conformism is impossible.

The solution to such a bug consists in requiring only the ownerhip of all the **effectively-refutable** typical properties.

The fact that, once again, Classical Measure Theory appears not to be self-consistent as to the characterization of classical algorithmic randomness has a great foundational relevance.

Given a classical probability space $CPS := (M, \mu)$:

DEFINITION 3.1.1

$S \subset M$ IS A NULL SET OF CPS:

$$\forall \epsilon > 0 \, \exists F_{\epsilon} \in HALTING(\mu) \; : \; S \subset F_{\epsilon} \; and \; \mu(F_{\epsilon}) < \epsilon \tag{3.1.3.3}$$

Let us introduce the following notions:

DEFINITION 3.1.2

UNARY PREDICATES ON M:

$$\mathcal{P}(M) \equiv \{p(x) \; : \; \text{predicate about } x \in M\} \tag{3.1.3.4}$$

DEFINITION 3.1.3

[1] Let us observe, by the way, that this inficiates the meaning of the generalization to infinite collectivities of the celebrated Nobel-prize for-Economics-winning Kenneth Arrow's theorem on the impossibility of democracy stating , in technical terms, that under the assumption that the decisive sets form an ultrafilter on the set of voters they form a principal filter too (and so there exist a dictator, i.e. a voter whose vote alone determines the result of any election). Such a generalization may be obtained in the same way the impossibility of applying the theorem stating the principality of any ultafilter on finite sets was overcome by Kurt Goëdel in his mathematical formalization of Anselm of Aosta's ontological proof simply by adding the assumption that being God is a positive property: appealing to the theorem stating that an ultrafilter on a (finite or infinite set) containing the intersection of all its elements is principal [Man98] [Odi00]

TYPICAL PROPERTIES OF CPS:

$$\mathcal{P}(CPS)_{TYPICAL} \equiv \{ p(x) \in \mathcal{P}(M) : \{x \in M : p(x) \text{ doesn't hold } \} \text{ is a null set}\} \tag{3.1.3.5}$$

Example 3.1.1

TYPICAL PROPERTIES OF A DISCRETE CLASSICAL PROBABILITY SPACE

If CPS is discrete-finite ($M = \{a_1 , \dots a_n\}$) or discrete-infinite ($M = \{a_n\}_{n \in \mathbb{N}}$) it is natural to assume that $\mu(\{a_i\}) > 0 \; \forall i$ since an element whose singleton has zero probability can be simply thrown away from the beginning.

It follows, than, that CPS has no null sets and, conseguentially, typical properties are simply the holding properties.

Example 3.1.2

SOME TYPICAL PROPERTY OF THE UNBIASED SPACE OF CBITS' SEQUENCES:

Among the typical properties of the **unbaised space of binary sequences** $(\Sigma^{\infty} , P_{unbaised})$ there are the following:

- **Borel normality of order** $m \in \mathbb{N}$:

$$p_{m-Borel}(\bar{x}) := << \lim_{n \rightarrow \infty} \frac{N_i(\vec{x}(n))}{\lfloor \frac{n}{m} \rfloor} = \frac{1}{2^m} >> \tag{3.1.3.6}$$

  where $N_i(\vec{y}) \, i \in \Sigma$ denotes the number of occurence of the letter $i \in \Sigma$ in the string $\vec{y} \in \Sigma^{\star}$

- **infinite recurrence**

$$p_{infinite\ recurrence}(\bar{x}) :=<< cardinality\{n \in \mathbb{N} : \frac{N_1(\vec{x}(n))}{n} = \frac{1}{2}\} = \aleph_0 >> \tag{3.1.3.7}$$

- **iterated-logarithm property**

$$p_{iterated\ logarithm}(\bar{x}) :=<< \limsup_{n \rightarrow \infty} \frac{\sum_{i=1}^{n} x_i - \frac{n}{2}}{\sqrt{n \log \log n}} \leq \frac{1}{\sqrt{2}} >> \tag{3.1.3.8}$$

- **transcendence**

$$p_{trascendence}(\bar{x}) :=<< \mathcal{N}(\bar{x}) \notin \mathbb{A} >> \tag{3.1.3.9}$$

- **irrecursivity**

$$p_{irrecursivity}(\bar{x}) :=<< \mathcal{N}(\bar{x}) \notin \Delta_0^0([0,1)) >> \tag{3.1.3.10}$$

- **irrationality**

$$p_{irrationality}(\bar{x}) :=<< \mathcal{N}(\bar{x}) \notin \mathbb{Q} >> \tag{3.1.3.11}$$

- **ownership of all substrings**

$$p_{\text{ownership of all substrings}}(\bar{x}) :=<< \forall \vec{y} \in \Sigma^{\star} \, \exists n, m \in \mathbb{N}_{+} : \vec{x}(n,m) = \vec{y} >> \tag{3.1.3.12}$$

- **difference from $\bar{y} \in \Sigma^{\infty}$**

$$p_{\text{difference from } \bar{y}}(\bar{x}) :=<< \bar{x} \neq \bar{y} >> \tag{3.1.3.13}$$

3.2 Impossibility of absolute conformism in Classical Probability Theory

Kolmogorov's original idea about the characterization of the **intrinsic randomness** of an **individual object** was to consider it as more random as more it is conformistic, in the sense of conforming itself to the collectivity belonging to all the overwhelming majorities, i.e. possessing all the typical properties [Vit97], [Cal94] .

Such an attitude results in the following:

DEFINITION 3.2.1

SET OF THE KOLMOGOROV-RANDOM ELEMENTS OF $(\Sigma^{\infty}\,, P_{unbaised})$:

$$KOLMOGOROV - RANDOM[(\Sigma^{\infty}\,, P_{unbaised})] \equiv \\ \{\, x \in M \,: p(x) \; holds \;\; \forall p \in \mathcal{P}[(\Sigma^{\infty}\,, P_{unbaised})]_{TYPICAL} \,\} \tag{3.2.3.1}$$

But an immediate application of the Cantorian diagolization-proof's technique [Odi89] lead to the following:

Theorem 3.2.1

NOT EXISTENCE OF KOLMOGOROV RANDOM SEQUENCES OF CBITS

$$KOLMOGOROV - RANDOM[(\Sigma^{\infty}\,, P_{unbaised})] \;=\; \emptyset \tag{3.2.3.2}$$

PROOF:

Let us consider again the family of unary predicates $p_{\text{difference from } \bar{y}}$ over Σ^{∞} depending on the parameter $\bar{y} \in \Sigma^{\infty}$ introduced in the example3.1.2

We already saw that they are all typical properties of $(\Sigma^{\infty}\,, P_{unbaised})$

$$p_{\text{difference from } \bar{y}}(\bar{x}) \;\in\; \mathcal{P}[(\Sigma^{\infty}\,, P_{unbaised})]_{TYPICAL} \;\; \forall \bar{y} \in \Sigma^{\infty} \tag{3.2.3.3}$$

Let us now observe that:

$$p_{\text{difference from } \bar{x}}(\bar{x}) \text{ doesn't hold } \; \forall \bar{x} \in \Sigma^{\infty} \tag{3.2.3.4}$$

So $p_{\text{difference from } \bar{x}}$ is a typical property that is not satisfied by any element of Σ^{∞}, immediately implying the thesis ■

The theorem3.2.1 shows that we have to relax the condition that a random sequence of cbits possesses **all the typical properties** requiring only that it satisfies **a proper subclass of typical properties**.

The right subclass was proposed by P. Martin Löf who observed that all the Classical Laws of Randomness, i.e. all the properties of Classical Probability Theory that are known to hold with probability one (such as the *Law of Large Numbers*, the *Law of Iterated Logarithm* and so on) are **effectively-falsificable** in the sense that we can effectively test whether they are violated (though we cannot effectively certify that they are satisfied).

This leads, assuming the Church-Turing's Thesis [Odi89] and endowed Σ^{∞} with the **product topology** induced by the **discrete topology** of Σ, to introduce the following notions:

DEFINITION 3.2.2

$S \subset \Sigma^{\infty}$ IS ALGORITHMICALLY-OPEN:

$$(S \text{ is open }) \, and \, (S = X\Sigma^{\infty} \, \mathbf{X \; recursively - enumerable}) \tag{3.2.3.5}$$

DEFINITION 3.2.3

ALGORITHMIC SEQUENCE OF ALGORITHMICALLY-OPEN SETS:

a sequence $\{S_n\}_{n \geq 1}$ of algorithmically open sets $S_n = X_n \Sigma^{\infty} : \exists X \subset \Sigma^{\star} \times \mathbb{N}$ **recursively enumerable** with:

$$X_n = \{\vec{x} \in \Sigma^{\star} : (\vec{x}, n) \in X\} \;\; \forall n \in \mathbb{N}_{+}$$

Given the classical probability space $CPS := (\Sigma^{\infty}, P)$:

DEFINITION 3.2.4

$S \subset \Sigma^{\infty}$ IS AN ALGORITHMICALLY-NULL SUBSET OF CPS:

$\exists \{G_n\}_{n \geq 1}$ algorithmic sequence of algorithmically-open sets :

$$S \subset \cap_{n \geq 1} G_n$$

and:

$$alg - \lim_{n \to \infty} P(G_n) = 0$$

i.e. there exist and increasing, unbounded, **recursive** function $f : \mathbb{N} \to \mathbb{N}$ so that $P(G_n) < \frac{1}{2^k}$ whenever $n \geq f(k)$

DEFINITION 3.2.5

LAWS OF RANDOMNESS OF CPS:

$$\begin{aligned} \mathcal{L}_{randomness}(CPS) \equiv \{ & p(\bar{x}) \in \mathcal{P}(\Sigma^{\infty}) : \\ & \{\bar{x} \in \Sigma^{\infty} : p(\bar{x}) \text{ doesn't hold } \} \text{ is an algorithmically null set of CPS}\} \end{aligned} \tag{3.2.3.6}$$

Example 3.2.1

SOME LAW OF RANDOMNESS OF THE UNBIASED SPACE OF CBITS' SEQUENCES: Let us consider again the typical properties of the classical probability space $(\Sigma^{\infty}, P_{unbiased})$ introduced in the example3.1.2.

Borel normality of order $m \in \mathbb{N}$, **infinite recurrence**, the **iterated-logarithm property**, **transcendence** and **irrationality** are all effectively-refutable and, hence, are all Laws of Randomness.

To refute that a sequence has the property of **irrecursivity**, or of **ownership of all substrings**, or of **difference from** $\bar{y} \in \Sigma^{\infty}$ would, instead, require the inspection the analysis of an infinite number of of its digits.

Hence all such typical properties are not effectively-refutable and, hence, are not laws of randomness.

We can now introduce the following:

DEFINITION 3.2.6

P-CONFORMISTICALLY RANDOM ELEMENTS OF CPS:

$$P - CONF - RANDOM(\Sigma^{\infty}) \ := \ \{\bar{x} \in \Sigma^{\infty} \ p(\bar{x}) \text{ holds } \ \forall p \in \mathcal{L}_{randomness}(CPS)\} \quad (3.2.3.7)$$

As usual the case of the unbaised measure deserves an ad hoc definition:

DEFINITION 3.2.7

CONFORMISTICALLY-RANDOM SEQUENCES:

$$CONF - RANDOM(\Sigma^{\infty}) \ := \\ P_{unbaised} - CONF - RANDOM(\Sigma^{\infty}) \quad (3.2.3.8)$$

Remark 3.2.1

WHY THE DIAGONALIZATION PROOF OF THEOREM3.2.1 DOESN'T APPLY TO P-CONFORMISTICALLY RANDOMNESS

Let us observe that the diagonalization proof of theorem3.2.1 is based on the one-parameter family of typical properties $p_{\text{difference from } \bar{y}}$, $\bar{y} \in \Sigma^{\infty}$. Since noone of these is a law of randomness the argument falls down.

3.3 Equivalence between Martin Löf-conformistical randomness and Chaitin randomness

Summing up, we have seen that Per Martin Löf introduced two approaches to the mathematical characterization of classical algorithmic randomness:

- the **statistical approach** discussed in chapter2 and resulting in the definition of the set $MARTINL\ddot{O}F - RANDOM(\Sigma^{\infty})$ whose equality with the set $CHAITIN - RANDOM(\Sigma^{\infty})$ is stated by theorem2.2.5
- the **logical approach** discussed in the previous sections and resulting in the definition of the set $CONF - RANDOM(\Sigma^{\infty})$

In this section we will prove Martin-Löf's Theorem showing the the complete equivalence of these approaches.

This requires the introduction of some technical ingredient, starting from the following:

Lemma 3.3.1

For every sequential $P_{unbaised}$-test V and for every natural $m \geq 1$:

$$\sum_{\vec{x} \in \Sigma^{n} \bigcap V_{m}} 2^{-|\vec{x}|} \; < \; 2^{-m} \tag{3.3.3.1}$$

PROOF:

It follows immediately from the cardinality inequality in the definition of a sequential Martin-Löf test ■

Then we need the following:

Lemma 3.3.2

Let V be a sequential $P_{unbaised}$-test. Then

$$\lim_{m \rightarrow \infty} P_{unbaised}(V_{m}\Sigma^{\infty}) \; = \; 0 \; \textit{constructively} \tag{3.3.3.2}$$

PROOF:

Take V and define for every natural $m \geq 1$ the sets $W_{m} \; := \; V_{m}\Sigma^{\infty}$. It is seen that for each $m \geq 1$, $W_{m} \; = \; \bigcup_{n=2}^{\infty} X_{n}$, where:

$$X_{n} \; := \; \bigcup_{\vec{x} \in \Sigma^{n} \bigcap V_{m}} \vec{x}\Sigma^{\infty} \tag{3.3.3.3}$$

Furthermore, $X_{n} \; \subset \; X_{n+1}$ and:

$$\begin{aligned} P_{unbaised}(X_{n}) \; &= \; \sum_{\vec{x} \in \Sigma^{n} \bigcap V_{m}} P_{unbaised}(\vec{x}\Sigma^{\infty}) \\ &= \; \sum_{\vec{x} \in \Sigma^{n} \bigcap V_{m}} 2^{-|\vec{x}|} \; = \; \frac{cardinality(\Sigma^{n} \bigcap V_{m})}{2^{n}} \\ &< 2^{-m} \end{aligned} \tag{3.3.3.4}$$

in view of lemma3.3.2 and of the fact that the sets $\{\vec{x}\Sigma^{\infty} : \vec{x} \in \Sigma^{n} \bigcap V_{m}\}$ are mutually disjoint. So:

$$P_{unbiased}(W_{m}) \; = \; \lim_{n \rightarrow \infty} P_{unbiased}(X_{n}) \; \leq \; 2^{-m} \tag{3.3.3.5}$$

Finally, put $H(m) \; := \; m+1$ and notice that if $m \; \geq \; H(k)$, then $P_{unbiased}(W_{m}) \; \leq 2^{-k}$ ■

The last ingredient required for proving Martin-Löf's Theorem is the following:

Lemma 3.3.3 *Let V be a sequential $P_{unbaised}$-test. Then $\bigcap_{m=1}^{\infty}(V_{m}\Sigma^{\infty})$ is an algorithmically-null subset of $(\Sigma^{\infty}, P_{unbaised})$*

PROOF:

Take V and define for every natural $m \geq 1$ the sets $W_{m} \; := \; V_{m}\Sigma^{\infty}$. Since V is r.e. it follows that the sequence $\{V_{m}\}_{m \in \mathbb{N}_{+}}$ is an algorithmic sequence of algorithmically opens sets.

By lemma3.3.2 it follows the thesis ■

We have at last all the ingredients required to prove the following:

Theorem 3.3.1

MARTIN-LÖF'S THEOREM:

$$CONF-RANDOM(\Sigma^{\infty}) \; = \; CHAITIN-RANDOM(\Sigma^{\infty}) \tag{3.3.3.6}$$

PROOF:

Fix a universal sequential $P_{unbaised}$-test U. Since:

$$\Sigma^{\infty} \; - \; CHAITIN-RANDOM(\Sigma^{\infty}) \; = \; \bigcap_{m=1}^{\infty} U_{m}\Sigma^{\infty} \tag{3.3.3.7}$$

we may apply lemma3.3.3 to conclude that $\Sigma^{\infty} - CHAITIN-RANDOM(\Sigma^{\infty})$ is an algorithmically-null set.

Next let $S \subset \Sigma^{\infty}$ be an arbitrary algorithmically-null set. We shall prove that:

$$S \; \subset \; \Sigma^{\infty} \; - \; CHAITIN-RANDOM(\Sigma^{\infty}) \tag{3.3.3.8}$$

To this aim let us consider an algorithmic sequence of algorithmically open sets $(G_{m})_{m \geq 1}$ such that:

$$S \; \subset \; \bigcap_{m=1}^{\infty} G_{m} \tag{3.3.3.9}$$

and:

$$P_{unbaised}(G_{t}) \; < \; 2^{-m} \;\; \forall t \geq H(m) \tag{3.3.3.10}$$

where $H : \mathbb{N} \mapsto \mathbb{N}$ is a fixed increasing, unbounded recursive function.

Write:

$$G_m \ := \ X_m \Sigma^{\infty} \ = \ (X_m \Sigma^{\star}) \Sigma^{\infty} \tag{3.3.3.11}$$

for all $m \geq 1$, where $X_m \subset \Sigma^{\star}$ is an r.e. set. We have to construct a sequential $P_{unbiased}$-test V such that:

$$\bigcap_{m=1}^{\infty} V_m \Sigma^{\infty} \ = \ \bigcap_{m=1}^{\infty} G_m \tag{3.3.3.12}$$

Put:

$$V_m \ := \ \bigcap_{i=1}^{H(m)} X_i \Sigma^{\star} \ \ m \in \mathbb{N}_+ \tag{3.3.3.13}$$

Clearly the set V defined as:

$$V \ := \ \{ (\vec{x}, m) \in \Sigma^{\star} \times \mathbb{N}_+ \ : \vec{x} \in V_m \} \tag{3.3.3.14}$$

is r.e., $V_{m+1} \subset V_m$ and is such that if $\vec{x} <_p \vec{y}$ and $\vec{x} \in V_m$ then $\vec{y} \in V_m$.

Fixed $n, m \in \mathbb{N}_+$:

$$\begin{aligned} & cardinality(\Sigma^n \bigcap V_m) \ \leq \ cardinality(X_{H(m)} \Sigma^{\star} \bigcap \Sigma^n \\ = \ & 2^n \, cardinality(X_{H(m)} \Sigma^{\star} \bigcap \Sigma^n) \, 2^{-n} \ = \ 2^n P_{unbaised}(((X_{H(m)} \Sigma^{\star}) \bigcap \Sigma^n) \Sigma^{\infty}) \\ & \leq \ 2^n P_{unbaised}((X_{H(m)} \Sigma^{\star}) \Sigma^{\infty}) \ \leq \ 2^{n-m} \end{aligned} \tag{3.3.3.15}$$

So V is a sequential $P_{unbaised}$-test and, hence, eq.3.3.3.12 holds by virtue of the strict monotonicity of H.

According to the universality of U one can find a natural c such that:

$$V_{m+c} \ \subset \ U_m \ \ \forall m \in \mathbb{N}_+ \tag{3.3.3.16}$$

Then:

$$\begin{aligned} S \ \subset \ & \bigcap_{m=1}^{\infty} V_m \Sigma^{\infty} \ \subset \ \bigcap_{m=1}^{\infty} V_{m+c} \Sigma^{\infty} \\ & \subset \bigcap_{m=1}^{\infty} U_m \Sigma^{\infty} \ = \ \Sigma^{\infty} \ - \ CHAITIN - RANDOM(\Sigma^{\infty}) \end{aligned} \tag{3.3.3.17}$$

■

Remark 3.3.1

ON WHY CLASSICAL PROBABILITY THEORY APPLIES TO REALITY

We can now fully appreciate the conceptual relevance of theorem2.2.1 (and the name we gave to it): it tells us that extracted at random a sequence according to the probability distribution μ the occured sequence will satisfy all the μ Laws of Randomness with certainty.

We indeed have to bless such a theorem: it is only for his courtesy that it is possible to give certain mathematical predictions concerning the statistical behaviour of classically-non deterministic phenomena.

This is particularly rilevant in the case in which μ is the unbaised probability measure $P_{unbiased}$:

it is only because making infinite independent tosses of a fair coin we obtain with certainty a sequence without intrinsic regularity that we can find a mathematical regularity in classical-nondeterminism.

This clarifies why, as we will discuss in chapter5 is very raesonable to expect that an analogous situation must happen also in Quantum Probability Theory.

Chapter 4

Classical algorithmic randomness as stability of the relative frequences under proper classical algorithmic place selection rules

4.1 Von Mises' Frequentistic Foundation of Probability

The mirable features of the Kolmogorovian measure-theoretic axiomatization of Classical Probability Theory [Kol56] has led to consider it as the last word about Foundations of Classical Probability Theory, leading to the general attitude of forgetting the other different axiomatizations and, in particular, von Mises' Frequentistic one [Mis81].

Richard Von Mises' axiomatization of Classical Probability Theory lies on the mathematical formalization of the following two empirical laws:

1. **Law of Stability of Statistic Relative Frequencies**

   "It is essential for the theory of probability that experience has shown that in the game of dice, as in all other mass phenomena which we have mentioned, the relative frequencies of certain attributes become more and more stable as the number of observations is increased" (cfr. pag.12 of [Mis81])

2. **Law of Excluded Gambling Strategies**

> *"Everybody who has been to Monte Carlo, or who has read descriptions of a gambling bank, know how many 'absolutely safe' gambling systems, sometimes of an enormously complicated character, have been invented and tried out by gamblers; and new systems are still suggested every day. The authors of such systems have all, sooner or later, had the sad experience of finding out that no system is able to improve their chance of winning in the long run,i.e. to affect the relative frequencies with which different colours of numbers appear in a sequence selected from the total sequence of the game. This experience forms the experimental basis of our definition of probability"* (cfr. pagg.25-26 of [Mis81])

According to Von Mises Probability Theory concerns properties of collectivities, i.e. of sequences of identical objects.

Considering each individual object as a letter of an alphabet Σ, we can then say that Probability Theory concerns elements of the set Σ^{∞} of the sequences of letters from Σ or, more properly, a certain subset $\mathcal{C}ollectives \subset \Sigma^{\infty}$ whose elements are called **collectives**.

Let us then introduce the set $\mathcal{A}ttributes(\Sigma)$ of the **attributes** of $\mathcal{C}$'s elements defined as the set of unary predicates about the generic $C \in \mathcal{C}ollectives$.

The mathematical formalization of the **Law of Stability of Statistic Relative Frequencies** results in the following:

AXIOM 4.1.1

AXIOM OF CONVERGENCE

HP:

$$C \in \mathcal{C}ollectives$$

$$A \in \mathcal{A}ttributes(\Sigma)$$

TH:

$$\exists \lim_{n \to \infty} \frac{N(A|\vec{C}(n))}{n}$$

where $N(A|\vec{C}(n))$ denotes the number of elements of the prefix $\vec{C}(n)$ of C of length n for which the attribute A holds.

Given an **attribute** $A \in \mathcal{A}ttributes(\Sigma)$ of a **collective** $C \in \mathcal{C}ollectives$ the axiom4.1.1 make consistent the following definition:

DEFINITION 4.1.1

VON MISES' FREQUENTISTIC PROBABILITY OF A IN C:

$$P_{VM}(A|C) := lim_{n\to\infty} \frac{N(A|\vec{C}(n))}{n} \tag{4.1.4.1}$$

Let us then introduce the following basic definition:

DEFINITION 4.1.2

GAMBLING STRATEGY:
$S : \Sigma^{\star} \stackrel{\circ}{\to} \{0,1\}$

Given a gambling strategy S:

DEFINITION 4.1.3

SUBSEQUENCE EXTRACTION FUNCTION INDUCED BY S:
$EXT[S] : \Sigma^{\infty} \to \Sigma^{\infty}$:

$$EXT[S](x_1 x_2 \cdots) := \text{ordered concatenation}(\{x_n : S(x_1 \cdots x_{n-1}) = 1, n \in \mathbb{N}_+\}) \tag{4.1.4.2}$$

The name in the definition4.1.3 is justified by the fact that obviously:

$$EXT[S](\bar{x}) \leq_s \bar{x} \ \ \forall \bar{x} \in \Sigma^{\infty} \tag{4.1.4.3}$$

where $\leq_s$ is the following:

DEFINITION 4.1.4

SUBSEQUENCE ORDERING RELATION ON Σ^{∞}

$$\bar{x} \leq_s \bar{y} := \bar{x} \text{ is a subsequence of } \bar{y} \tag{4.1.4.4}$$

Example 4.1.1

BET EACH TIME ON THE LAST RESULT

Considered the binary alphabet $\Sigma := \{0,1\}$, let us analyze the following gambling strategy:

$$S(x_1 \cdots x_n) := \begin{cases} \uparrow & \text{if } n = 0, \\ x_n & \text{otherwise} \end{cases} \quad x_1 \cdots x_n \in \Sigma^n, n \in \mathbb{N} \tag{4.1.4.5}$$

and the *subsequence extraction function* $EXT[S]$ it gives rise to.

Clearly we have that:

$\vec{x}$	$S(\vec{x})$
λ	$\uparrow$
0	0
1	1
00	0
01	1
10	0
11	1
000	0
001	1
010	0
011	1
100	0
101	1
110	0
111	1
0000	0
0001	1
0010	0
0011	1
0100	0
0101	1
0110	0
0111	1
1000	0
1001	1
1010	0
1011	1
1100	0
1101	1
1110	0
1111	1

Furthermore we have, clearly, that:

$$\begin{aligned} EXT[S](0^{\infty}) &= \lambda \\ EXT[S](0^{\infty}) &= 1^{\infty} \\ EXT[S](01^{\infty}\cdots) &= 0^{\infty} \\ EXT[S](10^{\infty}) &= 0^{\infty} \\ EXT[S](\bar{x}_{Champernowne}) &= 0101\cdots \end{aligned}$$

where $\bar{x}_{Champernowne}$ is the Champernowne sequence defined as the lexicografic ordered concatenation of the binary strings:

$$\bar{x}_{Champernowne} = 0100011011000001010011100101110111\cdots$$

Example 4.1.2

BET ON THE LESS FREQUENT LETTER

Considered again the binary alphabet $\Sigma \; := \; \{0,1\}$, let us analyze the following gambling strategy:

$$S(\vec{x}) \; = \; \begin{cases} \uparrow & \text{if } \vec{x} = \lambda \text{ or } N_0(\vec{x}) = N_1(\vec{x}), \\ 1 & \text{if } N_0(\vec{x}) > N_1(\vec{x}), \\ 0 & \text{otherwise.} \end{cases} \tag{4.1.4.6}$$

where $N_0(\vec{x}), N_1(\vec{x})$ denote the number of, respectively, zeros and ones in the string $\vec{x}$.

We have that:

$\vec{x}$	$S(\vec{x})$
λ	$\uparrow$
0	1
1	0
00	1
01	$\uparrow$
10	$\uparrow$
11	0
000	1
001	1
010	1
011	0
100	1
101	0
110	0
111	0
0000	1
0001	0
0010	1
0011	$\uparrow$
0100	1
0101	$\uparrow$
0110	$\uparrow$
0111	1
1000	1
1001	$\uparrow$
1010	$\uparrow$
1011	0
1100	$\uparrow$
1101	0
1110	0
1111	0

As to the extraction function of S:

$$\begin{aligned} EXT[S](0^{\infty}) &= 0^{\infty} \\ EXT[S](1^{\infty}) &= \lambda \\ EXT[S](01^{\infty}) &= 1^{\infty} \\ EXT[S](10^{\infty}) &= \lambda \\ EXT[S](\bar{x}_{Champernowne}) &= 10011011\cdots \end{aligned}$$

Denoted by $\mathcal{S}trategies(\mathcal{C}ollectives)$ the **set of gambling strategies** concerning $\mathcal{C}ollectives$, we can formalize the **Law of Excluded Gambling Strategies** by the following:

AXIOM 4.1.2

AXIOM OF RANDOMNESS
HP:

$$S \in \mathcal{S}trategies_{admissible}(\mathcal{C}ollectives)$$

$$C \in \mathcal{C}ollectives$$

$$A \in \mathcal{A}ttributes(\Sigma)$$

TH:

$$P_{VM}(\,A \,|\, EXT[S](C)\,) \;=\; P_{VM}(A|C)$$

where $\mathcal{S}trategies_{admissible}(\mathcal{C}ollectives) \subseteq \mathcal{S}trategies(\mathcal{C}ollectives)$ is the **set of admissible gambling strategies** whose mathematical characterization will be investigated in the next sections.

4.2 Classical Gambling in the framework of Classical Statistical Decision Theory

Classical Statistical Decision Theory [Ins00] concerns the following situation:

a *decision maker* have to make a single action $a \in \mathcal{A}ctions$ from a space $\mathcal{A}ctions$ of possible actions.

Features that are unknown about the external world are modelled by an unknown state of nature $s \in \mathcal{S}tates$ in a set $\mathcal{S}tates$ of possible states of nature.

The consequence $c(a, s) \in \mathcal{C}onsequences$ of his choice depends both on the action chosen and on the unknwown state of nature.

Before making his decision the decision maker may observe an outcome $X = x$ of an experiment, which depends on the unknown state s. Specifically the observation X is drawn from a distribution $P_X(\cdot|s)$.

His objectives are encoded in a real valued *utility function* $u(a, s)$.

Let us assume that the *decision maker* knows the *action space* $\mathcal{A}ctions$, *state space* $\mathcal{S}tates$ and *consequence space* $\mathcal{C}onsequences$, along with the probability distribution and the *utility function*.

His problem is:

observe $X = x$ and then choose an action $d(x) \in \mathcal{A}ctions$, using the information that $X = x$, to maximize, in some sense, $u(d(x), s)$.

Every decision process may obviously be seen as a gambling situation: the *action space* $\mathcal{A}ctions$ may be seen as the set of possible bets of the decision maker, that we will call from here and beyond the *gambler*, while the *utility function* gives the *payoff*.

Let us consider, in particular, the following gambling situation:

in the city's *Casino* at each turn $n \in \mathbb{N}$ the croupier tosses a fair coin.

Before the n^{th} toss the gambler can choose among one of the possbile choices:

- to bet one fiche on *head*
- to bet one fiche on *tail*
- not to play at that turn

Leaving all the philosophy behind its original foundational purpose we can, now, from inside the standard Kolomogorovian measure-theoretic formalization of Classical Probability Theory, appreciate the very intuitive meaning lying behind Von Mises' axioms.

Let us indicate by X_n the random variable on the binary alphabet $\Sigma := \{0, 1\}$ (where we will assume from here and beyond, that *head* $= 1$ and *tail* $= 0$) corresponding to the n^{th} coin toss and by $x_n \in \Sigma$ the result of the n^{th} coin toss.

Let us, furthermore, denote by $\bar{x} := (x_1, x_2, , \cdots) \in \Sigma^{\infty}$ the sequence of all the results of the coin tosses and by $\vec{x}(n) \in \Sigma^n$ its n^{th} prefix.

By hypothesis $\{X_n\}_{n \in \mathbb{N}}$ is a Bernoulli($\frac{1}{2}$) discrete-time stochastic process over Σ.

A gambling strategy $S : \Sigma^{\star} \stackrel{\circ}{\rightarrow} \{0, 1\}$ determines the gambler's decision at the n^{th} turn in the following way:

- if $S(\vec{x}(n-1)) = 1$ he bets on *head*
- if $S(\vec{x}(n-1)) = 0$ he bets on *tail*
- if $S(\vec{x}(n-1)) = \uparrow$ he doesn't bet at that turn

Example 4.2.1

APPLYING TO THE CASINO THE GAMBLING STRATEGY OF EXAMPLE4.1.1

Let us suppose that the first 10 coin tosses give the following string of results: $\vec{x}(n) = 1101001001$

Our evening to Casino may be told by the following table:

TOSS	RESULT OF THE TOSS	BET MADE ABOUT THAT TOSS	PAYOFF
1	1	no bet	0
2	1	1	+1
3	0	1	0
4	1	0	-1
5	0	1	-2
6	0	0	-1
7	1	0	-2
8	0	1	-3
9	0	0	-2
10	1	0	-3

As we see $PAYOFF(10) = -3$.

Example 4.2.2

APPLYING TO THE CASINO THE GAMBLING STRATEGY OF EXAMPLE4.1.2

Let us suppose again that the first 10 coin tosses give the following string of results: $\vec{x}(n) = 1101001001$.

Our evening to Casino may be told by the following table:

TOSS	RESULT OF THE TOSS	BET MADE ABOUT THAT TOSS	PAYOFF
1	1	no bet	0
2	1	0	-1
3	0	0	0
4	1	0	-1
5	0	0	0
6	0	0	+1
7	1	no bet	+1
8	0	0	+2
9	0	no bet	+2
10	1	1	+3

As we see $PAYOFF(10) = +3$.

The probability distribution of the string $\vec{x}(n)$ is the uniform distribution on Σ^{n} :

$$Prob[\vec{x}(n) = \vec{y}] \ = P_{unbaised\,,\,n}(\vec{y}) \ := \ \frac{1}{2^{n}} \ \ \forall \vec{y} \in \Sigma^{n}, \forall n \in \mathbb{N} \qquad (4.2.4.1)$$

When $n \to \infty$ such a distribution tends to the unbiased probability measure $P_{unbiased}$ on Σ^{∞}.

Clearly the possible **attributes** of a letter on the binary alphabet are:

- $a_1 \ := <<$ to be $1 >>$
- $a_0 \ := <<$ to be $0 >>$

so that:

$$\mathcal{A}ttributes(\Sigma) \ = \ \{a_1, a_0\} \qquad (4.2.4.2)$$

Whichever $\mathcal{C}ollectives \ \subset \ \Sigma^{\infty}$ is the axiom4.1.1 is, from inside the standard kolmogorovian measure-theoretic foundation, an immediate corollary of the Law of Large Numbers.

As far as axiom4.1.2 is concerned, anyway, the situation is extraordinarily subtler.

Every **intrinsic regularity** of $\vec{x}(n)$ could have been encoded by the gambler in a proper **winning strategy up to the** n^{th} **turn**.

The same definition of what a **winning strategy** is requires some caution: we can, indeed, give two possible definitions of such a concept:

DEFINITION 4.2.1 (AVERAGE-WINNING STRATEGY UP TO THE n^{th} TOSS)
a strategy so that the expectation value of the payoff after the first n tosses ***payoff(n)*** *is greater than zero*

The fact the a strategy is average-winning doesn't imply that the payoff after the n^{th} toss will be strictly positive with certainty: it happens if we are lucky.

Let us now introduce a weaker notion of a winning strategy:

DEFINITION 4.2.2 (LUCKY-WINNING STRATEGY UP TO THE n^{th} TOSS)
a strategy so that the the probability that the payoff after the first n tosses ***payoff(n)*** *is greater than zero is itself greater than zero*

For finite n every strategy is obviously lucky-winning.

Let us now consider the limit $n \to \infty$.

By purely measure-theoretic considerations we may easily prove the following:

Theorem 4.2.1 *WEAK LAW OF EXCLUDED GAMBLING STRATEGIES*
For $n \to \infty$ the set of the average-winning strategies tends to the null set

PROOF:

Given a gambling strategy $S : \Sigma^{\star} \stackrel{\circ}{\rightarrow} \{0, 1\}$ we have clearly that the conditional expectation of the payoff at the n^{th} turn conditioned to the payoff at the $(n-1)^{th}$ turn is the sum of two addenda:

- the payoff at the $(n-1)^{th}$ turn
- the expectation value of the gain at the $(n-1)^{th}$ turn

This second addendum is clearly equal to zero if the adopted gambling strategy prescribes not to bet at the n^{th} turn. Otherwise its is itself given by the sum of two addenda:

- one related to the case in which heads turn up and given by the probability of this fact, obviously equal to $\frac{1}{2}$, taken with positive sign if we betted on head and taken with negative sign if we betted on tail
- one related to the case in which tails turn up and given by the probability of this fact, obviously equal to $\frac{1}{2}$, taken with positive sign if we betted on tail and taken with negative sign if we betted on head

But these last two addenda obviously compensate each other, so that the conditional expectation of the payoff at the n^{th} turn conditioned to the payoff at the $(n-1)^{th}$ turn is simply given by the payoff at the $(n-1)^{th}$ turn.

This reasoning can be expressed in formulae as:

$$\begin{aligned} E[payoff(n)|payoff(n-1)] &= payoff(n-1) + \\ & If[S(\vec{x}_{n-1}) = \uparrow, 0, \frac{1}{2} \\ & If[S(\vec{x}_{n-1}) = 1, 1, -1] + \frac{1}{2} \\ & If[S(\vec{x}_{n-1}) = 0, 1, -1]] = payoff(n-1) \quad \forall n \in \mathbb{N} \end{aligned} \tag{4.2.4.3}$$

(where I have adopted Mc Carthy's LISP conditional notation [Car60] popularized by Wolfram's *Mathematica* [Wol96]).

Furthermore:

$$E[payoff(n)] = \sum_{k=-n+1}^{n-1} P[payoff(n-1) = k] \, E[payoff(n)|payoff(n-1)] \quad \forall n \in \mathbb{N} \tag{4.2.4.4}$$

We will prove that $\lim_{n \rightarrow \infty} E[payoff(n)] = 0$ by proving by induction on n that $E[payoff(n)] = 0 \;\; \forall n \in \mathbb{N}$.

That $E[payoff(1)] = 0$ follows immediately by the fact that $S(\lambda) = \uparrow \;\; \forall S$.

We have, conseguentially, simply to prove that $E[payoff(n-1)] = 0 \Rightarrow E[payoff(n)] = 0 \;\; \forall S$.

This is, anyway, an obvious conseguence of the equations eq.4.2.4.3 and eq.4.2.4.4 ■

Theorem4.2.1 is not, anyway, a great assurance for Casino's owner:

in fact it doesn't exclude that the gambler, if enough lucky, may happen to get a positive payoff for $n \to \infty$.

What will definitely assure him is the following:

Theorem 4.2.2 *STRONG LAW OF EXCLUDED GAMBLING STRATEGIES*
For $n \to \infty$ the set of the lucky-winning strategies tends to the null set

And here comes the astonishing fact: Theorem4.2.2 can't be proved with purely measure-theoretic concepts.

Our approach will consist in taking von Mises' axiom4.1.2 as a definition of the set of subsequences to which such an axiom applies.

Let us then define the **set of collectives** $\mathcal{C}ollectives \subset \Sigma^{\infty}$ as the set of sequences having not enough intrinsic regularity to allow, if they occur, a lucky-winning strategy. Clearly such a definition depends on the class $\mathcal{S}trategies_{admissible}(\mathcal{C}ollectives)$ of admissible gambling strategies.

It would appear natural ,at first, to admit every gambling strategy.

But such a choice would lead immediately to conclude that $\mathcal{C}ollectives = \emptyset$ since given two gambling strategies S_0 and S_1 so that:

$$EXT[S_i](\bar{x}) \text{ is made only of i } \; i = 0, 1 \; \forall \bar{x} \in \Sigma^{\infty} \tag{4.2.4.5}$$

we would have clearly that:

$$P_{VM}(a_i \,|\, EXT[S_1](\bar{x})\,) \neq P_{VM}(a_i \,|\, EXT[S_2](\bar{x}) \;\; \forall \bar{x} \in \Sigma^{\infty} \tag{4.2.4.6}$$

The history of the attempts of characterizing in a proper way the class of the admissible gambling strategies is very long and curious [Lam87], [Vit97], [Gil00] and involved many people: Church, Copeland, Dörge, Feller, Kamke, Popper, Reichenbach, Tornier, Waismann and Wald; I will report here only the conceptually more important contributions:

in the thirties Abraham Wald showed that:

Theorem 4.2.3

WALD'S THEOREM

$$(cardinality(\mathcal{S}trategies_{admissible}(\mathcal{C}ollectives)) = \aleph_0) \Rightarrow (\mathcal{C}ollectives \neq \emptyset) \tag{4.2.4.7}$$

In the fourties, basing on the observation that gambling strategies must be effectively followed, Alonzo Church proposed, according to the Church-Turing's Thesis [Odi89], to consider admissible a gambling strategy if and only if it is a **partial recursive function**.

With such an assumption:

$$\mathcal{S}trategies_{admissible}(\mathcal{C}ollectives) := C_{\Phi} - C_M - \Delta_0^0 - \overset{\circ}{MAP} \,(\Sigma^{\star}, \Sigma^{\star}) \tag{4.2.4.8}$$

it can be proved that:

$$P_{unbiased}(\mathcal{C}ollectives) \ = \ 1 \qquad (4.2.4.9)$$

immediately implying Theorem4.2.2.

Let us the introduce the following:

DEFINITION 4.2.3

CHURCH RANDOM SEQUENCES:

$$CHURCH - RANDOM(\Sigma^{\star}) \ := \ \mathcal{C}ollectives \ \text{ with the assumption of eq.4.2.4.8} \qquad (4.2.4.10)$$

Remark 4.2.1

MARTINGALES AND THE REASON WHY REAL CASINOS RESULT IN ACTIVE

It is important to observe that Theorem4.2.2 was proved under the assumption that the gambler bets always at a fixed odd.

Assuming a more general definition of a gambling strategy in which the odd betted each time is adjustable in function of a recursive function of the history up to that bet, it may be easily proved that winning gambling strategies do exist.

An example is given by **martingales**:

let us suppose that the gambler plays in the following way:

- he insists on betting always on *head*, doubling the stake after a loss
- he stops to bet for ever after the first win

In analyzing such a gambling situation Daniel Bernoulli introduced the so called **Saint Petersburg paradox**:

since the gambler bets 1 fiche that heads will turn up on the first throw, 2 fiches that heads will turn up on the second throw if it didn't turn up on the first, 4 fiches that heads will turn up on the third throw if it didn't turn up in the first two throws and so on, one could conclude the gabler's expected pay off is infinite:

$$\frac{1}{2}(1) \ + \ \frac{1}{4}(2) \ + \ \frac{1}{8}(4) \ + \cdots \ = \ \frac{1}{2} \ + \ \frac{1}{2} \ + \ \frac{1}{2} \ + \ \cdots \ = +\infty \qquad (4.2.4.11)$$

To see clearly where the mistake is, let us proceed by steps.

First of all let us observe that, since **ownerhip of all subsequences** is a Law of Randomness, we have in particular that **ownerhip of the subsequence 1** is a Law of Randomness too.

Hence heads will certainly turn up one day.

Conseguentially it is legitimate to express the expected payoff as a sum on the first time heads turn up, as it was done in eq.4.2.4.11:

$$\lim_{n \to \infty} E[payoff(n)] \;=\; \sum_{n=1}^{\infty} P_{unbaised\, n}(0^{n-1}1) gain(n) \qquad (4.2.4.12)$$

But the gain corresponding to the situation in which heads turn up for the first time at the n^{th} throw must take into account of all the fiches he lost in the previous $n-1$ turns.

So:

$$gain(n) \;=\; 2^{n-1} - \sum_{k=1}^{n-1} 2^{k} \;=\; 2^{n} \;-\; (2^{n-1} - 1) \;=\; 1 \qquad (4.2.4.13)$$

Hence:

$$\lim_{n \to \infty} E[payoff(n)] \;=\; \sum_{n=1}^{\infty} \frac{1}{2^{n}} \;=\; 2 \qquad (4.2.4.14)$$

But, if allowing to rule also the stakes, one can violate even the Weak Law of Excluded Gambling Systems, why don't Casinos go all in ruin?

The reason is that a gambling strategy as the displayed martingale requires an unbounded budget, i.e. that the gambler cannot go broke.

4.3 The weakness of Church randomness with respect to Chaitin randomness

The Law of Excluded Classical Gambling System could be seen, at a foundational level, as the corner stone for a mathematical characterization of the concept of classical algorithmic randomness.

With the intuitivelly compelling choice of eq.4.2.4.8 for the class of admissible gammblig strategies, this results in the notion of Church randomness introduce in the previous section.

It appears then natural to ask ourselves which inter-relation exists between the resulting notion of Church randomness and the notion of Martin-Löf Solovay Chaitin randomness we have arrived to recognize as the correct notion of classical algorithmic randomness.

We stressed in the remark3.3.1 the importance of the fact that $P_{unbaised}(CHAITIN-RANDOM(\Sigma^{\infty})) = 1$.

So we can appreciate the fact that:

Theorem 4.3.1

THE OCCURED SEQUENCE OF INFINITE INDEPENDENT TOSSES OF A FAIR COIN IS CERTAINLY CHURCH-RANDOM

$$P_{unbaised}(CHURCH-RANDOM(\Sigma^{\infty})) = 1 \quad (4.3.4.1)$$

PROOF:

Given a generic $S \in \Delta_0^0 - \overset{\circ}{MAP} (\Sigma^{\star}, \{0,1\})$ let us consider the unary predicate **failure of the gambling-system S** $p_{failure\ gambling-system\ S} \in \mathcal{P}(\Sigma^{\infty})$ defined as:

$$p_{failure\ gambling-system\ S}(\bar{x}) := << \lim_{n \rightarrow \infty} \frac{N_i(EXT[S](\vec{x})(n))}{n} = \lim_{n \rightarrow \infty} \frac{N_i(\vec{x}(n))}{n} \quad i \in \Sigma >> \quad (4.3.4.2)$$

The thesis follows immediately by the observation that:

$$p_{failure\ gambling-system\ S} \in \mathcal{P}_{TYPICAL}(\Sigma^{\infty}) \quad \forall S \in \Delta_0^0 - \overset{\circ}{MAP} (\Sigma^{\star}, \{0,1\}) \quad (4.3.4.3)$$

■

Let us , now, observe that:

Theorem 4.3.2

$$CHURCH-RANDOM(\Sigma^{\infty}) \subseteq CHAITIN-RANDOM(\Sigma^{\infty}) \quad (4.3.4.4)$$

PROOF:

The generic predicate $p_{failure\ gambling-system\ S}$ is effectively-refutable. Together with theorem4.3.1 this implies that:

$$p_{failure\ gambling-system\ S} \in \mathcal{L}_{RANDOMNESS}[(\Sigma^{\infty}, P_{unbiased})] \ \forall S \in \Delta_0^0 - \overset{\circ}{MAP}(\Sigma^{\star}, \{0,1\}) \tag{4.3.4.5}$$

from which the the thesis follows immediately ■

Church randomness is, anyway, weaker than Martin-Löf-Solovay-Chaitin randomness as it was proved by J. Ville in 1939. Demanding to the wonderful Michael Van Lambalgen's dissertation thesis [Lam87] (in particular to the section2.6 for an hystorical analysis of the decline of von Mises axiomatization of Classical Probability Theory after the Geneva conference of 1937, and the collection of objection , both philosophical and formal, it received by Frechet, to section3.1 for a deep analysis of the philosophical differences between Church randomness and Martin-Löf-Solovay-Chaitin randomness and to the fourth chapter for the more advanced available analysis of the formal differences between such notions) for further information, let us simply report the statement of Ville's result:

Theorem 4.3.3

VILLE'S THEOREM:

$$\exists\ \bar{x} \in CHURCH - RANDOM(\Sigma^{\infty}) \ : \ p_{\text{infinite recurrence}}(\bar{x}) \text{ doesn't hold} \tag{4.3.4.6}$$

$$\exists\ \bar{y} \in CHURCH - RANDOM(\Sigma^{\infty}) \ : \ p_{\text{iterated logarithm}}(\bar{y}) \text{ doesn't hold} \tag{4.3.4.7}$$

Since the **infinite recurrence property** and the **iterated logarithm property** are Laws of Randomness, Ville Theorem immediately implies that:

Corollary 4.3.1

$$CHURCH - RANDOM(\Sigma^{\infty}) \ \subset \ CHAITIN - RANDOM(\Sigma^{\infty}) \tag{4.3.4.8}$$

Part III

The road for quantum algorithmic randomness

Chapter 5

The irreducibility of quantum probability both to classical determinism and to classical nondeterminism

5.1 Why to treat sequences of qubits one has to give up the Hilbert-Space Axiomatization of Quantum Mechanics

The problem of giving a mathematical foundation, i.e. a rigorous mathematical axiomatization, of Quantum Mechanics was first faced by John Von Neumann through his 1932's masterpiece [Neu83] in which he introduced Hilbert spaces, codifying the rule they play in Quantum Mechanics.

So he introduced his, nowadays standard, Hilbert space axiomatization of Quantum Mechanics, where:

DEFINITION 5.1.1

HILBERT SPACE AXIOMATIZATION OF QUANTUM MECHANICS:

any axiomatization of Quantum Mechanics assuming the following two axioms:

AXIOM 5.1.1

HILBERT-SPACE'S AXIOM ON STATES:

The **pure states** of a **quantum mechanical systems** are **rays** in an Hilbert space $\mathcal{H}$

AXIOM 5.1.2

HILBERT-SPACE'S AXIOM ON OBSERVABLES:

The **observables** of a **quantum mechanical systems** are **self-adjoint operators** on $\mathcal{H}$. The expected value of the observable $\hat{O}$ in the state $|\psi>$ is:

$$E_{|\psi>}(\hat{O}) \;=\; \frac{<\psi|\hat{O}|\psi>}{<\psi|\psi>} \qquad (5.1.5.1)$$

The success and influence of the book [Neu83] was so great that the point of view therein exposed became suddenly the *koiné* about the foundation of Quantum Mechanics, taught in all undergraduate courses.

This had the curious effect of throwing a shadow on Von Neumann's successive intellectual path that led him to doubt not only about his 1932's Hilbert space axiomatization, but of the same fact that Quantum Mechanics may be formalized through an an Hilbert space formalization of some kind.

To understand the corner-stone of Von Neumann's post-32 doubts let us consider the **Separability Issue**.

Given the many subtilities involved it is useful to recall even the more elementary notions:

DEFINITION 5.1.2

HILBERT SPACE:

a complete inner-product space

Given an Hilbert space $\mathcal{H}$ we shall say that [Sim80]:

DEFINITION 5.1.3

$\mathcal{H}$ IS SEPARABLE: it has a finite or countable orthonormal basis

Given two Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ their tensor product, i.e. the Hilbert space $\mathcal{H}_1 \bigotimes \mathcal{H}_2$ is defined in the following way [Sim80]:

1. to any couple $(|\phi_1>, |\phi_2>)$ with $|\phi_1>\in \mathcal{H}_1$ and $|\phi_2>\in \mathcal{H}_2$ one can associate the conjugate bilinear form $|\phi_1> \bigotimes |\phi_2>$ defined on $\mathcal{H}_1 \times \mathcal{H}_2$ as:

$$(|\phi_1> \bigotimes |\phi_2>)(|\psi_1>, |\psi_2>) \;:=\; <\phi_1|\psi_1><\phi_2|\psi_2> \quad |\psi_1>\in \mathcal{H}_1 \,,\, |\psi_2>\in \mathcal{H}_2 \qquad (5.1.5.2)$$

2. one considers the set $\mathcal{E}$ of the finite linear combinations of such conjugate linear forms

3. one defines on $\mathcal{E}$ an inner product $<\cdot|\cdot>$ by defining:

$$<\phi_1 \bigotimes \phi_2|\phi_3 \bigotimes \phi_4> := <\phi_1|\phi_3><\phi_2|\phi_4> \qquad (5.1.5.3)$$

and extending by linearity to $\mathcal{E}$

4. one defines $\mathcal{H}_1 \times \mathcal{H}_2$ as the completion of $\mathcal{E}$ under such an inner product

Such a definition of the tensor product of two Hilbert spaces trivially generalizes to define the tensor product $\mathcal{H}_1 \bigotimes \cdots \bigotimes \mathcal{H}_n$ of a finite number of Hilbert spaces.

In particular one can consider the case in which the Hilbert spaces $\mathcal{H}_1 , \cdots , \mathcal{H}_n$ are equal:

$$\mathcal{H}_i = \mathcal{H} \;\; i = 1, \cdots , n \tag{5.1.5.4}$$

in which the above construction results in the following:

DEFINITION 5.1.4

n-FOLD TENSOR PRODUCT OF THE HILBERT SPACE $\mathcal{H}$:

$$\mathcal{H}^{\bigotimes n} := \bigotimes_{k=1}^{n} \mathcal{H} \tag{5.1.5.5}$$

If, anyway, one tries to generalize such a procedure to define the ∞-fold tensor product $\mathcal{H}^{\bigotimes \infty}$ of an Hilbert space $\mathcal{H}$ one immediately sees that the business doesn't work [Thi83]:

the squared norm of a vector $|\psi> := |\psi_1> \bigotimes \cdots \bigotimes |\psi_n> \in \mathcal{H}^{\bigotimes n}$ is given by:

$$||\psi||^2 = <\psi|\psi> = \prod_{k=1}^{n} <\psi_k|\psi_k> \tag{5.1.5.6}$$

Now if $n = \infty$ the productory can, in general, diverge so one has to restrict only to those vectors for which the r.h.s. of eq.5.1.5.6 converges.

Furthermore, on the remaining vectors, the productory can converge to zero even in those particular cases in which $<\psi_k|\psi_k> > 0 \;\; \forall k \in \mathbb{N}$.

In order to take the quotient space with respect to the zero vectors it is then necessary to form the equivalences classes not only of vectors with some factor zero, but also containing the vectors for which $\prod_{k=1}^{n} <\psi_k|\psi_k>$ converges to zero.

On such a quotient space the eq.5.1.5.6 defines a separating norm that can be used to complete it resulting in the required Hilbert space $\mathcal{H}^{\bigotimes \infty}$, with the linear structure defined in the usual way.

This does not yet, however, suffice to define the scalar product of different vector $|\psi>$ and $|\phi>$. Though only vectors such that:

$$<\psi_k|\psi_k> = <\phi_k|\phi_k> = 1 \;\; \forall k \in \mathbb{N} \tag{5.1.5.7}$$

need to be considered, there are still two possibilities, namely:

- **CASE-I**:

$$\prod_{k=1}^{\infty} | < \psi_k | \phi_k > | \ \rightarrow \ c \ > \ 0 \tag{5.1.5.8}$$

- **CASE-II**:

$$\prod_{k=1}^{\infty} | < \psi_k | \phi_k > | \ \rightarrow \ 0 \tag{5.1.5.9}$$

where $\rightarrow$ means unconditional convergence.

In case-2 $\prod_{k=1}^{\infty} < \psi_k | \phi_k > \rightarrow \ 0$ as well, and the vectors may be considered orthogonal.

In case-II, on the other hand, there is no guarantee that $\prod_{k=1}^{\infty} < \psi_k | \phi_k >$ converges. If $| < \psi_k | \phi_k > | \ = \ \exp(i\theta_k) | < \psi_k | \phi_k > |$, then their product is said to converge if not only $\prod_{k=1}^{\infty} | < \psi_k | \phi_k > |$ but also $\sum_k |\phi_k|$ converges.

One now encounters the convention that vectors may be deemed orthogonal whenever $\sum_k |\phi_k| \ \rightarrow \ \infty$ (we will indicate this situation as the **case-I.B**)

Let us then agree on the following definition of the inner product:

DEFINITION 5.1.5

$< \psi | \phi > = \ c \neq \ 0$ (**case-I.A**)

$$\lim_{n \rightarrow \infty} < \psi_n | \phi_n > = \ c \tag{5.1.5.10}$$

DEFINITION 5.1.6

$< \psi | \phi > = \ 0$ (**case-II** or **case-I.B**))

$$\lim_{n \rightarrow \infty} < \psi_n | \phi_n > = \ 0 \tag{5.1.5.11}$$

Let us now observe that **separability** is a rather robust property, i.e. a property that preserves under many operations.

Given an Hilbert space $\mathcal{H}$:

Theorem 5.1.1

PRESERVATION OF SEPARABILITY UNDER FINITE-FOLD TENSOR PRODUCT

$$\mathcal{H} \ \text{ is separable } \quad \Rightarrow \quad (\mathcal{H}^{\bigotimes n} \ \text{ is separable } \quad \forall n \in \mathbb{N}) \tag{5.1.5.12}$$

Given a sequence of Hilbert spaces $\{\mathcal{H}_n\}_{n \in \mathbb{N}}$ we have furthermore the following:

Theorem 5.1.2

PRESERVATION OF SEPARABILITY UNDER INFINITE DIRECT SUM:

$$(\mathcal{H}_n \text{ is separable } \forall n \in \mathbb{N}) \;\Rightarrow\; \bigoplus_{n \in \mathbb{N}} \mathcal{H}_n \text{ is separable} \tag{5.1.5.13}$$

These theorems are sufficient to guarantee the separability of almost all the Hilbert spaces appearing in Theoretical Physics:

For the theorem5.1.1 this is certainly the case when, in Nonrelativistic Quantum Mechanics, one considers a finite number of particles of spin s: since the Hilbert space for one particle is $\mathcal{H} := L^2(\mathbb{R}^3\, d\vec{x}) \bigotimes \mathbb{C}^{2s+1}$, the n - particle Hilbert space is $S_n \mathcal{H}^{\bigotimes n}$ if s is integer (i.e. if the particles are **bosons**) and $A_n \mathcal{H}^{\bigotimes n}$ if s is half-integer (i.e. if the particles are **fermions**) where S_n and A_n are, respectively, the **n-simmetrization**, **n-antisimmetrization** operators.

The underlying Hilbert space continues to remain separable even allowing an infinite number of particles as follows immediately introducing the following Hilbert spaces:

DEFINITION 5.1.7

FOCK SPACE ASSOCIATED TO $\mathcal{H}$:

$$\mathcal{H}^{\bigotimes \star} := \mathcal{F}(\mathcal{H}) := \bigoplus_{n \in \mathbb{N}} \mathcal{H}^{\bigotimes n} \tag{5.1.5.14}$$

DEFINITION 5.1.8

BOSONIC FOCK SPACE ASSOCIATED TO $\mathcal{H}$:

$$\mathcal{F}_S(\mathcal{H}) := \bigoplus_{n \in \mathbb{N}} S_n \mathcal{H}^{\bigotimes n} \tag{5.1.5.15}$$

DEFINITION 5.1.9

FERMIONIC FOCK SPACE ASSOCIATED TO $\mathcal{H}$:

$$\mathcal{F}_A(\mathcal{H}) := \bigoplus_{n \in \mathbb{N}} A_n \mathcal{H}^{\bigotimes n} \tag{5.1.5.16}$$

and observing that, for $\mathcal{H} := L^2(\mathbb{R}^3\, d\vec{x}) \bigotimes \mathbb{C}^{2s+1}$, they are separable owing to theorem5.1.1 and theorem5.1.2.

Let us now pass to Relativistic Quantum Mechanics, i.e. to Quantum Field Theory:

for a free-field theory the separability of the proper Fock spaces follows again immediately from theorem5.1.1 and theorem5.1.2.

For interacting field theories the situation is more complicated owing to the fact that a general mathematically-rigorous formalization of Quantum Field Theory, beside its exceptional developments [Wit99a],[Wit99b] and all the work of the Constructivists [Jaf87], [Jaf00], is unfortunately still lacking [Wit95].

One could simply assert that Wightman Axioms constraint the underlying Hilbert space to be separable [Sim75] but such an answer would sound as a rather dogmatical one.

A more convincing argument consists in considering that in the Lehmann-Symanzik-Zimmerman formalism the involved Hilbert spaces are only the asympotic In and Out Fock spaces [Str93].

Unfortunately the robustness of **separability** is not complete.
In fact:

Theorem 5.1.3

NOT PRESERVATION OF SEPARABILITY UNDER INFINITE-FOLD TENSOR PRODUCT
$\mathcal{H}^{\bigotimes \infty}$ is not separable even if $\mathcal{H}$ is separable

Example 5.1.1

THE HILBERT SPACES OF QUANTUM INFORMATION THEORY
How much classical information is contained in a state:

$$|\psi> := \alpha|+> + \beta|-> \quad \alpha, \beta \in \mathbb{C} : |\alpha|^2 + |\beta|^2 = 1 \tag{5.1.5.17}$$

of a $spin\frac{1}{2}$ system ?
Since the bidimensional complex projective space has the continuum power:

$$cardinality(\mathbb{C}P^2) = \aleph_1 \tag{5.1.5.18}$$

the specification of a point P on it requires the assignation of a whole sequence $\bar{x}_P \in \Sigma^{\infty}$.
In this way one is led to to argue that:

$$information(|\psi>) = \infty \, bits \tag{5.1.5.19}$$

But, given a $spin\frac{1}{2}$ system prepared in the state $|\psi>$, let us now suppose to make a measurement of the operator $\hat{S}_z$. The information gained by the knowledge of the experimental outcome is only of one bit.
So, from this reasoning, one is led to argue that:

$$information(|\psi>) = 1 \, bit \tag{5.1.5.20}$$

Obviously eq.5.1.5.19 and eq.5.1.5.20 are incompatible.
This simple reasoning shows that the quantification of the informational content of the state $|\psi>$ must be given in terms of a measure's unity not commensurable with that of **classical information**.
This is a a conceptually extremelly deep concept: there doesn't exist a unique, mathematically charaterizable, notion of information, resulting in a measure's unity , the **bit**, in terms of which one can analyze the informational content of both classical and quantum physical systems:
quantum information is not commensurable with **classical information**.
Hence one has to give up the universal notion of **bit**, replacing it with the following couple of notions:

- the **cbit**, i.e. the measure's unity of **classical information**
- the **qubit**, i.e. the measure's unity of **quantum information**

The quantum-informational amount of the state $|\psi>$ gives the operational definition of the **qubit**.

A more formal definition will be given, anyway, in the remark5.1.9 in terms of the notion of **combinatorial quantum information**.

As we will see in section7.3 the incommensurability of **classical information** and **quantum information** is deeply linked with the No-Cloning Theorem

DEFINITION 5.1.10

ONE QUBIT HILBERT SPACE:

$$\mathcal{H}_2 \; := \; \mathbb{C}^2 \tag{5.1.5.21}$$

Given an $n \in \mathbb{N}$:

DEFINITION 5.1.11

n QUBITS HILBERT SPACE:

$$\mathcal{H}_2^{\bigotimes n} \; := \; \mathbb{C}^{2^n} \tag{5.1.5.22}$$

DEFINITION 5.1.12

HILBERT SPACE OF QUBITS' STRINGS:

$$\mathcal{H}_2^{\bigotimes \star} \; := \; \mathcal{F}(\mathcal{H}_2) \tag{5.1.5.23}$$

On all these **separable** Hilbert spaces it is useful to introduce orthonormal complete bases, said the **computational basis** that embeds the strings of cbits in the quantum domain:

DEFINITION 5.1.13

COMPUTATIONAL BASIS OF $\mathcal{H}_2$:

$$\mathbb{E}_2 \; := \; \{|0>, |1>\} \; : \; |0> := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \; , \; |1> := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{5.1.5.24}$$

Remark 5.1.1

ON THE QUBIT OPERATOR

The adoption of the **computational language** requires some caution.

As to definition5.1.13, it is only a renaming of the usual language of spin 1/2 system:

$$|0> \; := \; |\uparrow_z> \tag{5.1.5.25}$$
$$|1> \; := \; |\downarrow_z> \tag{5.1.5.26}$$
$$\tag{5.1.5.27}$$

The correspondence clearly continues considering the projectors:

$$|0><0| \; = \; \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \; = \; \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \; = \; |\uparrow_z><\uparrow_z| \tag{5.1.5.28}$$

$$|1><1| \; = \; \begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \; = \; \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \; = \; |\downarrow_z><\downarrow_z| \tag{5.1.5.29}$$

The problem arises if one tries to introduce a **qubit operator** having the binary alphabet $\Sigma := \{0, 1\}$ as eigenvalues;

in fact,owing to the vanishing of the addendum concerning the zero eigenvalue, one has obviously that:

$$\hat{q} \; := \; 0\,|0><0| \; + \; 1\,|1><1| \; = \; |1><1| \; = \; |\downarrow_z><\downarrow_z| \tag{5.1.5.30}$$

So, in order of introducing a qubit operator, one has to avoid the zero eigenvalue, e.g. assuming the spectrum of the **qubit operator** to be the binary alphabet $\{+1, -1\}$, with the convention that the eigenvalue $+1$ corresponds to zero and the eigenvalue -1 corresponds to one.

With these conventions one has that:

$$\hat{q} \; := \; +1\,|0><0| \; + \; (-1)\,|1><1| \; = \; \hat{\sigma}_z \; = \; \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{5.1.5.31}$$

Given any positive integer number $n \geq 3$:

DEFINITION 5.1.14

COMPUTATIONAL BASIS OF $\mathcal{H}_2^{\bigotimes n}$:

$$\mathbb{E}_n \; := \; \{ \, |\vec{x}> , \, \vec{x} \in \Sigma^n \, \} \tag{5.1.5.32}$$

DEFINITION 5.1.15

COMPUTATIONAL BASIS OF $\mathcal{H}_2^{\bigotimes \star}$:

$$\mathbb{E}_\star \; := \; \{ |\vec{x}> , \, \vec{x} \in \Sigma^\star \, \} \tag{5.1.5.33}$$

The generic **string of qubits**, i.e. the generic vector of $\mathbb{H}_2^{\bigotimes \star}$ is then given by a linear combination of the form $\sum_{\vec{x} \in \Sigma^\star} c_{\vec{x}} |\vec{x}>$.

And what about **sequences of qubits**?

We can indeed introduce the following notions:

DEFINITION 5.1.16

HILBERT SPACE OF QUBITS' SEQUENCES:

$$\mathcal{H}_2^{\bigotimes \infty} := \bigotimes_{n \in \mathbb{N}} \mathcal{H}_2 \tag{5.1.5.34}$$

By theorem5.1.3 $\mathcal{H}_2^{\bigotimes \infty}$ is not separable.

The **Separability Issue** consists in the following question:

is it necessary to modify the axiom5.1.1 adding the constraint that the Hilbert space $\mathcal{H}$ is separable?

The thesis that the correct answer is affermative has been asserted by authoritative voices; for example Walter Thirring remembers that [Thi01]:

"For finite tensor products the dimension of the spaces is multiplicative and for infinite tensor product is is uncountable even if the individual spaces have only dimension = 2. This casts some doubt on whether there is a mathematically valid description of infinite quantum systems. Schrödinger once told me that the corresponding non-separable Hilbert space did not make sense to him. To determine N components of his ψ-function one needs N experiments and in a non-separable space one would need an uncountable number of measurements and this is nonsense. However such an opinion means that Schrödinger did not get the main message of Von Neumann's celebrated paper on infinite tensor products ."

Keeping aside for a moment Thirring's last remark, let us observe that there exist also many other arguments supporting a positive answer to the **Separability Issue**: for example on an not-separable Hilbert space the Gram-Schmidt orthogonalization process can be adopted only appealing to the Axiom of Choice [Sim75].

But let us now analyze Thirring's last remark: is Thirring right in claiming that Von Neumann's celebrated paper on infinite tensor products lead to give a negative answer to the Separability Issue?

Our point of view, though predictively completelly equivalent to Thirring's authoritative one, is philosophically different and lead, as to the Separability Issue, to the opposite answer, as we will arrive to discuss at the end of this section.

To show why, anyway, it may be useful to follow the reconstruction of Von Neumann's intellectual path on the Foundations of Quantum Physics made by Miklos Redei in [Red98], emerging from and condensated in [Red01]:

Hilbert spaces $\rightarrow$ orthocomplemented modular lattices $\rightarrow$ $W^{\star}$-algebras

that, as we will show, correspond conceptually to the path:

Quantum Mechanics $\rightarrow$ Quantum Logic $\rightarrow$ Quantum Probability

This requires , anyway the introduction of a whole abstract algebraic machinery.

DEFINITION 5.1.17

PARTIALLY ORDERED SET (POSET)

a couple $(\mathcal{L}\,,\,\preceq)$ such that $\mathcal{L}$ is a set, while $\leq$ is a partial ordering on $\mathcal{L}$, i.e. a reflexive, transitive, antisimmetric relation on $\mathcal{L}$

Given a poset $(\mathcal{L}\,,\,\preceq)$ and two element $a, b \in \mathcal{L}$:

DEFINITION 5.1.18

$$a \prec b \;:=\; (a \preceq b)\, and\, a \neq b \tag{5.1.5.35}$$

DEFINITION 5.1.19

$$a \succ b \;:=\; (a \succeq b)\, and\, a \neq b \tag{5.1.5.36}$$

Given a set $S \subseteq \mathcal{L}$:

DEFINITION 5.1.20

a IS AN UPPER BOUND OF S IN THE POSET $(\mathcal{L}\,,\,\preceq)$:

$$b \;\preceq a \;\; \forall b \in S \tag{5.1.5.37}$$

DEFINITION 5.1.21

a IS A LOWER BOUND OF S IN THE POSET $(\mathcal{L}\,,\,\preceq)$:

$$b \;\succeq a \;\; \forall b \in S \tag{5.1.5.38}$$

DEFINITION 5.1.22

a IS THE LEAST UPPER BOUND OF S IN THE POSET $(\mathcal{L}\,,\,\preceq)$:

$$b \;\preceq a \;\; \forall b \text{ upper bound of S in } (\mathcal{L}\,,\,\leq) \tag{5.1.5.39}$$

DEFINITION 5.1.23

a IS THE LEAST LOWER BOUND OF S IN THE POSET $(\mathcal{L}\,,\,\preceq)$:

$$b \;\succeq\; a \;\; \forall b \text{ lower bound of S in } (\mathcal{L}\,,\,\leq) \tag{5.1.5.40}$$

DEFINITION 5.1.24

LATTICE:
a poset $(\mathcal{L}, \preceq)$ such that:

$$\forall a, b \in \mathcal{L} \, , \, \exists a \bigvee b := \text{ least upper bound of } \{a, b\} \text{ in } \mathcal{L} \tag{5.1.5.41}$$

$$\forall a, b \in \mathcal{L} \, , \, \exists a \bigwedge b := \text{ greatest lower bound of } \{a, b\} \text{ in } \mathcal{L} \tag{5.1.5.42}$$

$$\exists \, 0_{\mathcal{L}} \in \mathcal{L} \; : \; 0_{\mathcal{L}} \preceq a \;\; \forall a \in \mathcal{L} \tag{5.1.5.43}$$

$$\exists \, 1_{\mathcal{L}} \in \mathcal{L} \; : \; a \preceq 1_{\mathcal{L}} \;\; \forall a \in \mathcal{L} \tag{5.1.5.44}$$

Given a lattice $(\mathcal{L}, \preceq)$:

DEFINITION 5.1.25

$a \in \mathcal{L}$ IS AN ATOM OF $(\mathcal{L}, \preceq)$:

$$b \preceq a \; \Rightarrow \; b = a \, or \, b = 0_{\mathcal{L}} \tag{5.1.5.45}$$

DEFINITION 5.1.26

$(\mathcal{L}, \preceq)$ IS ATOMIC:

$$\forall b \in \mathcal{L} \; \exists b \in \mathcal{L} \; atom \; : \; a \preceq b \tag{5.1.5.46}$$

DEFINITION 5.1.27

LOGICAL DIMENSION FUNCTION ON $(\mathcal{L}, \preceq)$:
a function $d \, : \, \mathcal{L} \mapsto [0, +\infty]$ such that:

$$a \preceq b \; \Rightarrow \; d(a) \leq d(b) \;\; \forall a, b \in \mathcal{L} \tag{5.1.5.47}$$

$$d(a) + d(b) = d(a \bigwedge b) + d(a \bigvee b) \;\; \forall a, b \in \mathcal{L} \tag{5.1.5.48}$$

DEFINITION 5.1.28

$(\mathcal{L}, \preceq)$ IS DISTRIBUTIVE:

$$a \bigvee (b \bigwedge c) = (a \bigvee b) \bigwedge (a \bigvee c) \;\; \forall a, b, c \in \mathcal{L} \tag{5.1.5.49}$$

DEFINITION 5.1.29

$(\mathcal{L}, \preceq)$ IS MODULAR:

$$a \preceq b \; \Rightarrow \; a \bigvee (b \bigwedge c) = (a \bigvee b) \bigwedge (a \bigvee c) \;\; \forall a, b, c \in \mathcal{L} \tag{5.1.5.50}$$

DEFINITION 5.1.30

ORTHOCOMPLEMENTATION ON $(\mathcal{L}, \preceq)$:
a map $\perp : \mathcal{L} \mapsto \mathcal{L}$ such that:

$$(a^{\perp})^{\perp} = a \;\; \forall a \in \mathcal{L} \tag{5.1.5.51}$$

$$a \preceq b \; \Rightarrow \; b^{\perp} \preceq a^{\perp} \;\; \forall a, b \in \mathcal{L} \tag{5.1.5.52}$$

$$a \bigwedge a^{\perp} = 0_{\mathcal{L}} \;\; \forall a \in \mathcal{L} \tag{5.1.5.53}$$

$$a \bigvee a^{\perp} = 1_{\mathcal{L}} \;\; \forall a \in \mathcal{L} \tag{5.1.5.54}$$

DEFINITION 5.1.31

ORTHOCOMPLEMENTED LATTICE:

a therne $((\mathcal{L}, \preceq, \perp)$ such that $(\mathcal{L}, \preceq)$ is a lattice while $\perp$ is an orthocomplementation on $(\mathcal{L}, \preceq)$

Given an orthocomplemented lattice $((\mathcal{L}, \preceq, \perp)$ an two its elements $a, b \in \mathcal{L}$

DEFINITION 5.1.32

a IS ORTHOGONAL TO B:

$$a \perp b := a \preceq b^{\perp} \tag{5.1.5.55}$$

Clearly, by the definition5.1.30, one has that orthogonality is a simmetric relation:

$$a \perp b \Leftrightarrow b \perp a \ \forall a, b \in \mathcal{L} \tag{5.1.5.56}$$

DEFINITION 5.1.33

$((\mathcal{L}, \preceq, \perp)$ IS ORTHOMODULAR:

$$a \preceq b \, and \, a \perp c \Rightarrow a \bigvee (b \bigwedge c) = (a \bigvee b) \bigwedge (a \bigvee c) \ \forall a, b, c \in \mathcal{L} \tag{5.1.5.57}$$

Orthomodularity is a weakening of modularity that is a weakening of distributivity as is stated by the following:

Theorem 5.1.4

$$distributivity \Rightarrow modularity \Rightarrow orthomodularity \tag{5.1.5.58}$$

$$orthomodularity \nRightarrow modularity \nRightarrow distributivity \tag{5.1.5.59}$$

We will soon see the utility of the following:

Theorem 5.1.5

THEOREM ON THE FINITE DIMENSION:

HP:

$$(\mathcal{L}, \preceq) \ lattice$$

$$\exists d \text{ logical dimension function } : \infty \notin Range(d)$$

TH:

$\mathcal{L}$ is modular

In a fundamental 1936's paper with G. Birkhoff [vN95], Von Neumann suggested the idea, yet implicitely advanced in the fifth section of the third chapter of [Neu83], that the difference between Quantum Mechanics and Classical Mechanics could be ascribed to the fact the algebraic structure of the set of all the propositions concerning a quantum system violates the laws of Classical Logic, obeying a new kind of logic.

This was the seed of the 65 year old research-field of Quantum Logic.

It must be remarked that the original Birkhoff and Von Neumann's definition of a quantum logic was more restrictive than that choram-populi later assumed in such a research field; to distinguish the two notion we will speak, respectively, of weak and strong quantum logics.

Anyway, exactly as the Theoretical Physicist's community foxilized on the 1932's snapshot of Von Neumann's intellectual path, the same happened to the Quantum Logicist's community that foxilized on the 1936's snapshot (mostly altering it), so don't catching all the reasons led Von Neumann to make the phase-transition:

$$\text{Quantum Logic} \rightarrow \text{Quantum Probability}$$

that, as we will briefly point in section5.2, can be seen as the starting point of the of the open intellectual challenge summarized by the path:

Quantum Mechanics as Nondistributive Logic $\rightarrow$ Quantum Mechanics as Noncommutative Probability $\rightarrow$ Quantum Mechanics as Noncommutative Geometry

The difference between Classical Logic and Quantum Logic is enclosed in the different algebraic structure that the set of all the propositions concerning a physical system obey as far as the **conjunction** $\bigwedge$, **disjunction** $\bigvee$ and **negation** $'$ are concerned:

DEFINITION 5.1.34

CLASSICAL LOGIC:
a **distributive**, **orthocomplemented** lattice

DEFINITION 5.1.35

STRONG QUANTUM LOGIC:
a **modular**, **orthocomplemented** lattice

DEFINITION 5.1.36

WEAK QUANTUM LOGIC:
an **orthomodular**, **orthocomplemented** lattice

Example 5.1.2

THE CLASSICAL LOGIC OF POWER-SETS

Given an arbitrary set S let us introduce on its power-set 2^S the partial-ordering relation:

$$a \preceq b \; := \; a \subseteq b \;\; a, b \in 2^S \tag{5.1.5.60}$$

It may be easily verified that $(2^S, \preceq)$ is a lattice, with:

$$a \bigwedge b \; := \; a \bigcap b \;\; \forall a, b \in 2^S \tag{5.1.5.61}$$

$$a \bigvee b \; := \; a \bigcup b \;\; \forall a, b \in 2^S \tag{5.1.5.62}$$

$$0_{2^S} \; = \; \emptyset \tag{5.1.5.63}$$

$$1_{2^S} \; = \; 2^S \tag{5.1.5.64}$$

Introduced on $(2^S, \preceq)$ the orthocomplementation map $\perp \; : \; 2^S \mapsto 2^S$:

$$a^{\perp} \; := \; S \; - \; a \;\; a \in 2^S \tag{5.1.5.65}$$

$(2^S \, , \, \preceq \, , \, \perp)$ is a classical logic.

If $cardinality(S) \; \in \; \mathbb{N}$ the map $d : 2^S \mapsto \mathbb{R}_+$ defined as:

$$d(S) \; := \; cardinality(S) \tag{5.1.5.66}$$

is a logical dimension function.

This is not the case, anyway, if $cardinality(S) \; \geq \; \aleph_0$, even generalizing definition5.1.27 in order of allowing infinite cardinal values of a logical dimension function, as can be seen, for example, observing that:

$$\mathbb{Z} \; \preceq \; \mathbb{Q} \; but \; cardinality(\mathbb{Z}) \; = \; cardinality(\mathbb{Q}) \; = \; \aleph_0 \tag{5.1.5.67}$$

$$\mathbb{R} - \mathbb{Q} \; \preceq \; \mathbb{R} \; but \; cardinality(\mathbb{R} - \mathbb{Q}) \; = \; cardinality(\mathbb{R}) \; = \; \aleph_1 \tag{5.1.5.68}$$

Example 5.1.3

THE STRONG QUANTUM LOGIC OF THE n-QUBITS HILBERT SPACE

Given the n-qubits Hilbert space $\mathcal{H}_2^{\bigotimes n}$ let us consider its **projective geometry**, i.e. the set $\mathcal{L}(\mathcal{H}_2^{\bigotimes n})$ of all its linear subspaces:

$$\mathcal{L}(\mathcal{H}_2^{\bigotimes n}) \; := \; \bigcup_{k=0}^{2^n} G_{k,2^n}(\mathbb{C}) \tag{5.1.5.69}$$

Introduced on $\mathcal{L}(\mathcal{H}_2^{\bigotimes n})$ the partial ordering relation:

$$a \preceq b \; := \; a \subseteq b \;\; a, b \in \mathcal{L}(\mathcal{H}_2^{\bigotimes n}) \tag{5.1.5.70}$$

the poset $(\mathcal{L}\,,\,\preceq)$ is an atomic lattice, with:

$$a \bigwedge b \;:=\; a \bigcap b \;\; a, b \in \mathcal{L}(\mathcal{H}_2^{\bigotimes n}) \tag{5.1.5.71}$$
$$a \bigvee b \;:=\; a \bigoplus b \;\; a, b \in \mathcal{L}(\mathcal{H}_2^{\bigotimes n}) \tag{5.1.5.72}$$
$$\tag{5.1.5.73}$$

whose atoms are the one-dimensional subspaces, namely the elements of $G_{1,2^n}(\mathbb{C}) = \mathbb{C}P^{2^n-1}$, said the **points** of the **projective geometry**, i.e. the **rays** of $\mathcal{H}_2^{\bigotimes n}$.

It may be easily verified that the following map:

$$d(a) \;:=\; dim(a) \;\; a \in \mathcal{L}(\mathcal{H}_2^{\bigotimes n}) \tag{5.1.5.74}$$

is a logical dimension function. Since:

$$\infty \;\notin\; Range(d) \;=\; \{0, 1, \cdots, 2^n\} \tag{5.1.5.75}$$

it follows by theorem5.1.5 that $(\mathcal{L}\,,\,\preceq)$ is modular.

So, introduced on $(\mathcal{L}(\mathcal{H}_2^{\bigotimes n})\,,\,\preceq)$ the orthocomplementation map:

$$a^{\perp} \;:=\; \{|\psi_1> \in \mathcal{H}_2^{\bigotimes n} \; : < \psi_1|\psi_2> = 0 \; \forall |\psi_2> \in \; a\} \;\; a \in \mathcal{L}(\mathcal{H}_2^{\bigotimes n}) \tag{5.1.5.76}$$

$((\mathcal{L}(\mathcal{H}_2^{\bigotimes n})\,,\,\preceq\,,\,\perp)$ is a strong quantum logic.

Example 5.1.4

THE WEAK QUANTUM LOGIC OF THE QUBITS' STRINGS HILBERT SPACE

Given the qubits' strings Hilbert space $\mathcal{H}_2^{\bigotimes \star}$ let us consider the set $\mathcal{L}(\mathcal{H}_2^{\bigotimes \star})$ of all its closed linear subspaces.

Introduced on $\mathcal{L}(\mathcal{H}_2^{\bigotimes n})$ the partial ordering relation of example5.1.3:

$$a \preceq b \;:=\; a \subseteq b \;\; a, b \in \mathcal{L}(\mathcal{H}_2^{\bigotimes \star}) \tag{5.1.5.77}$$

the poset $(\mathcal{L}\,,\,\preceq)$ is again an atomic lattice with atoms the **rays** of $\mathcal{H}_2^{\bigotimes \star}$.

As in example5.1.3 the following map:

$$d(a) \;:=\; dim(a) \;\; a \in \mathcal{L}(\mathcal{H}_2^{\bigotimes \star}) \tag{5.1.5.78}$$

is a logical dimension function. But since now:

$$\infty \;=\; dim(\mathcal{H}_2^{\bigotimes \star}) \;\in\; Range(d) \;=\; \{0, 1, \cdots, \infty\} \tag{5.1.5.79}$$

we can't apply theorem5.1.5 anymore.

Indeed it may be proved that the lattice $(\mathcal{L}(\mathcal{H}_2^{\bigotimes \star})$ is not modular but only orthomodular.

So, introduced on $(\mathcal{L}(\mathcal{H}_2^{\bigotimes \star}) \, , \, \preceq)$ the orthocomplementation map:

$$a^{\perp} \, := \, \{ |\psi_1 > \in \mathcal{H}_2^{\bigotimes \star} \, : < \psi_1 | \psi_2 >= 0 \, \forall | \psi_2 > \in \, a \} \;\; a \in \mathcal{L}(\mathcal{H}_2^{\bigotimes \star}) \quad (5.1.5.80)$$

$((\mathcal{L}(\mathcal{H}_2^{\bigotimes \star}) \, , \, \preceq \, , \, \perp)$ is a not a strong quantum logic but only a weak quantum logic.

The situation delineated by example5.1.3 and example5.1.4 is a particular case of Hilbert lattices' theory.

Given an arbitrary Hilbert space $\mathcal{H}$:

DEFINITION 5.1.37

HILBERT LATTICE OF $\mathcal{H}$:

the orthocomplemented lattice $(\mathcal{L}(\mathcal{H}) \, , \, \preceq \, , \, \perp)$ where, as usual, $\mathcal{L}(\mathcal{H})$ is the set of all the closed linear subspaces of $\mathcal{H}$, and:

$$a \preceq b \, := \, a \subseteq b \;\; a, b \in \mathcal{L}(\mathcal{H}) \quad (5.1.5.81)$$

$$a^{\perp} \, := \, \{ |\psi_1 > \in \mathcal{H} \, : < \psi_1 | \psi_2 >= 0 \, \forall | \psi_2 > \in \, a \} \;\; a \in \mathcal{L}(\mathcal{H}) \quad (5.1.5.82)$$

$$(5.1.5.83)$$

Theorem 5.1.6

$$(\mathcal{L}(\mathcal{H}) \, , \, \preceq \, , \, \perp) \text{ is a weak quantum logic} \quad (5.1.5.84)$$

$$(\mathcal{L}(\mathcal{H}) \, , \, \preceq \, , \, \perp) \text{ is a strong quantum logic} \;\; \Leftrightarrow \; dim(\mathcal{H}) < \infty \quad (5.1.5.85)$$

Theorem5.1.6 can be applied also to the qubit sequences' Hilbert space $\mathcal{H}_2^{\bigotimes \star}$ to infer that $(\mathcal{L}(\mathcal{H}_2^{\bigotimes \star}) \, , \, \preceq \, , \, \perp)$ is a weak quantum logic.

But here comes the great conceptual shock, to prepare which, let us observe, first of all, that the **Separability Issue** and Thirring's claim that Schrodinger negative answer to it was owed to a not-comprehension of Von Neumann's paper (written with J. Murray) on infinite tensor product clashes with the Von Neumann's 1936-dated confession to Birkhoff (partially reprinted in the paragraph7.1.2 of [Red98]):

"I would like to make a confession which may seem immoral: I do not believe absolutely in Hilbert spaces any more. After all Hilbert space (as far as quantum mechanical things are concerned) was obtained by generalizing Euclidean space, footing on the principle of 'conserving the validity al all formal rules'. $\cdots$ Now we begin to believe that it is not the vectors which matter, but the lattice of all linear (closed) subspaces. Because

1. *The vectors ought to represent the physical states, but they do it redundantly, up to a complex factor only,*
2. *and besides, the states are merely a derived notion, the primitive (phenomenologically given) notions being the qualities which correspond to the linear closed subspaces*

But if we wish to generalize the lattice of all linear closed subspaces from a Euclidean space to infinitely many dimensions, then one does not obtain Hilbert space, but the configuration which Murray and I called the 'case II_1'.(The lattice of all linear closed subspace of Hilbert space is our 'I_∞' case)"

What is Von Neumann speaking about?

To answer this question it is necessary to introduce some notion concerning $W^\star$-algebras; demanding to the immense literature (e.g. [Sun87], [Rin97a], [Rin97b], [Sak98], [BR92] from the purely mathematical side, to [Thi81], [Thi83], [Sim93], [Rob87], [Rob97], [Con94], [Rue99] for physically motivated treatment or to the reviews [Red95], [Kad01] if you want to survive the experience) for any further C_Φ-information we will here briefly recall the basic facts:

DEFINITION 5.1.38

ALGEBRA:
a couple (A , $\circ$) such that:

- A is as linear space on the complex field $\mathbb{C}$
- $\circ A \times A \to A \ \ (a,b) \to ab \equiv a \circ b$:

$$(ab)c = a(bc) \ \forall a,b,c \in A \tag{5.1.5.86}$$
$$(a+b)+c = a+(b+c) \ \forall a,b,c \in A \tag{5.1.5.87}$$
$$\exists I \in A : aI = Ia \ \forall a \in A \tag{5.1.5.88}$$

DEFINITION 5.1.39

INVOLUTIVE ALGEBRA ($\star - ALGEBRA$):
a couple (A , $\star$) such that:

- A is an algebra
- $\star : A \to A$ is an involution on A, i.e.:

$$(a^\star)^\star = a \ \forall a \in A \tag{5.1.5.89}$$
$$(a+\lambda b)^\star = a^\star + \lambda^\star b^\star \ \ \forall a,b \in A \, \forall \lambda \in \mathbb{C} \tag{5.1.5.90}$$
$$(ab)^\star = b^\star a^\star \ \ \forall a,b \in A \tag{5.1.5.91}$$

Given a $\star - algebra$ A:

DEFINITION 5.1.40

UNITARY GROUP OF A:

$$\mathcal{U}(A) := \{u \in A : uu^\star = u^\star u = I\} \tag{5.1.5.92}$$

DEFINITION 5.1.41

POSITIVE PART OF A:

$$A_+ \;:=\; \{a \in A \,:\, a = bb^\star \, b \in A\} \tag{5.1.5.93}$$

DEFINITION 5.1.42

SELF-ADJOINT PART OF A:

$$A_{sa} \;:=\; \{a \in A \,:\, a^\star = a\} \tag{5.1.5.94}$$

DEFINITION 5.1.43

SET OF THE PROJECTIONS OF A:

$$\mathcal{P}(A) \;:=\; \{a \in A \;:\, a = a^\star = a^2\} \tag{5.1.5.95}$$

Given an algebra A:

DEFINITION 5.1.44

NORM ON A:
a map $\| \cdot \| \,:\, A \rightarrow \mathbb{R}_+$ such that:

$$\|a\| \;\geq 0 \;\; \forall a \in A \tag{5.1.5.96}$$

$$\|a\| \;= 0 \;\Leftrightarrow a = 0 \;\; \forall a \in A \tag{5.1.5.97}$$

$$\|\lambda a\| \;= |\lambda| \|a\| \quad \forall a \in A \, \forall \lambda \in \mathbb{C} \tag{5.1.5.98}$$

$$\|a + b\| \leq \|a\| + \|b\| \;\; \forall a, b \in A \tag{5.1.5.99}$$

DEFINITION 5.1.45

NORMED ALGEBRA:
a couple (A , $\| \cdot \|$) such that:

- A is an algebra
- $\| \cdot \|$ is a norm on A :

$$\|ab\| \;\leq\; \|a\| \, \|b\| \;\; \forall a, b \in A \tag{5.1.5.100}$$

DEFINITION 5.1.46

BANACH ALGEBRA:
a normed algebra $(A \,, \| \cdot \|)$ such that A is complete w.r.t. $\| \cdot \|$

DEFINITION 5.1.47

BANACH INVOLUTIVE ALGEBRA ($B^\star - ALGEBRA$):
a couple (A , $\star$) such that:

- A is a Banach algebra

- $\star$ is an involution on A such that:

$$\|a^\star\| \;=\; \|a\| \;\; \forall a \in A \tag{5.1.5.101}$$

DEFINITION 5.1.48

$C^\star - ALGEBRA$:
a Banach $\star - algebra$ A such that:

$$\|a^\star a\| \;=\; \|a\|^2 \;\; \forall a \in A \tag{5.1.5.102}$$

Given a $C^\star$-algebra A:

DEFINITION 5.1.49

SPECTRUM OF $a \in A$:

$$Sp(a) \;:=\; \mathbb{C} \;-\; \{z \in \mathbb{C} \,:\, \exists (a-z)^{-1} \in A\} \tag{5.1.5.103}$$

DEFINITION 5.1.50

PART WITH DISCRETE SPECTRUM OF A:

$$A_{p.s.d} \;:=\; \{a \in A \,:\, cardinality(Sp(a)) \;\leq\; \aleph_0\} \tag{5.1.5.104}$$

DEFINITION 5.1.51

LINEAR FUNCTIONAL ON A:

$$\begin{aligned} \varphi \,:\, A \rightarrow \mathbb{C} \\ \varphi(\lambda a + \mu b) \;=\; \lambda\varphi(a) + \mu\varphi(b) \;\; \forall a, b \in A \,,\, \forall \lambda, \mu \in \mathbb{C} \end{aligned} \tag{5.1.5.105}$$

DEFINITION 5.1.52

DUAL OF A:

$$A^\star \;:=\; \{\varphi \,:\; \text{linear functional on A}\} \tag{5.1.5.106}$$

The dual $A^\star$ of a $C^\star$-algebra A is itself a normed space w.r.t the following norm:

DEFINITION 5.1.53

NORM OF $\varphi \in A^\star$

$$\|\varphi\| \;:=\; \varphi(I) \tag{5.1.5.107}$$

DEFINITION 5.1.54

POSITIVE LINEAR FUNCTIONALS ON a:

$$A^\star_+ \;:=\; \{\varphi(a^\star a) \;\geq\; 0 \;\; \forall a \in A\} \tag{5.1.5.108}$$

DEFINITION 5.1.55

STATES ON A:

$$S(A) \ = \ \{\omega \in A^{\star}_{+} \, : \, \|\omega\| = 1 \, \} \tag{5.1.5.109}$$

DEFINITION 5.1.56

THE STATE $\omega \in S(A)$ IS MIXED:

$$\exists \, \lambda \in (0,1) \, , \, \exists \omega_1, \omega_2 \in S(A) : \\ \omega_1 \neq \omega_2 \; e \; \omega = \lambda \omega_1 + (1-\lambda) \omega_2 \tag{5.1.5.110}$$

DEFINITION 5.1.57

PURE STATES OF A:

$$\Xi(A) \ \equiv \ \{ \omega \ \in \ S(A) \, : \, \omega \ \text{is not mixed} \ \} \tag{5.1.5.111}$$

A useful property we shall use in the sequel is the following:

Theorem 5.1.7

CAUCHY-SCHWARZ INEQUALITY:

$$|\omega(b^{\star} a)|^2 \ \leq \ \omega(b^{\star} b) \, \omega(a^{\star} a) \ \ \forall a, b \in A \, , \, \forall \omega \in S(A) \tag{5.1.5.112}$$

Given a $C^{\star}$-algebra A let us consider the set of all the linear functionals over $A^{\star}$, namely the dual of the dual $A^{\star\star}$.

Since an element of A $a \in A$ may be identified with the following linear function over $A^{\star}$:

$$a(\varphi) \ := \ \varphi(a) \ \ \varphi \in A^{\star} \tag{5.1.5.113}$$

it follows that:

$$A \ \subseteq \ A^{\star\star} \tag{5.1.5.114}$$

DEFINITION 5.1.58

$W^{\star}$-TOPOLOGY ON $A^{\star}$:

the coarsest topology on $A^{\star}$ w.r.t. which all the elements of A (seen as linear functionals over $A^{\star}$) are continuous

Given two $C^{\star} - algebras$ A and B :

DEFINITION 5.1.59

INVOLUTIVE MORPHISM ($\star$-MORPHISM) FROM A TO B:

a map $\tau : A \rightarrow B$ such that:

$$\tau(\lambda a + \mu b) \ = \lambda \tau(a) + \mu \tau(b) \ \ \forall a, b \in A \, , \, \forall \lambda, \mu \in \mathbb{C} \tag{5.1.5.115}$$

$$\tau(ab) \ = \tau(a) \tau(b) \ \ \forall a, b \in A \tag{5.1.5.116}$$

$$\tau(a^{\star}) \ = \tau(a)^{\star} \ \ \forall a \in A \tag{5.1.5.117}$$

DEFINITION 5.1.60

INVOLUTIVE ISOMORPHISM ($\star$-ISOMORPHISM) FROM A TO B:
an involutive morphism $\tau : A \to B$ that is bijective

Given a $C^{\star}$-algebra A and an Hilbert space $\mathcal{H}$:

DEFINITION 5.1.61

REPRESENTATION OF A ON $\mathcal{H}$:
an involutive morphism $\pi : A \to B(\mathcal{H})$ from A to $B(\mathcal{H})$

Given a representation π of A on the Hilbert space $\mathcal{H}$:

DEFINITION 5.1.62

π IS REDUCIBLE:

$$\exists\, V \subset \mathcal{H} \text{ linear subspace } : \pi(V) \subseteq V \tag{5.1.5.118}$$

Given two representations π_1 and π_2 of A on the Hilbert spaces, respectively, $\mathcal{H}_1$ and $\mathcal{H}_2$:

DEFINITION 5.1.63

π_1 AND π_2 ARE EQUIVALENT:

$$\exists U : \mathcal{H}_1 \to \mathcal{H}_2 \, isomorphism : \pi_2(a) = U \pi_1(a) U^{-1} \ \forall a \in A \tag{5.1.5.119}$$

Any state $\omega \in S(A)$ over a $C^{\star}$-algebra A gives rise to a particularly important representation of A we are going to introduce.

Defined the following subset of A:

$$\mathcal{N} := \{ a \in A : \omega(a^{\star} a) = 0 \} \tag{5.1.5.120}$$

let us define on the quotient space $\frac{A}{\mathcal{N}}$ the inner product:

$$< a | b > := \omega(a^{\star} b) \ \ [a], [b] \in \frac{A}{\mathcal{N}} \tag{5.1.5.121}$$

Let us observe, furthermore, that the canonical embedding $i : A \mapsto \frac{A}{\mathcal{N}}$:

$$i(a) := [a] = \{ b \in A : b = a + c \, , \, c \in \mathcal{N} \} \tag{5.1.5.122}$$

is a continuous application from A (endowed with the norm-topology) to $\frac{A}{\mathcal{N}}$ (endowed with the norm topology induced by the inner-product of eq.5.1.5.121).

We can then introduce the following:

DEFINITION 5.1.64

GELFAND-NAIMARK-SEGAL REPRESENTATION (GNS REPRESENTATION) OF A W.R.T. ω

the representation π_ω of A on the Hilbert space $\mathcal{H}_\omega$:

- $\mathcal{H}_\omega$ is the completion of the inner product space $(\frac{A}{\mathcal{N}} , < a|b >)$
- π_ω is the continuous extension of the application:

$$[\pi_\omega(a)]|[b] > := \; a\, b \;\; [b] \in \frac{A}{\mathcal{N}} \tag{5.1.5.123}$$

One has that:

Theorem 5.1.8

BASIC PROPERTIES OF THE GNS REPRESENTATION:

1. the vector:

$$|\Omega_\omega > := \; |[I] > \tag{5.1.5.124}$$

   is cyclic, i.e. $\pi_\omega(A)|\Omega_\omega >$ is dense in $\mathcal{H}_\omega$

2. any representation π of A admitting a ciclic vector $|\Phi >$ is equivalent to the GNS representation π_φ w.r.t. the state:

$$\varphi(a) \; := < \Phi|\pi(a)|\Phi > \quad a \in A \tag{5.1.5.125}$$

3.

$$\pi_\omega \text{ is irreducible } \;\Leftrightarrow\; \omega \in \Xi(A) \tag{5.1.5.126}$$

Let us now present the following fundamental:

Theorem 5.1.9

GELFAND'S ISOMORPHISM AT $C^\star$-ALGEBRAIC LEVEL:

HP:

A abelian $C^\star$-algebra

$C(X(A))$ $C^\star$-algebra of the complex-valued continuous (w.r.t. the $W^\star$-topology) on $X(A)$

TH:

A and $C(X(A))$ are $\star$-isomorphic

Indeed also the converse property holds, and theorem5.1.9 may be considerably streghtened, resulting in the following:

Theorem 5.1.10

CATEGORY EQUIVALENCE AT THE BASIS OF NONCOMMUTATIVE TOPOLOGY

The **category** having as **objects** the **Hausdorff compact topological spaces** and as **morphisms** the **continuous maps** on such spaces is equivalent to the category having as **objects** the **abelian $C^{\star}$-algebras** and as **morphisms** the **involutive morphisms** of such spaces.

Remark 5.1.2

THE METAPHORE BY WHICH WE CAN SPEAK ABOUT NONCOMMUTATIVE SETS FROM WITHIN ZFC:

Theorem5.1.10 says, in particular, that an abelian $C^{\star}$-algebra may be always seen as an algebra of function over a suitable topological space X.

This suggest to introduce a metaphore, that we call the **noncommutative metaphore** from here and beyond, according to which one looks at a noncommutative algebra A as if it was an algebras of functions over an hypothetic **noncommutative set**:

$$A \;=_{METAPHORE}\; C(X_{NC}) \tag{5.1.5.127}$$

Of course this is only a metaphore, but it is the only way we can speak about **noncommutative sets** from within the formal system of **commutative set theory** (namely the formal system ZFC of Zermelo Fraenkel endowed with the Axiom of Choice) giving foundations to Mathematics.

Since there is no possibility inside ZFC of formalizing eq.5.1.5.127 and so to speak directly of X_{NC} , we will never mention it and we will directly refer to A as a **noncommutative set**.

It should be even supreflous to remark that, of course, from the same fact we can speak about it inside ZFC, A is also a **commutative set**.

So it is fundamental, when we speak about A, to specify if we are looking at it as an ordinary **commutative set** or as a **noncommutative set**, i.e. as a way of speaking about the non formalizable-in-ZFC object X_{NC}.

Such a double nature, of course, reflects itself at different levels:

- at a logical level if we look at A as a **noncommutative set**, one can formalize its propostion calculus through the quantum logic QL(A).

  If instead one look at A as a **commutative set**, one can, of course, apply to it the ordinary classical (i.e. distributive) set-theoretical predicative calculus

- we will soon introduce the notion of **noncommutative cardinality** of a noncommutative set;

  according to such a notion we will arrive to characterize the noncommutative binary alphabet $\Sigma_{NC} \;=\; M_2(\mathbb{C})$ by the condition:

$$cardinality_{NC}(\Sigma_{NC}) \;=\; 1 \tag{5.1.5.128}$$

Anyway, obviously, looking at $M_2(\mathbb{C})$ simply as a commutative set, we can consider its commutative cardinality:

$$cardinality(M_2(\mathbb{C})) \; = \; \aleph_1^4 \; = \; \aleph_1 \tag{5.1.5.129}$$

Theorem5.1.10 introduces a **topological structure** over **noncommutative sets**.

It is just the first of a collection of Category Equivalence Theorems that allow to introduce an high hierarchy of more and more refined structures on **noncommutative sets**, resulting in the wonderful conceptual tower, namely Noncommutative Geometry, built by that genius named Alain Connes [Jaf91].

DEFINITION 5.1.65

$W^{\star}$-ALGEBRA (or ALGEBRAIC SPACE):
a $C^{\star} - ALGEBRA$ A such that $(A^{\star} \, , \, \| \cdot \|)$ is a Banach space

DEFINITION 5.1.66

COMMUTATIVE SPACE:
a commutative algebraic space

DEFINITION 5.1.67

NONCOMMUTATIVE SPACE:
a noncommutative algebraic space

Example 5.1.5

THE $W^{\star}$-ALGEBRA OF THE BOUNDED OPERATORS ON AN HILBERT SPACE

Given an arbitrary Hilbert space $\mathcal{H}$ the space $B(\mathcal{H})$ of all the bounded linear operators on $\mathcal{H}$ is a $W^{\star}$-algebra

DEFINITION 5.1.68

AUTOMORPHISMS OF A:

$$AUT(A) \; := \; \{ \tau : A \rightarrow A \text{ involutive isomorphism of A } \} \tag{5.1.5.130}$$

DEFINITION 5.1.69

INNER AUTOMORPHISMS OF A:

$$INN(A) \; := \; \{ \tau \in AUT(A) \, : \exists u \in \mathcal{U}(A) \, , \, \tau(a) = u a u^{\star} \; \forall a \in A \} \tag{5.1.5.131}$$

DEFINITION 5.1.70

OUTER AUTOMORPHISMS OF A:

$$OUT(A) := \frac{AUT(A)}{INN(A)} \tag{5.1.5.132}$$

Given two algebraic spaces A and B:

DEFINITION 5.1.71

POSITIVE MAPS FROM A TO B:

$$P(A,B) := \{ \tau : A \rightarrow B \, linear : \tau(A_{+}) \subseteq B_{+} \} \tag{5.1.5.133}$$

DEFINITION 5.1.72

COMPLETELY POSITIVE MAPS FROM A TO B:

$$CP(A,B) \equiv \{ \tau \in P(A,B) : \tau \otimes \mathbb{I}_{n} \in P(A,B) \ \forall n \in \mathbb{N} \} \tag{5.1.5.134}$$

DEFINITION 5.1.73

COMPLETELY POSITIVE UNITAL MAPS (CPU-MAPS OR CHANNELS) FROM A TO B:

$$CPU(A,B) \equiv \{ \tau \in CP(A,B) : \tau(\mathbb{I}) = \mathbb{I} \} \tag{5.1.5.135}$$

In particular:

DEFINITION 5.1.74

POSITIVE MAPS ON A:

$$P(A) := P(A,A) \tag{5.1.5.136}$$

DEFINITION 5.1.75

COMPLETELY POSITIVE MAPS ON A:

$$CP(A) \equiv CP(A,A) \tag{5.1.5.137}$$

DEFINITION 5.1.76

COMPLETELY POSITIVE UNITAL MAPS (CPU-MAPS OR CHANNELS) ON A:

$$CPU(A) := CPU(A,A) \tag{5.1.5.138}$$

One has the following:

Theorem 5.1.11

ON THE RELATIONSHIP BETWEEN POSITIVITY AND COMPLETE-POSITIVITY:

1.

$$A\ commutative \ \Rightarrow \ CP(A) \ = \ P(A) \qquad (5.1.5.139)$$

2.

$$A\ noncommutative \ \Rightarrow \ CP(A) \ \subset \ P(A) \qquad (5.1.5.140)$$

The analysis of channels is particularly simplified by the following:

Theorem 5.1.12

KRAUS-STINESPRING'S THEOREM:
HP:

$$A \subseteq B(\mathcal{H}) \text{ Von Neumann algebra acting on the Hilbert space } \mathcal{H}$$
$$\alpha \, : \, A \rightarrow A \text{ normal linear map}$$

TH:

$$\alpha \in CPU(A) \ \Leftrightarrow \ \exists \{V_i\}_{i \in I} \in \mathcal{B}(\mathcal{H})\} \ :$$
$$\alpha(a) \ = \ \sum_{i \in I} V_i^{\star} a V_i \ \forall a \in A$$
$$\sum_{i \in I} V_i^{\star} V_i \ = \ \mathbb{I} \qquad (5.1.5.141)$$

where the convergence is in the weak topology.

Remark 5.1.3

IDENTIFICABILITY OF $\star$-ISOMORPHIC $W^{\star}$-ALGEBRAS:
Since, from an algebraic viewpoint, $\star$-isomorphic $W^{\star}$-algebras are identical, they can be identified.

So, for example, the $W^{\star}$-algebra $B(\mathcal{H}_n)$ of all the bounded linear operators on an n-dimensional Hilbert space $\mathcal{H}_n$, with $n \in \mathbb{N}$ may be identificated with the $W^{\star}$-algebra $M_n(\mathbb{C})$ of all the $n \times n$ matrices with complex entries.

So, in particular, the algebra $B(\mathcal{H}_2^{\bigotimes n})$ of all the bounded linear operators on the n-qubits Hilbert space $\mathcal{H}_2^{\bigotimes n}$ may be identified with the $W^{\star}$-algebra $M_{2^n}(\mathbb{C})$

Given a $C^{\star} - algebra$ we will, obviously, say that:

DEFINITION 5.1.77

A IS ABELIAN:

$$[a,b] := ab - ba = 0 \ \forall a,b \in A \qquad (5.1.5.142)$$

Given an abelian $C^{\star} - algebra$ A:

DEFINITION 5.1.78

$$X(A) := \{\pi : \text{ representation of A on } \mathbb{C}\} \qquad (5.1.5.143)$$

Given a $C^{\star} - algebra$ A and a linear subspace $B \subseteq A$:

DEFINITION 5.1.79

B IS A SUB-$C^{\star}$-ALGEBRA OF A:
B is a $C^{\star} - algebra$ w.r.t. to the restriction to B of the $C^{\star} - algebraic$ structure of A

Given an Hilbert space $\mathcal{H}$ ed and a $sub - C^{\star} - algebra \ A \subseteq B(\mathcal{H})$ of $B(\mathcal{H})$:

DEFINITION 5.1.80

COMMUTANT OF A:

$$A' = \{a \in A : [a,b] = 0 \ \forall b \in B(\mathcal{H})\} \qquad (5.1.5.144)$$

DEFINITION 5.1.81

CENTRE OF A:

$$\mathcal{Z}(A) := A \cap A' \qquad (5.1.5.145)$$

DEFINITION 5.1.82

A IS A VON NEUMANN ALGEBRA:

$$A'' := (A')' = A \qquad (5.1.5.146)$$

The two notions of a $W^{\star}$-algebra and of a Von Neumann algebra introduced, respectively, in definition5.1.65 and definition5.1.82 would seem to have anything in common: the first is a purely abstract algebraic notion while the latter is a concrete notion concerning operators on an Hilbert space.

So it may appear rather shocking that these notions are indeed equivalent (remember remark5.1.3) , as is stated by the following:

Theorem 5.1.13

SAKAI'S THEOREM:
HP:

$$A \; C^\star - algebra$$

TH:

$$\text{A is } \star\text{-isomorphic to a Von Neumann algebra} \Leftrightarrow \text{A is a } W^\star - algebra$$

Up to now all these operator-algebraic stuff would seem no to have anything in common with Quantum Logic.

Anyway it may be proved that:

Theorem 5.1.14

ON THE QUANTUM LOGIC OF A VON NEUMANN ALGEBRA:

HP:

$$\mathcal{H} \text{ Hilbert space } A \qquad \subseteq B(\mathcal{H}) \text{ Von Neumann algebra}$$

TH:

$$QL(A) := (\mathcal{P}(A), \preceq, \perp) \text{ is a quantum logic}$$
$$\mathcal{P}(A)'' = A$$

where $\preceq$ and $\perp$ are, respectively, the partial-ordering relation and the orthocomplementation inherited from $\mathcal{L}(\mathcal{H})$.

Theorem5.1.14 tells us that, substantially, a Von Neumann algebra is generated by the quantum logic it gives rise to.

Indeed, as we will now show, the underlying quantum logics substantially govern the classification of Von Neumann algebras.

Given a Von Neumann algebra $A \subseteq B(\mathcal{H})$:

DEFINITION 5.1.83

A IS A FACTOR:

$$\mathcal{Z}(A) = \{\lambda I \, , \, \lambda \in \mathbb{C}\} \tag{5.1.5.147}$$

Factors are, substantially, the building blocks of Von Neumann algebras: any Von Neumann algebra A may, actually, be expressed as a direct integral of factors:

$$A = \int_{\mathcal{Z}(A)}^{\otimes} A_\lambda \, d\nu(\lambda)$$
$$\mathcal{Z}(A_\lambda) = \{\mathbb{C}\mathbb{I}\} \; \forall \lambda \in \mathcal{Z}(A) \tag{5.1.5.148}$$

Hence the analysis of a Von Neumann algebra may be reduced to the analysis of its building blocks.

Given, now, a generic Von Neumann algebra $A \subseteq B(\mathbb{H})$ and two its projections $a, b \in \mathcal{P}(A)$:

DEFINITION 5.1.84

a AND b ARE EQUIVALENT IN A:

$$a \sim_A b := \exists o \in A : (o|\psi >= 0 \, \forall |\psi > \in Range(a)^{\perp}) \\ and \, (\|o|\psi > \| = \||\psi > \| \, \forall |\psi > \in Range(a)\} \quad (5.1.5.149)$$

Remark 5.1.4

INTUITIVE MEANING OF $\sim_A$: EQUALITY OF THE DIMENSION RELATIVE TO A

Definition5.1.84 may appear rather counter-intuitive. Its meaning is that the existence of a partial (since it acts so only on Range(a) being identically null on its complement) isometry between Range(a) and Range(b) that belongs to A may be interpreted, informally speaking, as the fact that the **dimension relative to A** of the subspace a projects to is equal to the **dimension relative to A** of the subspace b projects to

The equivalence relation $\sim_A$ over $\mathcal{P}(A)$ may be used to introduce a new partial ordering on projections (different from that of the quantum logic of A)

$$a \trianglelefteq b := \exists c \in \mathcal{P}(A) : a \sim_A c \leq b \quad (5.1.5.150)$$

Remark 5.1.5

INTUITIVE MEANING OF $\trianglelefteq$: ORDERING ACCORDING TO THE RELATIVE DIMENSION

The intuitive meaning of the partial ordering $\trianglelefteq$ is induced by that of the equivalence relation $\sim_A$.

So the condition $a \trianglelefteq b$ means,intuitively, that the **dimension relative to A** of a is less or equal to the **dimension relative to A** of b.

But here comes the following:

Theorem 5.1.15

TOTAL ORDERING W.R.T. $\trianglelefteq$ OF A FACTOR'S EQUIVALENCE CLASSES OF PROJECTIONS

$$\mathcal{Z}(A) = \mathbb{C}I \Rightarrow (a \trianglelefteq b \, or \, b \trianglelefteq a \;\; \forall a, b \in \frac{\mathcal{P}(A)}{\sim_A}) \quad (5.1.5.151)$$

whose importance is owed to an immediate conseguence of its:

Corollary 5.1.1

ORDER TYPE OF $\frac{\mathcal{P}(A)}{\sim_A}$ IS AN INVARIANT FOR FACTORS

$$A, B \star -isomorphic\, factors \;\Rightarrow\; Type-order(\frac{\mathcal{P}(A)}{\sim_A})) \;=\; Type-order(\frac{\mathcal{P}(B)}{\sim_B})) \tag{5.1.5.152}$$

To determine the order type of a $\frac{\mathcal{P}(A)}{\sim_A}$ of a factor A a key concept is the finiteness of projections:

DEFINITION 5.1.85

$a \in \mathcal{P}(A)$ IS FINITE:

$$a \sim_A b \trianglelefteq a \;\Rightarrow\; a = b \;\; \forall b \in \mathcal{P}(A) \tag{5.1.5.153}$$

We can, at last, formalize the intuitive statements concerning the **relative dimension** of remark5.1.4 and remark5.1.5introducing the following fundamental notion:

DEFINITION 5.1.86

RELATIVE DIMENSION W.R.T. A:
a map $d : \mathcal{P}(A) \mapsto [0, +\infty]$ such that:

$$d(a) \;=\; 0 \;\Leftrightarrow\; a \;=\; 0 \;\; \forall a \in \mathcal{P}(A) \tag{5.1.5.154}$$

$$a \perp b \;\Rightarrow d(a+b) \;=\; d(a) + d(b) \;\; \forall a \in \mathcal{P}(A) \tag{5.1.5.155}$$

$$d(a) \;< d(b) \;\Leftrightarrow\; a \trianglelefteq b \;\; \forall a, b \in \mathcal{P}(A) \tag{5.1.5.156}$$

$$d(a) \;+\infty \;\Leftrightarrow\; a \text{ is finite } \;\; \forall a \in \mathcal{P}(A) \tag{5.1.5.157}$$

$$d(a) \;=\; d(b) \;\Leftrightarrow\; a \sim_A b \;\; \forall a, b \in \mathcal{P}(A) \tag{5.1.5.158}$$

$$d(a) \;+\; d(b) \;=\; d(a \bigwedge b) \;+\; d(a \bigvee b) \;\; \forall a, b \in \mathcal{P}(A) \tag{5.1.5.159}$$

We will denote, from here and beyond, the relative dimension w.r.t. a factor A by d_A.

The astonishing fact is that:

Theorem 5.1.16

UNICITY OF THE RELATIVE DIMENSION W.R.T. A FACTOR:

$$d_1 \,,\, d_2 \text{ relative dimensions w.r.t. A } \;\Rightarrow\; \exists c \in \mathbb{R}_+ \;:\; (d_1(a) \;=\; c\, d_2(a) \; \forall a \in \mathcal{P}(A)) \tag{5.1.5.160}$$

The importance of theorem5.1.16 lies in that it implies that the order type of $\frac{\mathcal{P}(A)}{\sim_A}$ can be read off the order type of d_A's range.

Murray and Von Neumann determined the possible ranges of d_A (suitably normalized) resulting in the following classification:

DEFINITION 5.1.87

A IS OF TYPE FINITE, DISCRETE ($Type(A) = I_n$)

$$Range(d_A) = \{0, 1, \ldots, n\} \;\; n \in \mathbb{N}_+ \tag{5.1.5.161}$$

DEFINITION 5.1.88

A IS OF TYPE INFINITE, DISCRETE ($Type(A) = I_\infty$):

$$Range(d_A) = \{0, 1, \ldots, +\infty\} \tag{5.1.5.162}$$

DEFINITION 5.1.89

A IS OF TYPE FINITE, CONTINUOUS ($Type(A) = II_1$):

$$Range(d_A) = [0, 1] \tag{5.1.5.163}$$

DEFINITION 5.1.90

A IS OF TYPE INFINITE, CONTINUOUS ($Type(A) = II_\infty$):

$$Range(d_A) = [0, +\infty] \tag{5.1.5.164}$$

DEFINITION 5.1.91

A IS OF TYPE PURELY INFINITE ($Type(A) = III$)

$$Range(d_A) = \{0, +\infty\} \tag{5.1.5.165}$$

Remark 5.1.6

THE ORDER TYPE OF $\frac{\mathcal{P}(A)}{\sim_A}$ DOESN'T ALLOW A COMPLETE CLASSIFICATION OF FACTORS

It is important, at this point, to remark that the the above classification of factors based on the order type of the algebraic dimension function's range is not complete.

The complete classification, furnished almost fourty years later by the great Alain Connes, will be briefly introduced in section5.2

It is, now, conceptually important to observe that the relative dimension with respect to factors, underlying their Murray-Von Neumann classification, is a Quantum-Logic's notion:

Theorem 5.1.17

RELATIVE DIMENSION W.R.T. A FACTOR IS A MATTER OF QUANTUM LOGIC

d_A is a lattice dimension function over the weak quantum logic QL(A)

Corollary 5.1.2

THE QUANTUM LOGIC OF A FINITE FACTOR IS STRONG:
HP:

$$A\ factor\ :\ Type(A)\ \in\ \{I_n\}_{n\in\mathbb{N}}\bigcup\{II_1\}$$

TH:

$$\text{QL(A) is a strong quantum logic}$$

PROOF:

Since d_A assumes only finite values this happens, obviously, also to its restriction to $\mathcal{P}(A)$ that, by theorem5.1.17, is an algebraic dimension function over QL(A).

By theorem5.1.5 the thesis immediately follows ■

We have, at last, almost all the ingredients required to understand the confession of Von Neumann to Birkhoff.

The last ingredients required are those deriving from the following:

Theorem 5.1.18

CHARACTERIZATION OF DISCRETE FACTORS:

$$Type(A)\ \in\ \{I_n\}_{n\in\{0,1,\cdots,\infty\}}\ \Leftrightarrow\ \exists\mathcal{H}\text{ Hilbert space }\ :\ A\ =\ B(\mathcal{H}) \quad (5.1.5.166)$$

PROOF:

A is $\star$-isomorphic to a $B(\mathcal{H})$, for a proper Hilbert space $\mathcal{H}$, iff the quantum logic of A is an Hilbert Lattice.

But a logic dimension function of an Hilbert lattice may be easily defined as the dimensionality, as linear subspaces, of its elements and, conseguentially, can assume only integer values.

By theorem5.1.16and theorem5.1.17 it immediately follows the thesis ■

Corollary 5.1.3

ATOMICITY OF A FACTOR'S QUANTUM LOGIC

$$QL(A)\text{ is atomic }\ \Leftrightarrow\ Type(A)\ \in\ \{I_n\}_{n\in\{0,1,\cdots,\infty\}} \quad (5.1.5.167)$$

PROOF:

By theorem5.1.18 we have that QL(A) is an Hilbert lattice iff A is discrete.

The thesis immediately follows ■

Given a $W^{\star}$-algebra A:

DEFINITION 5.1.92

TRACE ON A:
A linear map $\tau : A_{+} \mapsto [0,+\infty]$ such that:

$$\tau \circ \alpha = \tau \;\; \forall \alpha \in INN(A) \tag{5.1.5.168}$$

Given a trace τ on A:

DEFINITION 5.1.93

τ IS FINITE:

$$\infty \notin Range(\tau) \tag{5.1.5.169}$$

A very important property of finite factors is stated by the following:

Theorem 5.1.19

EXTENSIBILITY OF THE RELATIVE DIMENSION W.R.T. A FINITE FACTOR TO A FINITE TRACE
HP:

$$A \; factor \; : \; Type(A) \in \{I_n\}_{n \in \mathbb{N}} \bigcup \{II_1\}$$

TH:

$$\exists ! \tau_A \text{ finite trace on A } : \tau_A |_{\mathcal{P}(A)} = d_A \tag{5.1.5.170}$$

Theorem 5.1.20

HP:

$$A \; factor \; : \; Type(A) \in \{I_n\}_{n \in \mathbb{N}} \bigcup \{II_1\}$$

TH:

$$\exists ! \omega_A \in S(A) \; : \; \omega_A |_{A_{+}} = \tau_A \tag{5.1.5.171}$$

Example 5.1.6

THE FINITE TRACE ON THE n-QUBITS' $W^{\star}$-ALGEBRA

We know that:

$$B(\mathcal{H}_2^{\bigotimes n}) \;=\; \bigotimes_{k=1}^{n} M_2(\mathbb{C}) \;=\; M_{2^n}(\mathbb{C}) \qquad (5.1.5.172)$$

The finite trace on the $n \times n$ matrix algebra $M_n(\mathbb{C})$ is simply the normalized matricial trace:

$$\tau_n \;:=\; \frac{1}{n} Tr_n \;=\; \bigotimes_{k=1}^{n} \tau_2 \qquad (5.1.5.173)$$

so that the finite trace on $B(\mathcal{H}_2^{\bigotimes n})$ is τ_{2^n}.

Let us now consider an arbitrary $W^{\star}$-algebra A.

We want to characterize the condition stating that A is $C_{\Phi}-NC_M$-computable, i.e. is approximable with arbitrary precision by finite-dimensional matrix algebras.

Mathematically formalized such a constraint results in the following:

DEFINITION 5.1.94

A IS HYPERFINITE:

there exists an increasing sequence $\{A_n\}_{n \in \mathbb{N}}$ of $W^{\star}$-algebras of A such that:

$$A \;=\; (\bigcup_{n \in \mathbb{N}} A_n)'' \qquad (5.1.5.174)$$

Example 5.1.7

THE HYPERFINITE II_1 FACTOR R

Given the one dimensional lattice $\mathbb{Z}$ let us attach to the n^{th} lattice site the 1-qubit $W^{\star}$-algebra:

$$A_n \;:=\; M_2(\mathbb{C}) \;\; n \in \mathbb{Z} \qquad (5.1.5.175)$$

Given an arbitary set of sites $\Lambda \subseteq \mathbb{Z}$ let us define:

$$A_{\Lambda} \;:=\; \bigotimes_{n \in \Lambda} A_n \qquad (5.1.5.176)$$

Clearly we have that:

$$\Lambda_1 \subseteq \Lambda_2 \;\Rightarrow\; A_{\Lambda_1} \subseteq A_{\Lambda_2} \qquad (5.1.5.177)$$

$$\Lambda_1 \bigcap \Lambda_2 \;=\; \emptyset \;\Rightarrow\; [A_{\Lambda_1}, A_{\Lambda_2}] \;=\; 0 \qquad (5.1.5.178)$$

Let us now consider the state $\tau_{\Lambda} \in S(A_{\Lambda})$ defined as:

$$\tau_{\Lambda} := \bigotimes_{n \in \Lambda} \tau_{2} \tag{5.1.5.179}$$

Clearly we have, in particular, that the state:

$$\tau_{\{0,1,\cdots,n\}} = \tau_{2^{n}} \tag{5.1.5.180}$$

is nothing but the finite tracial state on the n-qubit $W^{\star}$-algebra $B(\mathcal{H}_{2}^{\bigotimes n})$ we saw in the example5.1.6

We are at last ready to introduce one of the main actors of this dissertation, namely the $W^{\star}$-algebra:

$$R := \pi_{\tau_{\mathbb{Z}}}(A_{\mathbb{Z}})'' \tag{5.1.5.181}$$

By eq.5.1.5.178 and the linearity of the GNS-representations we infer that R is itself a factor.

Eq.5.1.5.177 implies that R is hyperfinite.

We already know that the n-qubit $W^{\star}$-algebra is a type $I_{2^{n}}$ factor, i.e. that, taking into account the normalization coefficient $\frac{1}{2^{n}}$ of $\tau_{2^{n}}$(not considered, for convenience, in definition5.1.87), we have that:

$$Range(d_{B(\mathcal{H}_{2}^{\bigotimes n})}) = \{0 \, , \frac{1}{2^{n}} \, , \frac{2}{2^{n}} \, , \cdots 1\} \tag{5.1.5.182}$$

Since in the limit $n \rightarrow \infty$ the dyadic rationals fill the interval $[0 \, , 1]$ it follows that:

$$Range(\tau_{\mathbb{Z}}|_{\mathcal{P}(A_{\mathbb{Z}})}) = [0 \, , 1] \tag{5.1.5.183}$$

implying that R is a II_{1}-factor.

Since, as we will explain more clearly in section5.2, the hyperfinite II_{1}-factor is unique (obviously, remembering remark5.1.3, up to $\star$-isomorphism) it is precisely R.

We can, at last, face Von Neumann's confession to Birkhoff, clarifying why the right the right noncommutative space of qubits' sequences is not $B(\mathcal{H}_{2}^{\bigotimes \infty})$ but R.

This requires, first of all, to understand that the equivalence relation of definition 5.1.84 is nothing but the noncommutative analogue of the Theory of Cardinal Numbers, i.e. the the theory of the **noncommutative cardinal numbers** describing the infinity's degree of **noncommutative sets**.

In the words of Von Neumann:

"$\cdots$ the whole algorithm of Cantor theory is such that the most of it goes over in this case. One can prove various theorems on the additivity of equivalence and the transitivity of equivalence, which one would normally expect, so that one can introduce a theory of alephs here, just as in set theory. $\cdots$ I may call

this dimension since for all matrices of the ordinary space, is nothing else but dimension" (Unpublished, cited in [Red98])

"One can prove most of the Cantoreal properties of finite and infinite, and, finally, one can prove that given a Hilbert space and a ring in it , a simple ring in it, either all linear sets except the null sets are infinite (in which case this concept of alephs gives you nothing new), or else the dimensions, the equivalence classes, behave exactly like numbers and there are two qualitatively different cases. The dimensions either behave like integers, or else they behave like all real numbers. There are two subcases, namely there is either a finite top or there is not" (Unpublished, cited in [Red98])

Given a factor A, let us uniformize the commutative and noncommutative terminology introducing the following notation:

DEFINITION 5.1.95

A HAS NONCOMMUTATIVE CARDINALITY EQUAL TO $n \in \mathbb{N}$:

$$cardinality_{NC}(A) \; = \; n \; := \; Type(A) \; = \; I_n \tag{5.1.5.184}$$

DEFINITION 5.1.96

A HAS NONCOMMUTATIVE CARDINALITY EQUAL TO $\aleph_0$:

$$cardinality_{NC}(A) \; = \; \aleph_0 \; := \; Type(A) \; = \; I_\infty \tag{5.1.5.185}$$

DEFINITION 5.1.97

A HAS NONCOMMUTATIVE CARDINALITY EQUAL TO $\aleph_1$:

$$cardinality_{NC}(A) \; = \; \aleph_1 \; := \; Type(A) \; \in \; \{II_1, II_\infty\} \tag{5.1.5.186}$$

A HAS NONCOMMUTATIVE CARDINALITY EQUAL TO $\aleph_2$:

$$cardinality_{NC}(A) \; = \; \aleph_2 \; := \; Type(A) \; = \; III \tag{5.1.5.187}$$

The definition of noncommutative cardinality may then be extended to arbitary $W^\star$-algebras rqeuiring its additiviy w.r.t. the factor decomposition.

Let us then observe that in the commutative case (see theorem1.2.1) the passage from strings to sequences implies an increasing of one **commutative cardinal number**; this implies that:

1. it doesn't exist a bijection $b : \Sigma^\star \mapsto \Sigma^\infty$, i.e.:

$$cardinality(\Sigma^\star) \; \neq \; cardinality(\Sigma^\infty) \tag{5.1.5.188}$$

2. it does exist an injection $i : \Sigma^\star \mapsto \Sigma^\infty$, i.e.:

$$cardinality(\Sigma^\star) \; \leq \; cardinality(\Sigma^\infty) \tag{5.1.5.189}$$

3. the degree of infinity of Σ^{∞} is that immediately successive to the the degree of infinity of $\Sigma^{\star}$ [1], i.e.:

$$\nexists\, S \;:\; cardinality(\Sigma^{\star}) \;<\; cardinality(S) \;<\; cardinality(\Sigma^{\infty}) \tag{5.1.5.191}$$

Denoted by $\Sigma^{\star}_{NC}$ the $W^{\star}$**-algebra of qubits's strings** and by Σ^{∞}_{NC} the $W^{\star}$**-algebra of qubits' sequences**, theorem5.1.10 requires that the same conditions hold for noncommutative cardinality:

1.

$$cardinality_{NC}(\Sigma^{\star}_{NC}) \;\neq\; cardinality_{NC}(\Sigma^{\infty}_{NC}) \tag{5.1.5.192}$$

2.

$$cardinality_{NC}(\Sigma^{\star}_{NC}) \;\leq\; cardinality_{NC}(\Sigma^{\infty}_{NC}) \tag{5.1.5.193}$$

3.

$$\nexists\, A\, factor \;:\; cardinality_{NC}(\Sigma^{\star}_{NC}) \;<\; cardinality_{NC}(A) \;<\; cardinality_{NC}(\Sigma^{\infty}_{NC}) \tag{5.1.5.194}$$

Since:

$$\Sigma^{\star}_{NC} \;=\; B(\mathcal{H}_2^{\bigotimes \star}) \tag{5.1.5.195}$$

we have, conseguentially, that:

$$cardinality_{NC}(\Sigma^{\infty}_{NC}) \;=\; cardinality_{NC}(\Sigma^{\star}_{NC}) + 1 \;=\; \aleph_1 \tag{5.1.5.196}$$

Since we already know that $cardinality_{NC}(B(\mathcal{H}_2^{\bigotimes \infty})) \;=\; \aleph_0$ it follows that:

$$\Sigma^{\infty}_{NC} \;=\; R \;\neq\; B(\mathcal{H}_2^{\bigotimes \infty}) \tag{5.1.5.197}$$

Remark 5.1.7

[1] Such a constraint that there does not exist intermediate degrees of infinity requires the assumption of the following:

AXIOM 5.1.3

CONTINUUM HYPOTHESIS:

$$2^{\aleph_0} \;=\; \aleph_1 \tag{5.1.5.190}$$

that is well known to be **consistent** but **independent** from the formal system ZFC giving foundation to Mathematics [Odi89]

DIFFERENCE BETWEEN THE RAISING OF COMMUTATIVE CARDINALITY AND THE RAISING OF NONCOMMUTATIVE CARDINALITY

The fact that the passage from a separable to a non-separable Hilbert space involves a kind of passage from the **discrete** to the **continuum** may be highly misleading:

introduced the:

DEFINITION 5.1.98

COMPUTATIONAL RIGGED-BASIS OF $\mathcal{H}_2^{\bigotimes \infty}$:

$$\mathbb{E}_{\infty} := \{ |\bar{x} > , \bar{x} \in \Sigma^{\infty} \} \quad (5.1.5.198)$$

$$< \bar{x} | \bar{y} > = \delta(\bar{x} - \bar{y}) \ \ \bar{x}, \bar{y} \in \Sigma^{\infty} \quad (5.1.5.199)$$

$$\int_{\Sigma^{\infty}} dP_{unbiased} |\bar{x} >< \bar{x}| = \hat{\mathbb{I}} \quad (5.1.5.200)$$

theorem1.2.1 may be restated as:

$$cardinality(\mathbb{E}_{\star}) = \aleph_0 \quad (5.1.5.201)$$

$$cardinality(\mathbb{E}_{\infty}) = \aleph_1 \quad (5.1.5.202)$$

So eqs.5.1.5.201 are simply the reformulation in an Hilbert space setting on the constraint imponing the raising of one cardinal number in passing from the **commutative cardinality** of the **commutative space** of cbits' stings to the **commutative space** of cbits' sequences.

It is not the constraint imponing the raising of one cardinal number in passing from the **noncommutative cardinality** of the **noncommutative space** of cbits' strings to the **noncommutative space** of cbits' sequences, namely the following:

Theorem 5.1.21

ON THE NONCOMMUTATIVE CARDINALITIES OF STRINGS AND SEQUENCES OF QUBITS:

$$cardinality_{NC}(\Sigma_{NC}^{\star}) = \aleph_0$$

$$cardinality_{NC}(\Sigma_{NC}^{\infty}) = \aleph_1$$

Remark 5.1.8

THE PHENOMENON OF CONTINUOUS DIMENSION FROM A LOGICAL POINT OF VIEW

The phenomenon of continuous dimension involved in the passage from noncommutative cardinality $\aleph_0$ to noncommutative cardinality $\aleph_1$ has an intuitive logic meaning: the lost of **atomicity** of the underlying quantum logic states the disapperance of the **atomic propositions** as stated by corollary5.1.3.

We want here to give a more intuitive picture of what does it means.

In the quantum logic of $QL(B(\mathcal{H}_2^{\bigotimes \star}))$ the propositions of the form:

$$p_{\int_{\Sigma^\infty} c(\bar{x})|\bar{x}>} \quad := \quad \int_{\Sigma^\infty} c(\bar{x})^\star \quad < \quad \bar{x}| \quad \int_{\Sigma^\infty} c(\bar{x})|\bar{x} \quad > \tag{5.1.5.203}$$

are **atomic proposition**, i.e. correspond to the elementary statements from which all the others are generated through the logical connectives.

This is not the case in $QL(\Sigma_{NC}^\infty)$; one could think that the rule of elementary propositions is therein played by projections of the form:

$$p_{k\,,\vec{n}} \;:=\; \bigotimes_{i \in \mathbb{Z}} a_{i\,,\vec{n}} \tag{5.1.5.204}$$

$$p_{i\,,\vec{n}} \;:=\; \begin{cases} \frac{1}{2}(I_2 \,+\, \vec{\sigma} \cdot \vec{n}) & \text{if } i = k, \\ I_2 & \text{otherwise.} \end{cases} \tag{5.1.5.205}$$

(where I_2 denotes the bidimensional identity matrix).

that, interpreting Σ_{NC}^∞ as the $W^\star$-algebra of a quantum spin-1/2 chain at infinite temperature, correspond to the statement << the spin in the k^{th} lattice site points in the direction $\vec{n}$ >>.

Anyway $p_{k\,,\vec{n}}$ is not atomic as can be inferred by the fact that the $\aleph_1$ non-commutative cardinality of Σ_{NC}^∞ implies the existence of a projection $p_{k\,,\vec{n}}^1 \in \mathcal{P}(\Sigma_{NC}^\infty)$ such that:

$$d_{\Sigma_{NC}^\infty}(p_{k\,,\vec{n}}^1) \;=\; \frac{d_{\Sigma_{NC}^\infty}(p_{k\,,\vec{n}})}{2} \tag{5.1.5.206}$$

and so:

$$p_{k\,,\vec{n}}^1 \;\trianglelefteq\; p_{k\,,\vec{n}} \tag{5.1.5.207}$$

But then there exist a projection $p_{k\,,\vec{n}}^2 \in \mathcal{P}(\Sigma_{NC}^\infty)$ such that:

$$p_{k\,,\vec{n}}^2 \;\trianglelefteq\; p_{k\,,\vec{n}} \; and \; p_{k\,,\vec{n}}^2 \;\sim_{\Sigma_{NC}^\infty}\; p_{k\,,\vec{n}}^1 \tag{5.1.5.208}$$

and hence:

$$d_{\Sigma_{NC}^\infty}(p_{k\,,\vec{n}}^2) \;=\; d_{\Sigma_{NC}^\infty}(p_{k\,,\vec{n}}^1) \;=\; \frac{d_{\Sigma_{NC}^\infty}(p_{k\,,\vec{n}})}{2} \tag{5.1.5.209}$$

The projection $p_{k\,,\vec{n}}^2$ is thus a non-zero projection strictly smaller than $p_{k\,,\vec{n}}$, so that, conseguentially, $p_{k\,,\vec{n}}$ is not an atom.

Let us finally, as promized, discuss Walter Thirring's reasoning that lead him to give a negative answer to the **Separability Issue** despite of Shrödinger opposite position [Thi01]:

"However such an opinion means that Shrödinger did not get the main message of Von Neumann's celebrated paper on infinite tensor products. There he shows that the corresponding operator algebras are highly reducibly represented in this vast non-separable space and there are many (inequivalent) subrepresentations which act on a separable subspace"

What Thirring is speaking about is the analysis he explicitly reports in the section1.4 of [Thi83]:

the cases **case-I.A** and **case-I** discussed in view of definition5.1.5 and definition5.1.6 give rise to the following two equivalence relations inside $\mathcal{H}_2^{\bigotimes \infty}$:

DEFINITION 5.1.99

$|\psi>, |\phi> \in \mathcal{H}_2^{\bigotimes \infty}$ ARE STRONGLY-EQUIVALENT:

$$|\psi> \sim_S |\phi> := \prod_n{}' < \psi_n|\phi_n > \rightarrow c \neq 0 \tag{5.1.5.210}$$

DEFINITION 5.1.100

$|\psi>, |\phi> \in \mathcal{H}_2^{\bigotimes \infty}$ ARE WEAKLY-EQUIVALENT:

$$|\psi> \sim_W |\phi> := \prod_n{}' < \psi_n|\phi_n > \rightarrow c > 0 \tag{5.1.5.211}$$

where the symbol $\prod'$ means that any finite number of factors 0 are to be left out.

Both the quotient spaces $\frac{\mathcal{H}_2^{\bigotimes \infty}}{\sim_S}$ and $\frac{\mathcal{H}_2^{\bigotimes \infty}}{\sim_W}$ are linear spaces.

Furthermore one has that:

$$cardinality(\frac{\mathcal{H}_2^{\bigotimes \infty}}{\sim_W}) > \aleph_0 \tag{5.1.5.212}$$

$$[|\psi>]_W \neq [|\phi>]_W \Rightarrow <\psi|\phi> = 0 \;\; \forall |\psi>, |\phi> \in \mathcal{H}_2^{\bigotimes \infty} \tag{5.1.5.213}$$

$$[[|\psi>]_W]_S \neq [[|\phi>]_W]_S \Rightarrow <\psi|\phi> = 0 \;\; \forall |\psi>, |\phi> \in \mathcal{H}_2^{\bigotimes \infty} : [|\psi>]_W = [|\phi>]_W \tag{5.1.5.214}$$

Adopting the notation used in example5.1.7, the key point is that

Theorem 5.1.22

ON THE HIGH REDUCIBILITY OF THE REPRESENTATIONS OF $A_{\mathbb{Z}}$ ON $\mathcal{H}_2^{\bigotimes \infty}$

HP:

π representation of $A_{\mathbb{Z}}$ over $\mathcal{H}_2^{\bigotimes \infty}$

TH:

$$[|\psi>]_S \text{ is separable } \quad \forall |\psi> \in \mathcal{H}_2^{\bigotimes \infty} \tag{5.1.5.215}$$

$$\pi([|\psi>]_S) \subseteq [|\psi>]_S \;\; \forall |\psi> \in \mathcal{H}_2^{\bigotimes \infty} \tag{5.1.5.216}$$

$$\text{the sub-representations arising from different weak equivalence classes are inequivalent} \tag{5.1.5.217}$$

According to Thirring theorem5.1.22 implies that one has to answer negatively to the Separability issue.

According to him, one can consistentely assume that qubits sequences are described by rays of the not-separable Hilbert space $\mathcal{H}_2^{\bigotimes \infty}$.

Simply, as always happens in the limit of infinite degrees of freedom, different representations of the observables' algebra may become inequivalent so that one has to select the representation suitable to the physical situation he is studying.

Since such a representation lives on a separable subspace of $\mathcal{H}_2^{\bigotimes \infty}$ everything seems ok.

This way of recovering an Hilbert space axiomatization of Quantum Mechanics is, anyway, apparent:

one start a priori with the observable's algebra and returns to the usual Hilbert space formalism only a posteriori, after a suitable representation is used.

Such an attitude to the algebraic approach (precisely codified in the section1.8 of [Str85]), though FAPP completelly equivalent to the one we support, is philosophically disappealing since it founds on axioms based on posteriori derived quantities.

According to theorem5.1.13 one can, in a completelly equivalent way, forget concrete algebras of operators on Hilbert spaces, forget Hilbert spaces themselves, and speak only about $W^{\star}$-algebras.

Futhermore there is no reason to represent these $W^{\star}$-algebras, returning in this way to an Hilbert space setting.

Such a view point corresponds, substantially, to give a positive answer to the Separability Issue, to infer from that that an Hilbert space axiomatization in terms of the not-separable Hilbert space $\mathcal{H}_2^{\bigotimes \infty}$ is not acceptable and, conseguentially, to conclude that, as to qubits' sequences, one has to give up the idea to remain inside the boundaries of an Hilbert space axiomatization.

We would like to end this section clarifying more properly the concept of qubit, through the following:

Remark 5.1.9

THE NONCOMMUTATIVE COMBINATORY INFORMATION AND THE DEFINITION OF THE QUBIT

It should be clear, at this point, the the **qubit** may be defined, in a conceptually more satisfying way, in the following way:

Given a **noncommutative set** A let us introduce the following notion:

DEFINITION 5.1.101

NONCOMMUTATIVE COMBINATORY INFORMATION:

$$I_{NC\ combinatory}(A) \ := \ \log_2 cardinality_{NC}(A) \tag{5.1.5.218}$$

By theorem5.1.21 we have, via axiom5.1.3, that:

$$I_{NC\ combinatory}(\Sigma_{NC}^{\star}) \ = \ \log_2(\aleph_0) \tag{5.1.5.219}$$

$$I_{NC\ combinatory}(\Sigma_{NC}^{\infty}) \ = \ \log_2(\aleph_1) \ = \ \aleph_0 \tag{5.1.5.220}$$

Then we can at last define precisely the qubit as:

DEFINITION 5.1.102

QUBIT:

$$1 \text{ qubit} \ := \ I_{NC\ combinatory}(\Sigma_{NC}) \tag{5.1.5.221}$$

where:

$$\Sigma_{NC} \ := \ \mathcal{B}(\mathcal{H}_2) \tag{5.1.5.222}$$

is the **noncommutative binary alphabet**

5.2 On the rule Noncommutative Measure Theory and Noncommutative Geometry play in Quantum Physics

In the previous section, precisely in the remark5.1.2 we have introduced the Noncommutative Metaphore allowing to speak about noncommutative sets from inside the ZFC axiomatization of commutative set theory.

By theorem5.1.10 we have then given foundations to Noncommutative Topology, i.e. the analysis of topological structure on noncommutative sets.

The next floor in the construction of the noncommutative tower is the introduction of Noncommutative Measure Theory [Str95],[Str00b].

DEFINITION 5.2.1

ALGEBRAIC PROBABILITY SPACE: (A , ω), where:

- A is a Von Neumann algebra
- ω is a state on A

The notion of **algebraic probability space** is a noncommutative generalization of the notion of **classical probability space** as is implied by the following:

Theorem 5.2.1

GELFAND'S ISOMORPHISM AT $W^{\star}$-ALGEBRAIC LEVEL:

1. a generic **classical probability space** (X , μ) may be equivalententely seen as the algebraic probability space $(L^{\infty}(X, \mu) , \omega_{\mu})$, with:

$$\begin{aligned} \omega_{\mu}(A) &\in S(A) \\ \omega_{\mu}(a) \ &:= \int_{X} a(x) d\mu(x) \end{aligned} \tag{5.2.5.1}$$

2. given a generic **abelian algebraic probability space** (A , ω) there exist a **classical probability space** (X , μ) and a $\star$ - isomorphism $\mathcal{I}_{GELFAND} : A \rightarrow L^{\infty}(X, \mu)$, namely the **Gelfand isomorphism**, under which the state $\omega \in S(A)$ corresponds to the state $\omega_{\mu} \in L^{\infty}(X, \mu)$.

DEFINITION 5.2.2

NONCOMMUTATIVE PROBABILITY SPACE

a non-abelian algebraic probability space.

Given a finite factor A:

DEFINITION 5.2.3

UNBIASED ALGEBRAIC PROBABILITY SPACE ON A:
the algebraic probability space $(A\,,\,\tau_{unbiased})$, where:

$$\tau_{unbiased} \;:=\; \tau_A \tag{5.2.5.2}$$

Let us now clarify an important point.
Given a Von Neumann algebra $A \;\subseteq\; B(\mathcal{H})$:

DEFINITION 5.2.4

NORMAL STATES ON A:

$$S(A)_n \;:=\; \{\omega \in S(A) \;:\; \sup_{\alpha} \omega(a_\alpha) \;=\; \omega(\sup_{\alpha} a_\alpha) \quad \forall \text{ bounded increasing net } \{a_\alpha\} \text{ in A } \} \tag{5.2.5.3}$$

The importance of normal states is owed to a key feature of them, to formalize which let us first introduce the following sequence of norms on $B(\mathcal{H})$:

DEFINITION 5.2.5

n^{th} OPERATORIAL NORM ON $B(\mathcal{H})$

$$\|a\|_n \;:=\; (Tr|a|^n)^{\frac{1}{n}} \tag{5.2.5.4}$$

where:

$$|a| \;:=\; \sqrt{a^\star a} \tag{5.2.5.5}$$

is the **modulus** of the operator a, whose name is owed to its rule in the polar decomposition $a \;=\; U|a|$ by which any bounded operator on $\mathcal{H}$ can be expressed as a product of a partial isometry U times the modulus of a, as in the usual polar decomposition $z \;=\; e^{iarg(z)}|z|$ of complex numbers.

The definition5.2.5 contains the usual norm $\|\cdot\|$ of the $W^\star$-algebraic structure of $B(\mathcal{H})$ as the $n = \infty$ case:

$$\|a\|_\infty \;=\; \|a\| \;\; a \in B(\mathcal{H}) \tag{5.2.5.6}$$

Introduced the subspace of the finite-rank bounded operators on $\mathcal{H}$:

$$\mathcal{E}(\mathcal{H}) \;:=\; \{a \in B(\mathcal{H}) \;:\; dim(Range(a)) < +\infty\} \tag{5.2.5.7}$$

let us introduce the following sequence of operators' classes:

DEFINITION 5.2.6

n-CLASS BOUNDED OPERATORS ON $\mathcal{H}$:

$$\mathcal{C}_n(\mathcal{H}) \;:=\; completion(\mathcal{E}(\mathcal{H}), \|\cdot\|_n) \tag{5.2.5.8}$$

In particular, the operators in $\mathcal{C}_1(\mathcal{H})$ are called **trace class**, those in $\mathcal{C}_2(\mathcal{H})$ **Hilbert-Schmidt**, while the operators in $\mathcal{C}(\mathcal{H}) \;:=\; \mathcal{C}_\infty(\mathcal{H})$ are called **compact** or **infinitesimal**, this last name being owed to the rule they play, as we will see, in Noncommutative Differential Calculus.

Let us then introduce the following notion:

DEFINITION 5.2.7

DENSITY OPERATORS ON $\mathcal{H}$:

$$\mathcal{D}(\mathcal{H}) \; := \; \{\rho \in \mathcal{C}_1(\mathcal{H}) \bigcap (\mathcal{B}(\mathcal{H}))_+ \; : \; Tr\rho = 1\} \qquad (5.2.5.9)$$

The key feature of the normal states over a Von Neumann algebra $A \subseteq B(\mathcal{H})$ may then be stated as follows:

Theorem 5.2.2

ON THE DENSITY OPERATORS OF NORMAL STATES:

$$\omega \in S(A)_n \; \Leftrightarrow \; (\exists \rho_\omega \in \mathcal{D}(\mathcal{H}) \; : \; \omega(a) \; = \; Tr(\rho_\omega a) \;\; \forall a \in A) \qquad (5.2.5.10)$$

and is important essentially owing to the following:

Theorem 5.2.3

NORMALITY OF THE STATES OF NONCOMMUTATIVE SPACES WITH FINITE NONCOMMUTATIVE CARDINALITY

$$cardinality_{NC}(A) \; \in \; \mathbb{N} \; \Rightarrow \; S(A)_n \; = \; S(A) \qquad (5.2.5.11)$$

Example 5.2.1

n QUBITS' NONCOMMUTATIVE PROBABILITY SPACES

Given an n qubit probability space $(B(\mathcal{H}_2^{\bigotimes n}) \, , \, \omega)$ theorem5.2.3 implies that everything can be rephrased in terms of the more popular couple $(\mathcal{H}_2^{\bigotimes n} \, , \, \rho_\omega)$.

So, in this case when can make any noncommutative-probabilistic analysis avoiding all the algebraic machinery,e.g. according the lines developed in [Par92].

This applies, in particular, for the n qubit unbaised noncommutative probability space $(B(\mathcal{H}_2^{\bigotimes n}) \, , \, \tau_{unbiased})$.

Given an **algebraic random variable** $a \in A$ over the **algebraic probability space** (A, ω):

DEFINITION 5.2.8

n^{th} MOMENT OF a:

$$M_n(a) \; := \; \omega(a^n) \qquad (5.2.5.12)$$

Of particular rilevance are the following:

DEFINITION 5.2.9

EXPECTATION VALUE OF a:

$$E(a) \; := \; M_1(a) \qquad (5.2.5.13)$$

DEFINITION 5.2.10

VARIANCE OF a:

$$Var(a) := \sqrt{E(a^2) - (E(a))^2} \tag{5.2.5.14}$$

The information contained in the moments'- sequence of a may be usefully incorporated in the following:

DEFINITION 5.2.11

CHARACTERISTIC FUNCTION OF a:
$ZQ_a : Convergence - circle(a) \rightarrow \mathbb{C}$

$$ZQ_a(t) := \sum_{n=0}^{\infty} M_n(a) \frac{t^n}{n!} \tag{5.2.5.15}$$

where $Convergence - circle(a) := \{z \in \mathbb{C} : |z| \leq R_{Convergence-circle(a)}\}$ is the circle in the complex plane with centre the origin inside which the sum converges.

When $R_{Convergence-circle(a)} > 0$ we have that:

$$M_n(a) = \frac{d^n ZQ_a(t)}{dt^n}(t=0) \tag{5.2.5.16}$$

Given two **algebraic random variables** a e b on the **algebraic probability space** (A, ω):

DEFINITION 5.2.12

a and b are INDEPENDENT:

$$E(a^n b^m) = E(a^n) E(b^m) \ \forall n, m \in \mathbb{N} \tag{5.2.5.17}$$

Given two sets Q_1 and Q_2 of algebraic random variables on **algebraic probability space** (A, ω):

DEFINITION 5.2.13

Q_1 and Q_2 ARE INDEPENDENT:
q_1 e q_2 are independent $\forall q_1 \in Q_1 , \forall q_2 \in Q_2$

We have the following:

Theorem 5.2.4

DEPENDENCE OF NONCOMMUTATING RANDOM VARIABLES:

$$a \, and \, b \ independent \Rightarrow [a, b] = 0 \tag{5.2.5.18}$$

Given a self-adjoint algebraic random variable $a \in A_{sa}$:

DEFINITION 5.2.14

CLASSICAL PROBABILITY MEASURE OF a:
the classical probability measure μ_a induced by ω on the **spectrum** Sp(a) of a

DEFINITION 5.2.15

RESULT OF A MEASUREMENT OF a:
The classical random variable v_a on the **spectrum** Sp(a) of a having μ_a as classical probability distribution.

Given two noncommutative probability spaces $(A_1\,,\,\omega_1)$ and $(A_2\,,\,\omega_2)$ let us introduce the following notion:

DEFINITION 5.2.16

TENSORIAL PRODUCT OF $(A_1\,,\,\omega_1)$ AND $(A_2\,,\,\omega_2)$:

$$(A_1\,,\,\omega_1) \bigotimes (A_2\,,\,\omega_2) \;:=\; (A_1 \bigotimes A_2\,,\,\omega_1 \cdot \omega_2) \tag{5.2.5.19}$$

where:

$$\omega_1 \cdot \omega_2(a_1 \bigotimes a_2) \;:=\; \omega_1(a_1)\omega_2(a_2) \;\; \forall a_1 \in A_1\,,\, \forall a_2 \in A_2 \tag{5.2.5.20}$$

Clearly we have the following:

Theorem 5.2.5

AUTOMATIC INDEPENDENCE ON TENSORIAL PRODUCTS:
$a_1 \otimes \mathbb{I}$ and $\mathbb{I} \otimes a_2$ are **independent algebraic random variables** on $(A_1\,,\,\omega_1) \otimes (A_2\,,\,\omega_2)$ $\forall a_1 \in A_1\,,\, \forall a_2 \in A_2$
Given an **algebraic probability space** $(A\,,\,\omega)$:

DEFINITION 5.2.17

$(A\,,\,\omega)$ IS FACTORIZABLE:

$$\exists A_1, A_2 \; W^{\star}\text{-algebras} \;,\, \omega_1 \in S(A_1)\,,\, \omega_2 \in S(A_2) \;:\; (A\,,\,\omega) \;=\; (A_1\,,\,\omega_1) \bigotimes (A_2\,,\,\omega_2) \tag{5.2.5.21}$$

DEFINITION 5.2.18

$(A\,,\,\omega)$ IS ENTANGLED:
it is not factorizable ed A is not an I_2 - factor.

Let us consider, now, the following problem:
given a noncommutative probability space is it possible to approximate it through a classical probability space up to a given perturbative order ?.

To assign an **algebraic random variable** a on the **algebraic probability space** (A, ω) is equivalent to assign the moments'- sequence $\{M_n(a)\}_{n \in \mathbb{N}}$;

Given a **noncommutative probability space** (A, ω) and a collection $Q := \{q_1, \cdots q_n\}$ of **noncommutative random variables** on it, one could think of trying to approximate the quantum random variables contained in Q by classical random variables reproducing correctly the moments up to a certain order.

This may be formalized in the following way:

DEFINITION 5.2.19

CLASSICAL APPROXIMATION OF Q UP TO THE n^{th} ORDER:

a bijection $Ap : Q \mapsto C$, where C is a collection of classical random variables on a suitable classical probability space (M, P) such that:

$$E(q_1^{i_1} \cdots q_n^{i_n}) = \int_M dP Ap(q_1)^{i_1} \cdots Ap(q_n)^{i_n} \;\; i_1, \cdots i_n \in \mathbb{N} : \sum_{k=1}^{n} i_k \leq n \tag{5.2.5.22}$$

Given a classical approximation $Ap : Q \mapsto C$ of Q up to the n^{th} order, let us introduce the following notion:

DEFINITION 5.2.20

CHARACTERISTIC FUNCTION ASSOCIATED TO Ap:

$ZC_{Ap} : \mathbb{C}^n \to \mathbb{C}$

$$ZC_{Ap}(t_1, \cdots, t_n) := \int_M dP e^{\sum_{i=1}^{n} t_i Ap(q_i)} \tag{5.2.5.23}$$

We will have, then, clearly that:

$$E(q_1^{i_1} \cdots q_n^{i_n}) = \frac{d^{\sum_{k=1}^{n} i_k} ZC_{Ap}(t_1, \cdots, t_n)}{dt_1^{i_1} \cdots dt_n^{i_n}}(t_1 = 0, \cdots, t_n = 0) \;\; i_1, \cdots i_n \in \mathbb{N} : \sum_{k=1}^{n} i_k \leq n \tag{5.2.5.24}$$

It appears , then, clear that a classical approximation up to the n^{th} order of Q involves precisely the consideration of a series-expansion of the associated characteristic function up to the n^{th} order.

Let us introduce, now, the following fundamental notion:

DEFINITION 5.2.21

Q IS IRRIDUCIBLE TO CLASSICAL PROBABILITY UP TO THE n^{th} ORDER :

it doesn't exist a classical approximation of Q up to the n^{th} order.

Demanding to [Pet93], [Ben93] for any suppletive notion, let us now briefly recall here the basic notions concerning the theory of noncommutative dynamical systems.

Given an **algebraic probability space** (A, ω):

DEFINITION 5.2.22

ENDOMORPHISMS OF (A , ω):

$$END(A , \omega) := \{ \tau : A \rightarrow A \text{ surjective } \star \text{ - morphism of A } : \omega \in S_{\tau}(A) \} \tag{5.2.5.25}$$

where $S_{\tau}(A)$ is the set of the τ - invariant states on A.

DEFINITION 5.2.23

AUTOMORPHISMS OF (A , ω):

$$AUT(A , \omega) := \{ \tau : A \rightarrow A \text{ bijective endomorphism of } (A , \omega) \} \tag{5.2.5.26}$$

DEFINITION 5.2.24

ALGEBRAIC DYNAMICAL SYSTEM :
(A , ω , τ) such that:

- (A , ω) is an algebraic probability space
- τ is an endomorphism of (A , ω)

Remark 5.2.1

ON THE PASSAGE FROM THE HEISENBERG-PICTURE TO THE SCHRÖDINGER-PICTURE OF DYNAMICS:
We have implicitely assumed Heisenberg's picture of dynamics (in which states are fixed while observable evolve with time).
The passage to the Schrödinger picture (in which observables are fixed while states evolve with time) is, anyway, straightforward:
given a $\star$-morphism C from a $W^{\star}$-algebra B to a $W^{\star}$-algebra A:

DEFINITION 5.2.25

DUAL OF C:
the map $C_{\star} : S(A) \rightarrow S(B)$:

$$(C_{\star}\alpha)(b) := \alpha(Cb) \;\; \forall \alpha \in S(A) \, , \forall b \in B \tag{5.2.5.27}$$

Given an algebraic dynamical system (A , ω , τ):

DEFINITION 5.2.26

(A , ω , τ) IS REVERSIBILE
τ is an automorphism of (A , ω).

DEFINITION 5.2.27

(A, ω, τ) IS NONCOMMUTATIVE
(A, ω) is noncommutative

The notion of **(reversibile) algebraic dynamical system** is a noncommutative generalization of the notion of **(reversibile) classical dynamical system**.

In fact:

1. $(X, \mathcal{F}, \mu, T)$ (reversibile) classical dynamical system $\Rightarrow$ $(L^{\infty}(X,\mu), \omega_{\mu}, \tau_{T})$ (reversibile) algebraic dynamical system

   where:

$$\begin{aligned} \tau_T & \text{ automorphism of } L^{\infty}(X,\mu) \\ \tau_T(a) & \equiv a \cdot T^{-1} \end{aligned} \tag{5.2.5.28}$$

2. given a (reversibile) algebraic dynamical system (A, ω, τ) with A abelian $W^{\star}$-algebra , then equation eq.5.2.5.28 univoquely individualizes an endomorphism (automorphism) T of the assoociated classical probability space.

Such a result may be enunciated in the abstract language of Categories' Theory as the following:

Theorem 5.2.6

CATEGORY EQUIVALENCE AT THE BASIS OF NONCOMMUTATIVE PROBABILITY

The **category** having as **objects** the **classical probability spaces** and as **morphisms** the **endomorphisms (automorphisms)** of such spaces is equivalent to the **category** having as objects the **abelian algebraic probability spaces** and as **morphisms** the **endomorphisms (automorphisms)** of such spaces.

Let us now analyze the symmetries of algebraic dynamical systems: on discussing derivations on a $C^{\star}$-algebra A we have already met strongly-continuous one-parameter subgroups of AUT(A).

Given, in general, a Lie group G:

DEFINITION 5.2.28

SET OF THE AUTOMORHISMS' GROUPS OF A REPRESENTING G:

$$GR - AUT(G, A) := \{ \{\alpha_g\}_{g \in G} \text{ strongly-continuous subgroup of AUT(A) } \} \tag{5.2.5.29}$$

DEFINITION 5.2.29

SET OF THE INNER AUTOMORHISMS' GROUPS OF A REPRESENTING G:

$$GR - INN(G\,,\,A) \;:=\; \{\{\alpha_g\}_{g \in G} \,\in\, G - AUT(G\,,\,A)\;: \alpha_g \in INN(A)\, \forall g \in G\} \tag{5.2.5.30}$$

DEFINITION 5.2.30

SET OF THE OUTER AUTOMORHISMS' GROUPS OF A REPRESENTING G:

$$GR - OUT(G\,,\,A) \;:=\; \frac{GR - AUT(G\,,\,A)}{GR - INN(G\,,\,A)} \tag{5.2.5.31}$$

Mackey's notion of **system of imprimitivity** as well as its unsharp generalization, i.e the notion of **generalized system of imprimitivity** often also called **system of covariance** (cfr. e.g the 3^{th} chapter of [Pru92] and the section2.3 of [Hol99]), may be generalized to the Quantum Probability's framework in the following way:

DEFINITION 5.2.31

COVARIANCE SYSTEM ON A W.R.T. G:
a couple $(E\,,\,\{\alpha_g\}_{g \in G})$ such that:

- $E \in \overset{\circ}{MAP}\,(X, A_+)$ is a POVM on A
- $$\{\alpha_g\}_{g \in G} \;\in\; GR - AUT(G\,,\,A) \tag{5.2.5.32}$$
- $$\alpha_g\, E(B) \;=\; E(g\, B) \;\; \forall B \in HALTING(E)\,, \forall g \in G \tag{5.2.5.33}$$

Remark 5.2.2

QUANTUM PHYSICS VERSUS NONCOMMUTATIVE SETS
He have seen in section5.1 how Von Neumann's investigations on the foundations of Quantum Mechanics led him to implicitely introduce Noncommutative Set Theory.

This was the starting point of a foundational school aimed at explicating the transition from Classical Physics to Quantum Physics in terms of the ansatz:

$$\text{commutative spaces} \;\rightarrow\; \text{noncommutative spaces}$$

The school looking at the modification of Probability Theory involved in such an ansatz as the root of the quantum peculiarity is called Quantum Probability.

Such a position is exemplified by the following words of Raymond F. Streater [Str00b]:

"It took some time before it was understood that quantum theory is a generalization of probability, rather than a modification of the laws of mechanics. This was not helped by the term quantum mechanics*; more, the Copenhagen interpretation is given in terms of probability, meaning as understood at the time. Bohr has said that the interpretation of microscopic measurements must be done in terms of classical terms, because the measuring instruments are large, and are therefore describe by classical laws. It is true, that the springs and cogs making up a measuring instrument themselves obey classical laws; but this does not mean that the* information *held on the instrument, in the numbers indicated by the dials, obey classical statistics. If the instruments faithfully measures an atomic variable, then the numbers indicated by the dials should be analyzed by quantum probability, however large the instruments is"*

Such a viewpoint pervaded Richard Feynman's thought[Hib65]:

"But far more fundamental was the discovery that in nature the laws of combining probabilities were not those of the classical probability theory of Laplace. The quantum-mechanical laws of the physical world approach very closely the laws of Laplace as the size of the objects involved in the experiment increases. Therefore the laws of probabilities which are conventionally applied are quite satisfactory in analyzing the behaviour of the roulette wheel but no the behaviour of a single electron or a photon of light"

being at the heart of his path-integral formalism based on the observation that the **Law of Composed Probabilities**:

$$P(x_1|x_3) \ = \ \sum_{x_2 \in \mathcal{E}} P(x_1|x_2)P(x_2|x_3) \tag{5.2.5.34}$$

(with $\mathcal{E}$ denoting the space of events) doesn't hold in Quantum Probability where it is replaced by the **Law of Composed Probability-amplitudes**:

$$AP(x_1|x_3) \ = \ \sum_{x_2 \in \mathcal{E}} AP(x_1|x_2)AP(x_2|x_3) \tag{5.2.5.35}$$

that, owing to the link between **probabilities** and **probabilities-amplitudes**:

$$P(x_1|x_3) \ = \ |AP((x_1|x_3)|^2 \tag{5.2.5.36}$$

implies that:

$$\begin{aligned} P(x_1|x_3) \ &= \ |\sum_{x_2 \in \mathcal{E}} AP(x_1|x_2)AP(x_2|x_3)|^2 \ = \\ &(\sum_{x_2 \in \mathcal{E}} AP(x_1|x_2)AP(x_2|x_3))^{\star} (\sum_{x_2 \in \mathcal{E}} AP(x_1|x_2)AP(x_2|x_3)) = \\ &\sum_{x_2 \in \mathcal{E}} P(x_1|x_2)P(x_2|x_3) \ + CT(x_1|x_3) \end{aligned} \tag{5.2.5.37}$$

where the non-null **correction-term**:

$$CT(x_1|x_3) \neq 0 \tag{5.2.5.38}$$

is the basis of the interference between different paths contributing to a path-integral.

It was always such a viewpoint that led Feynman [Fey99] to geniously perceive that the difference between Quantum Probability from Classical Probability implies the irreducibility of Quantum Computational Complexity Theory to Classical Computational Complexity Theory , catching the essence of Quantum Computation, as we will discuss more completely in section5.4.

To see why not only the Measure Theory, but also the geometry of noncommutative sets play a fundamental role for Quantum Physics, let us analyze the metric aspects of Quantum Information Theory.

At this regard our point of view is rather different from the usual one, being based on the following:

Remark 5.2.3

IT IS WRONG TO APPLY COMMUTATIVE GEOMETRY TO NONCOMMUTATIVE SETS

The metric aspect of Classical Information Theory is required in order of formalizing the concept of **distance** among **classical probability distributions**.

This may be done in terms of some conceptually appealing **metric** one can introduce on the **space of classical probability distributions**

Clearly the same situation appears in Quantum Information Theory, where one needs to quantify the **distance** among **quantum probability distributions**.

This has led to introduce suitable **metrics** on the space of **quantum probability distributions** generalizing the classical ones in a nice way.

In **Information Geometry**, furthermore, one goes further introducing a suitable **riemannian metric** on the **space of classical probability distributions** such to formulate many Classical Statistics' issues in a purely **riemannian-geometric** context.

So it has appeared natural to mimic such an attitude in Quantum Information Theory, giving rise to the discipline of **Quantum Information Geometry**, in which one introduces a suitable **riemannian metric** on the **space of quantum probability distributions** properly generalizing the classical one, again recasting many Quantum Statistics's issues in a **riemannian-geometric** context.

According to us, anyaway, these approaches are unsatisfactory, in that they ultimatively apply the usual **Commutative Geometry** to **noncommutative spaces**:

since the space of **space of quantum probability distributions** is a **noncommutative space** its metric properties should be formalized in terms of **noncommutative metrics**.

The same reasoning applies to **Quantum Information Geometry**: since the **space of quantum probability distributions** is a **noncommutative space** one should introduce on it a **noncommutative riemannian-geometric structure** rather than a **commutative riemannian-geometric structure**.

In the sequel we will see how this leads to an application of Alain Connes's Noncommutative Geometry in all its power and beauty.

Given the set of n elements $M := \{1, \cdots, n\}$ let us denote by $\mathcal{D}(M)$ the set of the probability distributions over M (endowed with the Borel-σ-algebra derived from the discrete topology).

Since:

$$\mathcal{D}(M) = \{\vec{p} = (p_1, \cdots, p_n) \in \mathbb{R}^n \ : \sum_{i=1}^{n} p_i = 1 \, , \, p_i \geq 0 \; i = 1, \cdots, n\} \quad (5.2.5.39)$$

we have that $\mathcal{D}(M)$ is an $(n-1)$-simplex of $\mathbb{R}^n$.

A first reasonable distance over $\mathcal{D}(M)$ it is natural to take in consideration is the following:

DEFINITION 5.2.32

CLASSICAL TRACE DISTANCE ON $\mathcal{D}(M)$:

$$D_T(\vec{p}^{(A)}, \vec{p}^{(B)}) \ := \ \frac{1}{2} \sum_{i \in M} (|p_i^{(A)} - p_i^{(B)}|) \quad (5.2.5.40)$$

The intuitive meaning of the definition5.2.32 is clarified by the following[Chu00]:

Theorem 5.2.7

CLASSICAL TRACE DISTANCE AS DISTANCE OF THE CLASSICAL PROBABILITY OF ANTIPODAL EVENTS:

$$D_T(\vec{p}^{(A)}, \vec{p}^{(B)}) \ = \ \max_{e \in 2^M} |p^A(e) \ - \ p^B(e)| \quad (5.2.5.41)$$

The natural quantum corrispective of definition5.2.32 could seem the following:

given an n-dimensional Hilbert space $\mathcal{H}$:

DEFINITION 5.2.33

QUANTUM TRACE DISTANCE ON $\mathcal{D}(\mathcal{H})$:

$$D_T(\rho^{(A)}, \rho^{(B)}) \ := \ \frac{1}{2} \| \rho^{(A)} - \rho^{(B)} \|_1 \quad (5.2.5.42)$$

It is remarkable that also in the quantum case an analogous of theorem5.2.7 holds [Chu00]:

Theorem 5.2.8

QUANTUM TRACE DISTANCE AS DISTANCE OF THE QUANTUM PROBABILITY OF ANTIPODAL EVENTS:

$$D_T(\rho^{(A)}, \rho^{(B)}) = \max_{P \in B(\mathbb{H})_+} TrP(\rho^{(A)} - \rho^{(B)}) \tag{5.2.5.43}$$

Theorem5.2.8 has an immediate operational interpretation to appreciate which we have to enter the highly insidious lands of quantum measurements.

Given a $W^\star$-algebra A:

DEFINITION 5.2.34

OBSERVATIONAL CHANNEL ON A:

$$\alpha \in CPU(C, A) \ : \ C \text{ commutative space}$$

DEFINITION 5.2.35

POSITIVE OPERATOR VALUED MEASURE (POVM) ON A :

a partial map $E \in \overset{\circ}{MAP} (X, A_+)$ such that:

- $HALTING(E)$ is a σ-algebra over a set X
- $$\sum_i E(F_i) = E(\cup_i F_i)$$
$$\forall \{F_i \in HALTING(E)\} \ : \ F_i \cap F_j = \emptyset \, , \forall i \neq j \tag{5.2.5.44}$$
- $$E(X) = \mathbb{I} \tag{5.2.5.45}$$

DEFINITION 5.2.36

PROJECTION VALUED MEASURE (PVM) ON A:

a POVM E on A such that:

$$E(F) \in \mathcal{P}(A) \ \forall F \in HALTING(E) \tag{5.2.5.46}$$

Theorem 5.2.9

NAIMARK'S THEOREM:

HP:

$$\mathcal{H} \text{ Hilbert space}$$

$$E \text{ POVM on } \mathcal{B}(\mathcal{H})$$

TH:

There exist an Hilbert space $\mathcal{K} \supset \mathcal{H}$ and a PVM $\tilde{E}$ on $\mathcal{B}(\mathcal{H})$ such that:

$$\tilde{E}(F) \;=\; P_{\mathcal{H}}\, E(F)\, P_{\mathcal{H}} \;\; \forall F \in HALTING(E)$$

where $P_{\mathcal{H}}$ is the projector from $\mathcal{K}$ to $\mathcal{H}$.

DEFINITION 5.2.37

OPERATIONAL PARTITIONS OF UNITY ON A:

$$OPU(A) \;:=\; \{\mathcal{V} \;:=\; (V_1\,, \cdots V_n)\,(n \in \mathbb{N}) \;: \\ V_i \;\in\; A_+ \;\; i = 1, \cdots, n \; and \\ \sum_{i=1}^{n} V_i^{\star} V_i \;=\; I\} \quad (5.2.5.47)$$

Given a operational partition of unity $\mathcal{V} \;:=\; (V_1\,, \cdots V_n) \;\in\; OPU(A)$:

DEFINITION 5.2.38

CHANNELS' SET OF $\mathcal{V}$:
the set $\{\alpha_1(\mathcal{V})\,, \cdots, \alpha_n(\mathcal{V})\}$, where $\alpha_i(\mathcal{V})$ is the channel (owing to theorem5.1.12) of A :

$$\alpha_i(\mathcal{V})(a) \;:=\; V_i^{\star} a V_i \;\; a \in A \qquad (5.2.5.48)$$

DEFINITION 5.2.39

REDUCTION CHANNEL OF $\mathcal{V}$:
the channel (owing to theorem5.1.12) $R(\mathcal{V}) \in CPU(A)$:

$$R(\mathcal{V}) \;:=\; \sum_{i=1}^{n} \alpha_i(\mathcal{V}) \qquad (5.2.5.49)$$

The interrelation among these notions is the following:

- a POVM $E \;:\; X \;\overset{\circ}{\rightarrow}\; A_+$ whose halting set is the Borel-σ-algebra of a topology on X may be seen as an observational channel $E \;:\; C(X) \rightarrow A$
- an observational channel $\alpha \in CPU(C, A)$ such that $cardinality_{NC}(C) \in \mathbb{N}$ indivuates an operational partition of unity

We have spent much efforts, in section5.1, to discuss a statement by Walter Thirring in which he claimed that Schödinger's positive answer to the separability issue was owed to the fact he didn't understand Von Neumann's paper on infinite tensor products.

But we are perfectly aware that if there is someone knowing exceptionally all the mirabilities of the noncommutative approach is precisely Walter Thirring, who has given in [Thi81] and [Thi83] one of its most authoritative presentations.

We have implicitely adopted such an approach in section5.2, though not exlicitely presenting its underlying axiomatization.

We will do this here, partly moving away from the basic-assumption-2.2.32 of [Thi81].

DEFINITION 5.2.40

NONCOMMUTATIVE AXIOMATIZATION OF QUANTUM MECHANICS:

any axiomatization of Quantum Mechanics assuming the following two axioms:

AXIOM 5.2.1

NONCOMMUTATIVE AXIOM ON OBSERVABLES:

The **observables** of a **quantum mechanical systems** are POVM's over a noncommutative space A, called its **observables' algebra**

AXIOM 5.2.2

NONCOMMUTATIVE AXIOM ON STATES:

The **states** of a **quantum mechanical systems** are states over its **observables' algebra**

We will assume, from here and beyond, a Noncommutative Axiomatization of Quantum Mechanics endowed with the other following axioms:

AXIOM 5.2.3

NONCOMMUTATIVE AXIOM ON DYNAMICS OF A CLOSED SYSTEM:

The dynamical evolution of a **closed quantum mechanical system** S is given by a **strongly-continuous group of inner automorphisms** of its **observables' algebra**

AXIOM 5.2.4

NONCOMMUTATIVE AXIOM ON MEASUREMENT:

If on a **quantum mechanical system** S, prepared in the state $\omega \in S(A)$, it is performed the measurement mathematically described by the operational partition of unity $\mathcal{V} := \{V_1 , \cdots , V_n\}$ then:

- during the measurement S is **open**
- by definition one says that the i^{th}**-experimental outcome occurs** if on a suitable **classical display** one reads the number $i \in \{1, \cdots , n\}$
- if the i^{th}**-experimental outcome occurs** then then S's observables' algebra evolves according to the the **channel** $\alpha_i(\mathcal{V})$

- the i^{th}-**experimental outcome occurs** with probability:

$$p_i := \omega(\alpha_i(I)) \tag{5.2.5.50}$$

Axiom5.2.3 and axiom5.2.4 are consistent owing to the following:

Theorem 5.2.10

DYNAMICS OF AN OPEN QUANTUM MECHANICAL SYSTEM:
The dynamical evolution of an **open quantum mechanical system** S is given by a **one-parameter family of channels** of its **observables' algebra**

Remark 5.2.4

NONCOMMUTATIVE AXIOMATIZATIONS AND UNBOUNDED OPERATORS:
A first natural reaction to definition5.2.40 is to ask what about unbounded operators:
if the **observables' algebra** of a quantum system is assumed to be a noncommutative space $A \subseteq \mathcal{B}(\mathcal{H})$ isn't one arbitarily throwing away all the self-adjoints elements of $\mathcal{O}(\mathcal{H}) - \mathcal{B}(\mathcal{H})$?

The answer to such an objection touches the original argument that led Irving Segal in 1947 to introduce the algebraic approach (cfr. the introduction of [Haa96]): given a self-adjoint unbounded operator T on an Hilbert space $\mathcal{H}$ the Spectral Theorem allows us to define the operator $f(T)$ for every Lebesgue-integrable function $f \in \mathcal{B}(\mathbb{R})$, the set of linears operators obtained varying f being called the **abelian $W^{\star}$-algebra generated by T** (cfr. the section7.2 of [Sim80].

Since one can look at the passage from T to f(T) simply as a relabeling of the possible experimental outcomes, the physically relevant notion is that of the **abelian $W^{\star}$-algebra generated by T**, of which one can always choose a bounded element such as e^T.

Remark 5.2.5

ON SUPERSELECTION RULES
Let us observe that axiom5.2.1 says that an observable of a quantum mechanical system is a POVM on its observables' algebra, but it doesn't say that any POVM on such an observable's algebra is an observable of the system.

Similarly, axiom5.2.2 says that a physical state of a quantum mechanical system is a state on its observables' algebra, but it doesn't say that any state on such an observable's algebra is a physical state of the system.

Finally, axiom5.2.4 tells us what happens when on a quantum mechanical system it is performed the measurement mathematically described by a partitional operation of unity, but it doesn't say that any operational partition of unity describes a possible measurement.

If on a quantum mechanical systems with observables' algebra A there exist a self-adjoint operator $a \in A_{sa}$ such that the PVM associated to it by the Spectral Theorem cannot be physical observable, one says that the system has Superselection Rules.

Remark 5.2.6

IF GOD PLAYS DICES IS A KINEMATICAL ISSUE AND NOT A DYNAMICAL ONE

The way axiom5.2.4 is formalized may be partially misleading owing to the fact that it would seem to introduce a **dynamical indeterminism** in the theory.

This is not the case: we spoke about of collection $\{\alpha_i\}$ of possible dynamical evolutions, each with a classical probability p_i of occurring, only for simplicity, but it is exactly the same as saying the that the observable's algebra evolves according to the **reduction channel** $R(\mathcal{V})$ of $\mathcal{V}$

We can now appreciate the physical meaning of Theorem5.2.8: it tells us that $D_T(\rho_1, \rho_2)$ is the maximal distance of the classical probabilities of a measurement outcome between the case in which the state before the measurement is ρ_1 and the case in which the state before the measurement is ρ_2.

Trace distance is not, anyway, the only reasonable distance over $\mathcal{D}(M)$ one can introduce.

An other example is the following:

DEFINITION 5.2.41

CLASSICAL ANGLE DISTANCE ON $\mathcal{D}(M)$:

$$D_A(\vec{p}^{(A)}, \vec{p}^{(B)}) \ := \ \arccos F(\vec{p}^{(A)}, \vec{p}^{(B)}) \qquad (5.2.5.51)$$

where:

DEFINITION 5.2.42

CLASSICAL FIDELITY ON $\mathcal{D}(M)$:

$$F(\vec{p}^{(A)}, \vec{p}^{(B)}) \ := \ \sum_{i \in M} \sqrt{p_i^{(A)} \, p_i^{(B)}} \qquad (5.2.5.52)$$

The name **angle distance** is justified by the following considerations: the vectors $\vec{\xi}^{(A)} = \begin{pmatrix} \sqrt{p_1^A} \\ \vdots \\ \sqrt{p_n^A} \end{pmatrix}, \vec{\xi}^{(B)} = \begin{pmatrix} \sqrt{p_1^B} \\ \vdots \\ \sqrt{p_n^B} \end{pmatrix}$ belong to the n-sphere of unitary radius $S^{(n)}$.

So $D(p_1, p_2)$ is precisely the angle between $\vec{\xi_1}$ and $\vec{\xi_2}$, i.e. the geodesic distance between them on the riemannian manifold $(S^{(n)}, g_{S^{(n)}})$, $g_{S^{(n)}} := i^{\star} \delta$

being the metric induced on $S^{(n)}$ by its inclusion's embedding $i : S^{(n)} \rightarrow \mathbb{R}^n$ in the euclidean space $(\mathbb{R}^n , \delta)$ [Nak95].

The quantum corrispective of definition5.2.41 used by the Quantum Computation's community is the following:

DEFINITION 5.2.43

QUANTUM ANGLE DISTANCE ON $\mathcal{D}(\mathcal{H})$:

$$D_A(\rho^{(A)}, \rho^{(B)}) \ := \ \arccos F(\rho^{(A)}, \rho^{(B)}) \qquad (5.2.5.53)$$

where:

DEFINITION 5.2.44

QUANTUM FIDELITY ON $\mathcal{D}(\mathcal{H})$:

$$F(\rho^{(A)}, \rho^{(B)}) \ := \ Tr \sqrt{\sqrt{\rho^{(A)}} \rho^{(B)} \sqrt{\rho^{(A)}}} \qquad (5.2.5.54)$$

A geometric interpretation of the **quantum angle distance** analogous to the classical one is furnished by the following:

Theorem 5.2.11

FIRST UHLMANN'S THEOREM:

HP:

$$\rho^{(A)} \, , \, \rho^{(B)} \ \in \ \mathcal{D}(\mathcal{H})$$

TH:

$$F(\rho^{(A)} \, , \, \rho^{(B)}) \ = \ \max_{|\psi_A> \in PUR(\rho^{(A)}, \mathcal{H}) \, , \, |\psi_B> \in PUR(\rho^{(B)}, \mathcal{H})} | < \psi_A | \psi_B > |$$

where, given two generical Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ and a density matrix $\rho \in \mathcal{D}(\mathcal{H}_A)$:

DEFINITION 5.2.45

PURIFICATIONS OF ρ WITH RESPECT TO $\mathcal{H}_B$:

$$PUR(\rho \, , \, \mathcal{H}_B) \ := \ \{ |\psi > \in \mathcal{H}_A \bigotimes \mathcal{H}_B \ : \ Tr_{\mathcal{H}_B} |\psi > = \ \rho \} \qquad (5.2.5.55)$$

So the cosin of the angle distance between two density matrices is equal to the maximum inner product between purifications of such density matrices.

The **quantum angle distance** is not, anyway, the only possible quantum corrispective of definition5.2.41 that, as many other notions, had been extensively studied in the Mathematical-Physics' literature, many years before the Quantum Computation's community rediscovered it.

Indeed the geometric interpretation of the **classical angle distance** between two distributions as the geodesic distance on the unit sphere among their square-root densities, may be seen as the first taste of **Classical Information Geometry**, namely the approach to Classical Probability Theory studying the set of all the probability measures on a given sample space from a differential-geometric viewpoint [Č82], [Ama85].

Indeed, the more relevant application of Information Geometry concerns **Statistical Estimation**:

given a submanifold $N \subset \mathbb{R}^m$.

DEFINITION 5.2.46

CLASSICAL STATISTICAL MODEL WITH SAMPLE SPACE M AND PARAMETER SPACE N:

$$CSM(M,N) := \{ \vec{\xi}(\theta) = \begin{pmatrix} \xi_1(\theta) \\ \vdots \\ \xi_n(\theta) \end{pmatrix} :$$
$$\xi_i(\theta) = \sqrt{p_i(\theta)} \, , \vec{p}(\vec{\theta}) := \begin{pmatrix} p_1(\theta) \\ \vdots \\ p_n(\theta) \end{pmatrix} \in \mathcal{D}(M) \, \forall \theta := \begin{pmatrix} \theta_1 \\ \vdots \\ \theta_m \end{pmatrix} \in N \} \quad (5.2.5.56)$$

So a **classical statistical model** $CSM(M,N)$ with **sample space** M and **parameter space** N is a collection of square-roots probability distributions over M parametrized through points of N.

By construction $CSM(M,N)$ is a submanifold of S^n.

As we will know show, definition5.2.41 naturally induces a riemannian metric on $CSM(M,N)$, called the **Fisher-Rao riemannian metric**, playing a key rule, through the Cramer-Rao Inequality, in the theory of the statistical inference of $\vec{\theta}$ (or, more generally, a suitable function of it), from a finite set of statistical data.

Given a function $f \in C^{\infty}(N, \mathbb{R})$ and a parametrized family of classical random variables $X(\vec{\theta})$ over M with distribution $p(x|\vec{\theta})$:

DEFINITION 5.2.47

$X(\vec{\theta})$ IS AN UNBAISED ESTIMATOR OF THE FUNCTION f:

$$E[X(\vec{\theta})] \; = \; f(\vec{\theta}) \;\; \forall \vec{\theta} \in N \qquad (5.2.5.57)$$

The meaning of definition5.2.47 lies in that from sampling of X we get some information about the function $f(\vec{\theta})$ we want to estimate.

Clearly, the smaller is the variance of $X(\vec{\theta})$ the higher is the classical information we gain by the estimation process.

The Cramer-Rao inequality states the existence of an upper bound about such information.

What is surprising in that, is the simple geometric nature underlying such a bound.

Let us introduce the following:

DEFINITION 5.2.48

FISHER-RAO RIEMANNIAN METRIC:

the riemannian metric over CSM (M , N):

$$g_{CSM(M,N)} \;:=\; g_N|_{CSM(M,N)} \;=\; i^{\star}(\delta) \qquad (5.2.5.58)$$

where δ is again the euclidean metric on $\mathbb{R}^n$ while $i : CSM(M,N) \rightarrow \mathbb{R}^n$ is the inclusion-embedding of $CSM(M,N)$ in $\mathbb{R}^n$.

Then one has that:

Theorem 5.2.12

CRAMER RAO INEQUALITY:

$$Var[X(\vec{\theta})] \;\geq\; g^{ij}_{CSM(M,N)} \partial_i f \partial_j f \qquad (5.2.5.59)$$

where we have expressed the Fisher-Rao riemannian metric through the global coordinates $\{\theta^i\}$ over N:

$$g_{CSM(M,N)} \;=\; (g_{CSM(M,N)})_{ij} d\theta^i \bigotimes d\theta^j \qquad (5.2.5.60)$$

and where $\partial_i f \;:=\; \frac{\partial f}{\partial \theta^i}$.

We can now appreciate how the issue of finding a quantum generalization of definition5.2.41 fits in the more ambitious process of constructing a **Quantum Information Geometry** playing in **Quantum Estimation Theory** the same rule **Classical Information Geometry** plays in **Classical Estimation Theory**.

Such a project has been pursued extensively by many authors [Pet97], [Sud99] [Hug98], [Str00a], conceptually in the framework of Helstrom's Quantum Statistical Decision Theory for a modern presentation of which we demand to the section2.2 of [Hol99].

All the proposed approaches, anyway, or reconduct the quantum case to the classical one (e.g. the approach by Brody and Hughston based on an application of the Fisher riemannian metric to the horizontal lift of paths in the Stiefel bundle underlying the Aharonov-Anandan geometric phase [Boh93]) or introduce suitable riemannian geometric structures on the space of the quantum states (e.g. the riemannian geometric structure underlying Hasegawa's α-divergence, or Petz's monotone riemannian metrics [Rus98] on which we will return in section8.1 on discussing the rule of the Wigner-Araki-Dyson skew information for superselection-rules).

But then the considerations of remark5.2.3 apply.

To sketch an idea of how **Quantum Information Geometry** should be constructed in terms of noncommutative riemannian spaces, we have to go further in the construction of the noncommutative tower.

The next floor after Noncommutative Topology and Noncommutative Measure Theory is Noncommutative Differential Calculus [Con92], [Con94], [Con98].

Commutative Differential Calculus started with Leibniz's **infinitesimals** (or equivalentely Newton's fluxions).

The difficulty of furnishing a rigorous mathematical formalization of the notion of **infinitesimal** inside Commutative Analysis, led the fathers of Commutative Calculus to replace them by well-defined objects, i.e integrals, recasting the foundations of Commutative Analysis inside the boundaries of Commutative Measure Theory.

In fact, though usually used as a linguistic shortcut by physicists, statements like the following:

" Let us call $dp(x)$ the probability that a particle is found in the interval $[x, x+dx]$"

has no rigorous meaning, as can be seen observing that the natural condition that the **commutative infinitesimal** dp(x) should satisfy, namely:

$$dp(x) \ < \ \epsilon \ \ \forall \epsilon > 0 \tag{5.2.5.61}$$

obviously implies that:

$$dp(x) \ = \ 0 \tag{5.2.5.62}$$

The well-defined quantities are only the integrals:

$$\int dp(x) f \tag{5.2.5.63}$$

of suitable functions.

So the fate of the poor infinitesimal dp(x) was very sick until Robinson's Nonstandard Analysis gave it a rigorous mathematical status as a nonstandard-real, though at the price of high logico-mathematical sophistications.

So it is very curious that, as we will now show the issue of defining an **infinitesimal** in a **noncommutative space** is highly simpler.

Given an Hilbert space $\mathcal{H}$ let us analyze if there is some natural way of defining an infinitesimal element of the noncommutative space $\mathcal{B}(\mathcal{H})$. Exactly as in the commutative case, then natural condition that one would require in order of considering an element $a \in \mathcal{B}(\mathcal{H})$ as an infinitesimal is that:

$$\|a\| \ < \ \epsilon \ \ \forall \epsilon > 0 \tag{5.2.5.64}$$

But in the same way eq.5.2.5.61 implies eq.5.2.5.62 one has that eq.5.2.5.64 implies that:

$$a = 0 \tag{5.2.5.65}$$

Contrary to the commutative case, anyway, the condition of eq.5.2.5.64 may be slightly modified in order of becoming meaningful, substituting the condition of eq.5.2.5.64 by the condition:

$$\forall \epsilon > 0 \, , \, \exists \text{ a subspace } E_{\epsilon} \subset \mathcal{H} \, : \, dim(E) < \infty \, and \, \|a|_{E^{\perp}}\| < \epsilon \tag{5.2.5.66}$$

Since an operator a satisfies the condition of eq.5.2.5.66 iff it is compact, it follows that the set of the infinitesimals elements of $\mathcal{B}(\mathcal{H})$ are exactly the the set $\mathcal{C}(\mathcal{H})$ of the compact operators on $\mathcal{H}$:

DEFINITION 5.2.49

$a \in \mathcal{B}(\mathcal{H})$ IS INFINITESIMAL:

$$a \in \mathcal{C}(\mathcal{H}) \tag{5.2.5.67}$$

Given a noncommutative infinitesimal $a \in \mathcal{C}(\mathcal{H})$:

DEFINITION 5.2.50

n^{th} CHARACTERISTIC VALUE OF a:

$$\mu_n(a) := \inf\{\|a\|_{E^{\perp}} \, , \, dim(E) \leq n\} \tag{5.2.5.68}$$

We can then classify the order of noncommutative infinitesimals in the following way:

given an $\alpha \in \mathbb{R}_+$:

DEFINITION 5.2.51

INFINITESIMALS OF ORDER α:

$$\mathcal{I}_{\alpha}(\mathcal{H}) := \{a \in \mathcal{C}(\mathcal{H}) \, : \, \mu_n(a) = O(\frac{1}{n^{\alpha}}) \, for \, n \rightarrow \infty\} \tag{5.2.5.69}$$

The next step in the construction of Noncommutative Calculus is the definition of noncommutative integration.

Given a trace-class operator $a \in \mathcal{C}_1(\mathcal{H})$ one would be tempted to define its noncommutative integral over $\mathcal{B}(\mathcal{H})$ simply as its trace:

$$Tr(a) := \sum_n < \psi_n | a | \psi_n > \tag{5.2.5.70}$$

that is independent from the choice of the orthonormal basis $\{|\psi_n >\}$ of $\mathcal{H}$.

Since the characteristic values $\mu_0(a) \geq \mu_1(a) \geq \cdots \mu_n(a) \to 0$ of an operator $a \in \mathcal{B}(\mathcal{H})$ are nothing but the eigenvalues of $|a|$ one has that:

$$Tr(a) \;=\; \sum_{n=0}^{\infty} \mu_n(a) \;\; \forall a \in (\mathcal{B}(\mathcal{H}))_+ \tag{5.2.5.71}$$

But let us now observe that a reasonable notion of noncommutative integration has to satisfy the following constraints:

1. **the integral of infinitesimals of order one must converge**

$$\int_{NC} a \;<\; +\infty \;\; \forall a \in \mathcal{I}_1(\mathcal{H}) \tag{5.2.5.72}$$

2. **the integral of infinitesimals of order greater than one must vanish**

$$\int_{NC} a \;<\; 0 \;\; \forall a \in \mathcal{I}_\alpha(\mathcal{H}), \alpha > 1 \tag{5.2.5.73}$$

Since $\mathcal{I}_1(\mathcal{H}) \;\not\subseteq\; \mathcal{C}_1(\mathcal{H})$ the simple trace Tr(a) doesn't satisfy the constraint of eq.5.2.5.72. Furthermore it doesn't satisfy also eq.5.2.5.73.

Hence it doesn't work.

A good notion of noncommutative-integral was, instead, obtained by J. Dixmier starting from the observation that:

$$\sum_{n=0}^{\infty} \mu_{n-1}(a) \;\stackrel{\times}{\leq}\; \log n \tag{5.2.5.74}$$

So he introduced a quantity, now called the Dixmier trace, that, informally speaking, extracts the coefficient of the logarithmic divergence.

Though in all the more important cases it is given simply by:

$$\lim_{n \to \infty} \frac{1}{\log n} \sum_{n=0}^{n-1} \mu_n(a) \tag{5.2.5.75}$$

in the general case such an expression presents two problems: its linearity and its convergence.

Given an infinitesimal $a \in \mathcal{C}(\mathcal{H})$ let us consider the argument of the limit at the r.h.s. of eq.5.2.5.75, namely:

$$\gamma_n(a) \;:=\; \frac{1}{\log n} \sum_{n=0}^{n-1} \mu_n(a) \tag{5.2.5.76}$$

Since it obeys the relation [Con94]:

$$\gamma_n(a_1 + a_2) \;\leq\; \gamma_n(a_1) + \gamma_n(a_2) \;\leq\; \gamma_{2n}(a_1 + a_2)(1 + \frac{\log 2}{\log n}) \tag{5.2.5.77}$$

we see that linearity would follow from convergence.

Unfortunately, though always bounded, the sequence $\{\gamma_n\}$ doesn't always converge.

Considered the Banach space of bounded sequences $l^{\infty}(\mathbb{N})$ let us introduce the space of all the linear forms $\lim_{\omega}$ on it such that:

1. $$\gamma_n \leq 0 \Rightarrow \lim_{\omega} \gamma_n \leq 0 \quad (5.2.5.78)$$

2. $$\exists \lim_{n \to +\infty} \gamma_n \Rightarrow \lim_{\omega} \gamma_n = \lim_{n \to +\infty} \gamma_n \quad (5.2.5.79)$$

3. $$\lim_{\omega} \{(\gamma_n)^n\} = \lim_{\omega} \gamma_n \quad (5.2.5.80)$$

4. $$\lim_{\omega} \gamma_{2n} = \lim_{\omega} \gamma_{2n} \quad (5.2.5.81)$$

To each of such linear forms $\lim_{\omega}$ (they are infinite) it is associated a **Dixmier trace**, according to the following:

DEFINITION 5.2.52

DIXMIER TRACE OF $a \in (\mathcal{B}(\mathcal{H}))_{+} \bigcap \mathcal{I}_1(\mathcal{H})$:

$$tr_{\omega}(a) := \lim_{\omega} \gamma_n = \lim_{\omega} \frac{1}{\log n} \sum_{n=0}^{n-1} \mu_n(a) \quad (5.2.5.82)$$

By eq.5.2.5.77 it follows that a Dixmier trace is additive on positive infinitesimals of order one, so that, owing to eq.5.2.5.77, it can be extended by linearity to the whole $\mathcal{I}_1(\mathcal{H})$.

That a Dixmier trace is indeed a trace,i.e. that:

$$tr_{\omega}(\alpha(a)) = tr_{\omega}(a) \;\; \forall a \in \mathcal{I}_1(\mathcal{H}), \forall \alpha \in INN(\mathcal{B}(\mathcal{H})) \quad (5.2.5.83)$$

follows immediately by the unitary invariance of the characteristic values of an infinitesimal a owed to the fact that they are nothing but the eigenvalues of $|a|$.

Since any linear form lim_{ω} assumes only finite values, a Dixmier trace satisfies by construction the first constraint, namely eq.5.2.5.72, we required for a reasonable notion of noncommutative integration.

Furthermore, since the space of all infinitesimal of order higher than one is a two-sided ideal whose elements satisfy the condition:

$$\lim_{n \to \infty} \mu_n(a) = 0 \quad (5.2.5.84)$$

and so:

$$\lim_{n \to \infty} \gamma_n \qquad (5.2.5.85)$$

it follows that a Dixmier trace satisfies also the second constraint, namely eq.5.2.5.73, we ask to a noncommutative integral.

After **noncommutative integration** let us pass to **noncommutative differentiation**.

Let us observe, at this purpose, that a key rule of commutative differentiation is given by Leibniz's rule for the differential of products:

$$d(f_1 f_2) \;=\; d(f_1) f_2 \;+\; f_1 d(f_2) \qquad (5.2.5.86)$$

So it appears natural to attempt to characterize the notion of noncommutative differentiation imponing that eq.5.2.5.86 holds in the noncommutative case too. The resulting notion, introduced by Kaplansky in 1953, is that of a derivation [Sak91], namely the following:

DEFINITION 5.2.53

DERIVATION ON A $C^{\star}$-ALGEBRA A:

a linear operator $\delta : D(\delta) \to A$ from a $\star$-subalgebra $D(\delta)$ to A such that:

$$\delta(ab) \;:=\; \delta(a)b \;+\; a\delta(b) \;\; \forall a, b \in D(\delta) \qquad (5.2.5.87)$$

Given a derivation δ on a $C^{\star}$-algebra A:

DEFINITION 5.2.54

δ IS AN INVOLUTIVE DERIVATION ($\star$- DERIVATION):

$$\delta(a^{\star}) \;=\; \delta(a)^{\star} \;\; \forall a \in D(\delta) \qquad (5.2.5.88)$$

Let us now observe that we are used, by Functional Analysis, to the fact that the assignment of a one-parameter strongly continuous group (or semigroup) of operators is equivalent to the assignment of its generator:

- by the Stone's Theorem [Sim80] we know that the assignment of a strongly continuous one-parameter group U(t) of unitary operators on an Hilbert space $\mathcal{H}$ is equivalent to the assignment of its generator, namely the (unique) self-adjoint operator A such that:

$$U(t) \;=\; e^{itA} \;\; \forall t \in \mathbb{R} \qquad (5.2.5.89)$$

- by the Hille-Yosida's Theorem [Sim75] we know that the assignment of a strongly continuous one-parameter semigroup C(t) of contractions on an Hilbert space $\mathcal{H}$ is equivalent to the assignment of its generator, namely the (unique) self-adjoint operator A such that:

$$C(t) \;=\; e^{-tA} \;\; \forall t \in \mathbb{R}_{+} \qquad (5.2.5.90)$$

So we are not surprised that a similar situation occurs also for strongly continuous one-parameter subgroups of the automorphisms' group AUT(A) of a generic $C^{\star}$ algebra.

Demanding to the paragraph3.4 of [Sak91] for details it is sufficient here to recall that exactly as Edward Nelson's notion of analytic vectors allows to construct directly the exponential e^{A} of a self-adjoint operator A as a power series, the same happens in our operator-algebraic setting allowing to define, as a series-power, the exponential e^{δ} of an involutive derivation δ on a $C^{\star}$-algebra.

Then one has the following:

Theorem 5.2.13

ON THE GENERATORS OF STRONGLY CONTINUOUS ONE-PARAMETER GROUPS OF AUTOMORPHISMS

HP:

$$A \ \ C^{\star} - algebra$$

$(\alpha_{t})_{t \in \mathbb{R}}$strongly continuous one-parameter subgroup of AUT(A)

TH:

$$\exists! \, \delta \ \star\text{-derivation on A} \ : \ (\alpha_{t} \ = \ e^{t \delta} \ \ \forall t \in \mathbb{R})$$

Let us then consider the particular case of one-parameter groups of inner automorphisms.

Theorem5.2.13 immediately implies the following:

Corollary 5.2.1

HP:

$$A \ \ C^{\star} - algebra$$

$(\alpha_{t})_{t \in \mathbb{R}}$ strongly continuous one-parameter subgroup of INN(A)

$$\delta \text{ generator of the group } (\alpha_{t})_{t \in \mathbb{R}}$$

TH:

$$\exists!\, D \in A_{sa} \,:\, \delta(a) \,=\, i\,[D,a]\,\forall a \in A$$

Let us now introduce the following notion:

DEFINITION 5.2.55

SPECTRAL TRIPLE:
a therne $(A\,,\,\mathcal{H}\,,\,D)$ such that:

- $\mathcal{H}$ is an Hilbert space
- $A \subseteq \mathcal{B}(\mathcal{H})$ is a $\star$ - subalgebra of $\mathcal{B}(\mathcal{H})$
- D is a self-adjoint operator on $\mathcal{H}$ such that:

$$[D,a] \;\in\; \mathcal{B}(\mathcal{H}) \;\; \forall a \in A$$
$$(D-\lambda)^{-1} \;\in\; \mathcal{C}(\mathcal{H}) \;\; \forall \lambda \in \mathbb{C} - \mathbb{R}$$

Given a spectral triple $(A\,,\,\mathcal{H}\,,\,D)$:

DEFINITION 5.2.56

$(A\,,\,\mathcal{H}\,,\,D)$ IS EVEN:
there is a $\mathbb{Z}_2$ grading on $\mathcal{H}$,i.e. an operator Γ on $\mathcal{H}$ such that:

$$\Gamma^\star \;=\; \Gamma \tag{5.2.5.91}$$
$$\Gamma^2 \;=\; 1 \tag{5.2.5.92}$$
$$\{\Gamma, D\} \;:=\; \Gamma D \;-\; D\Gamma \;=\; 0 \tag{5.2.5.93}$$
$$[\Gamma, a] \;=\; 0 \;\; \forall a \in A \tag{5.2.5.94}$$

DEFINITION 5.2.57

$(A\,,\,\mathcal{H}\,,\,D)$ IS ODD:
it is not even

Given an $n > 0$:

DEFINITION 5.2.58

$(A\,,\,\mathcal{H}\,,\,D)$ HAS DIMENSION n $\;(dim([\,(A\,,\,\mathcal{H}\,,\,D)\,]) \;=\; n)$:

$$|D|^{-1} \in \mathcal{I}_{\frac{1}{n}}(\mathcal{H}) \tag{5.2.5.95}$$

We can at last formalize all the previously machinery about noncommutative differentiation and integration in the following way:
given an n-dimensional spectral triple $(A\,,\,\mathcal{H}\,,\,D)$

DEFINITION 5.2.59

NONCOMMUTATIVE INTEGRAL OF $a \in A$:

$$\int_{NC} a := \frac{1}{V} tr_{\omega} a |D|^{-n} \tag{5.2.5.96}$$

where V is a normalization factor such that:

$$\int_{NC} I := \frac{1}{V} tr_{\omega} |D|^{-n} = 1 \tag{5.2.5.97}$$

By the previously discussed properties of the Dixmier trace one has that:

Theorem 5.2.14

BASIC PROPERTIES OF THE NONCOMMUTATIVE INTEGRAL IN A SPECTRAL TRIPLE:

1. $$\int_{NC} ab = \int_{NC} ba \ \ \forall a, b \in A \tag{5.2.5.98}$$

2. $$\int_{NC} a^{\star} a \geq 0 \ \ \forall a \in A \tag{5.2.5.99}$$

3. $$\int_{NC} a = 0 \ \ \forall a \in \mathcal{I}_{\alpha}(\mathcal{H}) \, , \, \alpha > 1 \tag{5.2.5.100}$$

Then:

DEFINITION 5.2.60

NONCOMMUTATIVE DIFFERENTIAL OF $a \in A$:

$$d_{NC} a := [D, a] \tag{5.2.5.101}$$

Example 5.2.2

QUANTIZED CALCULUS ON THE CIRCLE AND MANDELBROT'S SET

Let us consider the spectral triple $(A \, , \, \mathcal{H} \, , \, D)$, where:

- $$\mathcal{H} := L^{2}(S^{(1)}, d\vec{x}_{Lebesgue}) \tag{5.2.5.102}$$

- $$A := L^{\infty}(S^{(1)}, d\vec{x}_{Lebesgue}) \tag{5.2.5.103}$$

  where a function $f \in A$ is seen as a multiplication operator:

  $$(f\psi)(t) := f(t)\psi(t) \ \ f \in A, \psi \in \mathcal{H} \tag{5.2.5.104}$$

- D is the linear operator on $\mathcal{H}$ defined by:

$$De_n \; := \; sign(n)e_n \, , \, e_n(\theta) \; := e^{in\theta} \; \forall \theta \in S^{(1)} \tag{5.2.5.105}$$

Let us now consider again the quadratic maps on the complex plane $p_c(z) := z^2 + c$ we considered in section1.6.

Demanding to 14^{th} chapter of [Fal90] for details it will be sufficient to our purposes to remind that the Julia set of the application $p_c(z)$ may be simply expressed as:

$$J[p_c(z)] \; = \; \partial \{ z \in \mathbb{C} : \sup_{n \in \mathbb{N}} |p_c^{(n)}(z)| < \infty \} \tag{5.2.5.106}$$

and that it may be proved that there exist an homeomorphism $Z : S^{(1)} \rightarrow J[p_c(z)]$.

Denoted by D the Hausdorff dimension of $J[p_c(z)]$ Alain Connes was able to prove that:

1. $|d_{NC} Z|$ is an infinitesimal of order $\frac{1}{D}$
2. $$\exists \lambda > 0 \; : \; (\int_{J[p_c(z)]} f d\Lambda_D) \; = \; \lambda \int_{NC} f(Z) |D|^{-1} |d_{NC} Z|^D \;\; \forall f \in C(J[p_c(z)]) \tag{5.2.5.107}$$

   where $d\Lambda_D$ is the Hausdorff measure on $J[p_c(z)]$.

The eq.5.2.5.107 tells us that the integral w.r.t. the Hausdorff measure of continuous functions over the Julia set $J[p_c(z)]$ may be computed as a noncommutative integral in the spectral triple $(A \, , \, \mathcal{H} \, , \, D)$.

Since the Mandelbrot's set $\mathcal{M}$ we introduced by definition1.6.6 is linked to the family of Julia sets $J[p_c(z)]$ by the condition:

$$\mathcal{M} \; = \; \{ c \in \mathbb{C} \; : \; J[p_c(z)] \text{ is connected } \} \tag{5.2.5.108}$$

eq.5.2.5.107 could be useful to investigate some of the still unknown properties of $\mathcal{M}$

So, up to this point, we have seen how the notion of a spectral triple implements Noncommutative Calculus.

We shall now see that it, indeed, makes much more: it implements Noncommutative Riemannian Geometry.

Demanding to [Nak95], [Gil95], [Lan97], [Esp98], [Fig01] for details, let us recall that a **spin structure** on an n-dimensional riemannian manifold (M, g) is a lifting of its orthonormal frame bundle $O(M) \stackrel{\pi}{\rightarrow} M$ to a bundle $S(M) \stackrel{\pi}{\rightarrow} M$, said a **spin bundle** over M, in which the structure group $O(n)$ is replaced by its universal covering group (that is by definition the spin group SPIN(n)) through the substitution of the transition functions t_{ij} by new transition functions $\tilde{t}_{ij}$ such that:

$$\phi(\tilde{t}_{ij}) \;=\; t_{ij} \tag{5.2.5.109}$$

where $\phi : SPIN(n) \mapsto SO(n)$ is the double covering.

DEFINITION 5.2.61

SPIN MANIFOLD:

a riemannian manifold (M, g) which admit a spin structure

A well known theorem of riemannian geometry states that (M, g) is a spin manifold iff its first two Stiefel-Whitney classes $w_1(M)$ and $w_2(M)$ vanish (the vanishing of $w_1(M)$ being equivalent to the orientability of M)

In this case it may, of course, admit different spin structures, corresponding to different choices of the transition functions $\tilde{t}_{ij}$.

Given an n-dimensional spin manifold (M, g) let us consider a section $\{e_a, a = 1, \cdots, n\}$ of its orthonormal frame bundle and let us relate it to the natural basis $\{\partial_\mu\}$ by the n-beins, with components e_a^μ, so that the components $\{g^{\mu\nu}\}$ of the metric g and the components $\{\eta^{ab}\}$ of the flat metric over M may be related by the equations:

$$g^{\mu\nu} \;=\; e_a^\mu e_b^\nu \eta^{ab} \tag{5.2.5.110}$$

$$\eta^{ab} \;=\; e_a^\mu e_b^\nu g_{\mu\nu} \tag{5.2.5.111}$$

We will assume, from here and beyond, that the curve indices $\{\mu\}$ are raised and lowered by the curved metric g while the flat indices $\{a\}$ are raised and lowered by the flat metric η.

Denoted by ∇ the Levi-Civita connection of (M, g) (i.e. the unique torsion free affine connection on M that is compatible with g) let us introduce its connection coefficients $\omega_{\mu a}^b$ defined by the condition

$$\omega_{\mu a}^b e^b \;:=\; \nabla_\mu e_a \;\; \mu, \nu = 1, \cdots, n \tag{5.2.5.112}$$

Let us now introduce the Clifford bundle $C(M) \xrightarrow{\pi}$ over M, whose fiber at $x \in M$ is the complexified Clifford algebra $Cliff_{\mathbb{C}}$, and the space $\Gamma(M, C(M))$ of sections on it.

Called $\mathcal{H} := L^2(M, S)$ the Hilbert space of the irreducible spin bundle over M, with the inner product given by:

$$< \psi_1 | \psi_2 > := \int_M d\mu(g) \bar{\psi}_1(x) \psi_2(x) \tag{5.2.5.113}$$

let us now introduce that the map $\gamma : \Gamma(M, C(M)) \;\rightarrow\; \mathcal{B}(\mathcal{H})$ defined by the condition:

$$\gamma^\mu(x) \;:=\; \gamma(dx^\mu) \;:=\; \gamma^a e_a^\mu \tag{5.2.5.114}$$

and extended as an algebra map requiring its linearity under linear combinations with coefficients taking values in the algebra $A := \mathcal{F}(M)$ of complex valued smooth functions over M.

$\Gamma(M, C(M))$ is as $\star$-algebra and γ is an involutive morphism.

By the definition of a Clifford algebra and by eq.5.2.5.114 the curved Dirac matrices $\{\gamma^{\mu}(x)\}$ and the flat Dirac matrices $\{\gamma^{a}\}$ obey the relations:

$$\gamma^{\mu}(x)\gamma^{\mu}(x) + \gamma^{\nu}(x)\gamma^{\mu}(x) = -2g(dx^{\mu}, dx^{\nu}) = -2g^{\mu\nu} \quad \mu, \nu = 1, \cdots, n \tag{5.2.5.115}$$

$$\gamma^{a}\gamma^{b} + \gamma^{b}\gamma^{a} = -2\eta^{ab} \quad a, b = 1, \cdots, n \tag{5.2.5.116}$$

The lift of the Levi-Civita connection to the bundle of spinors is then:

$$\nabla^{S}_{\mu} = \partial_{\mu} + \omega^{S}_{\mu} = \partial_{\mu} + \frac{1}{4}\omega_{\mu ab}\gamma^{a}\gamma^{b} \tag{5.2.5.117}$$

We can then introduce the following:

DEFINITION 5.2.62

DIRAC OPERATOR:

the linear operator D on the Hilbert space $\mathcal{H}$ given by:

$$D := \gamma \circ \nabla^{S} \tag{5.2.5.118}$$

The properties of the Dirac operator justify the following:

DEFINITION 5.2.63

CANONICAL SPECTRAL TRIPLE OF (M, g):

the n-dimensional spectral triple $(A, \mathcal{H}, D)$, where (we recall that):

1. $A := \mathcal{F}(M)$ is the algebra of all complex valued smooth functions on M
2. $\mathcal{H}$ is the Hilbert space of square integral sections (w.r.t. the the metric measure $d\mu(g)$) of the irreducible spinor bundle over M
3. D is the Dirac operator of (M, g)

If n is even the canonical spectral triple of (M, g) is even, the $\mathbb{Z}_2$-grading being given by:

$$\Gamma := \gamma^{n+1} := i^{\frac{n}{2}}\gamma^{1}\cdots\gamma^{n} \tag{5.2.5.119}$$

And now comes the first astonishing fact:

Theorem 5.2.15

THE CANONICAL SPECTRAL TRIPLE OF A SPIN MANIFOLD ENCODES ALL ITS RIEMANNIAN STRUCTURE

1. the geodesic distance d(p , q) of two points of (M,g) is given by:

$$d(p,q) \; = \; \sup_{f \in A} \{ |f(p) - f(q)| \, : \, \| [D,f] \| \leq 1 \} \;\; \forall p,q \in M \qquad (5.2.5.120)$$

2. the integration of a function $a \in A$ w.r.t. the metric measure of (M,g) is substantially given by its noncommutative integral:

$$\int_M d\mu(g) a \; = \; c(n) \int_{NC} a \;\; \forall a \in A \qquad (5.2.5.121)$$

where:

$$c(n) \; := \; 2^{n - \lfloor \frac{n}{2} \rfloor - 1} \, \pi^{\frac{n}{2}} \, \Gamma(\frac{n}{2}) \qquad (5.2.5.122)$$

By a suitable definition of an equivalence relation among spectral triples, also the converse holds, i.e., given a commutative spectral triple $(A \, , \, \mathcal{H} \, , \, D)$ there exist a closed finite-dimensional riemannian spin manifold (M,g) whose canonical spectral triple is equivalent to $(A \, , \, \mathcal{H} \, , \, D)$.

Furthermore:

- given a diffeomorphism $\phi \in Diff(M)$ of a closed finite-dimensional riemannian spin manifold (M,g) we may associate to it the automorphism α_{ϕ} of the corrispondent involutive algebra $A := \mathcal{F}(M)$, defined as:

$$\alpha_{\phi}(f)(x) \; := \; f(\phi^{-1}(x)) \;\; \forall f \in \mathcal{F}(M), \forall x \in M \qquad (5.2.5.123)$$

- given an automorphism $\alpha \in AUT(A)$ of a commutative spectral triple $(A \, , \, \mathcal{H} \, , \, D)$ there exist a diffeomorphism $\phi \in Diff(M)$ of the associated closed finite-dimensional riemannian spin manifold (M,g) such that $\alpha = \alpha_{\phi}$

All these results may then be enunciated in the abstract language of Categories' Theory as the following:

Conjecture 5.2.1

THE CATEGORY EQUIVALENCE AT THE BASIS OF NONCOMMUTATIVE GEOMETRY

The **category** having as **objects** the **closed finite-dimensional riemannian spin manifolds** and as **morphisms** the **diffeomorphisms of such manifolds** is equivalent to the **category** having as **objects** the **abelian spectral triples** and as **morphisms** the **automorphisms of the involved involutive algebras**.

We can now, at last, see how Noncommutative Geometry allows to afford Quantum Information Geometry.

Given a spectral triple $(A, \mathcal{H}, D)$ over the $W^{\star} - algebra$ A by eq.5.2.5.120 and conjecture5.2.1 it results natural to define the following noncommutative generalization of the geodesic distance among probability distributions:

DEFINITION 5.2.64

NONCOMMUTATIVE GEODESIC DISTANCE AMONG $\omega_1 \in S(A)$ AND $\omega_2 \in S(A)$:

$$d(\omega_1 \, , \, \omega_2) \; := \; \sup_{a \in A} \{ |\omega_1(a) - \omega_2(a)| \; : \; \| [D, a] \| \leq 1 \} \qquad (5.2.5.124)$$

So, given a Von Neumann algebra $A \subseteq \mathcal{B}(\mathcal{H})$, our genuinely noncommutative approach to Quantum Information Geometry is completely specified if we succeed in individuating a *"natural"* **noncommutative Dirac operator** to use in order of defining the correct spectral triple $(A \, , \mathcal{H} \, , D)$ to use for computing the distance among noncommutative probability measures by eq.5.2.64.

Let us consider, at this purpose, the commutative case:

given a spin manifold (M, g) the correct operator to use in order to obtain the correct expression for the geodesic distance, namely the Dirac operator D of (M ,g), is that obtained minimizing the action :

$$S(x, \Lambda) \; := \; Tr_{L^2(M,S)}(\chi(\frac{x^2}{\Lambda^2})) \qquad (5.2.5.125)$$

where Λ is a cut-off with the dimensions of the inverse of a length, χ is a proper cut-off function throwing away the contribution of the x^2's eigenvalues greater than Λ^2 that we will assume to be Heaviside's step function and x denotes the unknown operatorial quantity.

The action of eq.5.2.5.125 is defined on the set $OP[\mathcal{F}(M) \, , \, L^2(M, S)]$ of all the self-adjoint operators x on $L^2(M, S)$ such that $(\mathcal{F}(M) \, , \, L^2(M, S) \, , \, x)$ is a spectral triple.

The meaning of the cut-off Λ for the variational problem of eq.5.2.5.125 is the following:

1. one impose the variational condition:

$$\frac{\delta S(x, , \Lambda)}{\delta x} \; = \; 0 \qquad (5.2.5.126)$$

obtaining an equation of the form:

$$F_1[x, \Lambda] \; = \; 0 \qquad (5.2.5.127)$$

where F_1 is a certain functional of the unknown quantity x and the cut-off Λ

2. one takes the limit $\Lambda \rightarrow \infty$ in eq.5.2.5.127 obtaining a new equation of the form:

$$F_2[x] \; = \; 0 \qquad (5.2.5.128)$$

where F_2 is another functional of the only unknown operator x

By conjecture5.2.1 is appears then natural to generalize noncommutatively such a variational procedure, i.e. to choose the operator x by which to compute, via eq.5.2.64, the noncommutative geodesic distance between two states as the solution of the variational problem for the following:

DEFINITION 5.2.65

NONCOMMUTATIVE SPECTRAL ACTION FOR $(A, \mathcal{H})$:
the map $S : OP[\mathcal{H} , A] \rightarrow \mathbb{R}$ given by:

$$S[x , \Lambda] := Tr_{\mathcal{H}}(\chi(\frac{x^2}{\Lambda^2})) \tag{5.2.5.129}$$

where:

$$OP[\mathcal{H} , A] := \{x : (\mathcal{H} , A , x) \text{ is a spectral triple } \} \tag{5.2.5.130}$$

Example 5.2.3

DISTANCE OF A NONCOMMUTATIVE PROBABILITY DISTRIBUTION ON THE NONCOMMUTATIVE SPACE OF QUBITS' SEQUENCES BY THE UNBIASED ONE.

Let us apply our noncommutative-geometric approach to Quantum Information Geometry to answer the following question:

how much a given noncommutative probability distribution $\omega \in S(\Sigma_{NC}^{\infty})$ differs from the unbaised one $\tau_{unbaised}$?

According to our strategy such a distance is given by:

$$d(\omega , \tau_{unbiased}) := \sup_{\bar{x}_{NC} \in \Sigma_{NC}^{\infty}} \{ |\omega(\bar{x}_{NC}) - \tau_{unbiased}(\bar{x}_{NC})| : \| [D, \bar{x}_{NC}] \| \leq 1 \} \tag{5.2.5.131}$$

where D is the element of $OP[\mathcal{H}_{\tau_{\mathbb{Z}}} , \Sigma_{NC}^{\infty}]$ minimizing the spectral action of definition5.2.65.

Leaving, anyway, aside Quantum Information Geometry, let us investigate a more direct strategy of Quantum Statistical Inference, namely Quantum Bayesianism.

The issue of formalizing Quantum Bayesian Theory has been recentely analyzed by various authors [Oza97], [Cav00], [Sch01].

Unfortunately no one of them adopts the general language of Quantum Probability Theory, on which the mathematical foundations of the whole matter, from a less empirical point of view, lies.

An exeption to this attitude is the authorithative exposition of Quantum Statistical Decision Theory made by Alexander S. Holevo in the section2.2 of [Hol99], from which, as already happened as to Quantum Information Geometry, we will implicitly move away.

Though well-knowing that, as we will see, Bayes' Formula is nothing but a matter of conditional expectations, Holevo keeps away from its natural noncommutative generalization, namely definition5.2.66.

Indeed, according to him:

"Conditional expectations play a less important part in quantum than in classical probability, since in general the conditional expectation into a given subalgebra $\mathcal{B}$ with respect to a given state S exists only if $\mathcal{B}$ and S are related in a very special way which in a sense reduces the situation to the classical one; for more see n. 1.3 in Chapter 3." (extracted from section1.3.2 of [Hol99])

Holevo's argument, clarified in section3.1.3, is based on Takesaki's theorem, namely our theorem5.2.20; while the conseguences we will infer from this theorem we be essentially:

1. the impossibility of quantum-bayesian-subjectivism (as first remarked by Miklos Redei: cfr. the seection 8.2 of [Red98])
2. the existence of the constraint5.2.88

Holevo's claim that Takesaki's Theorem implies a reduction to the classical case is wrong, being based on the observation that, in our terminology, the constraint5.2.88, is certainly satisfied if the modular operator of S belongs to the commutant of $\mathcal{B}$; such a condition, though sufficient, is indeed far from being necessary.

Let us so start to analyze one of the deepest conseguences of **Quantum Probability Theory**: the **Bayesian Statistical Inference Theory**:

Let us consider a statistician having access only to the information concerning the all algebraic random variables belonging to a $W^{\star}$-sub-algebra $A_{accessible}$ of a quantum probability space $(A\, ,\, \omega)$.

This means that he doesn't know the state $\omega \in S(A)$ but only its restriction to the algebra $A_{accessible}$ he can test, i.e.:

$$\omega_{accessible} \;:=\; \omega|_{A_{accessible}} \;\in S(A_{accessible}) \tag{5.2.5.132}$$

Let us suppose that, at the beginning, he hasn't used even this partial available information:

according to the Bayesian Theory the best estimation of the true state ω that he can make in this situation is to assume as estimation the uniform algebraic probability distribution:

$$\omega_{A\ PRIORI} \;:=\; \tau_{unbiased} \tag{5.2.5.133}$$

Here it does arises the first problem, common both to the classical case and to the quantum case: the **canonical trace** $\tau_{unbiased}$ exists if and only if the Von Neumann algebra A is finite.

Supposed, anyway, that this is the case let us consider the **statistical-inference's problem** :

which is the optimal way by which the statistician can improve his estimation of the true state ω using the information that is available to him, i.e. using $\omega_{accessible}$?

The answer of the Bayesian Theory is inclosed in the following:

DEFINITION 5.2.66

BAYES FORMULA:

$$\omega_{A\ PRIORI}(\cdot) = \tau_{unbiased}(\cdot) \rightarrow \omega_{A\ POSTERIORI}(\cdot) := \omega_{accessible}(E_{unbiased} \cdot) \tag{5.2.5.134}$$

where $E_{unbiased} : A \mapsto A_{accessible}$ is the **conditional expectation w.r.t. $A_{accessible}$ $\tau_{unbiased}$-invariant** whose definition and properties we are going to introduce.

Given a $W^{\star}$-algebra A:

DEFINITION 5.2.67

CONDITIONAL EXPECTATION ON A W.R.T. $A_{accessible}$:

a linear map $E : A \rightarrow A_{accessible}$ such that:

1.
$$E(a) \geq 0 \ \forall a \in A_{+} \tag{5.2.5.135}$$

2.
$$E(a) = a \ \forall a \in A_{accessible} \tag{5.2.5.136}$$

3.
$$E(ab) = E(a)b \ \forall a \in A, \forall b \in A_{accessible} \tag{5.2.5.137}$$

Let us suppose that the Von Neumann algebra A and its subalgebra $A_{accessible}$ act on the Hilbert space $\mathcal{H}$, i.e. $A_{accessible} \subset A \subseteq \mathcal{B}(\mathcal{H})$. We will say that:

DEFINITION 5.2.68

A IS INJECTIVE:

$$\exists\, E : \mathcal{B}(\mathcal{H}) \rightarrow A \text{ conditional expectation on } \mathcal{B}(\mathcal{H}) \ w.r.t.\ A \tag{5.2.5.138}$$

In an epoch making result of 1976 Alain Connes proved that:

Theorem 5.2.16

$$injectivity \Leftrightarrow hyperfiniteness \tag{5.2.5.139}$$

Given a conditional expectation on A w.r.t. to $A_{accessible}$ and a state $\omega \in S(A)$:

DEFINITION 5.2.69

E IS ω-PRESERVING:

$$\omega \circ E = E \tag{5.2.5.140}$$

The issue about the existence of state-preserving conditional expectations is rather subtle involving the Tomita-Takesaki Modular Theory [Ara97].

Given a Von Neumann algebra A acting on a separable Hilbert space $\mathcal{H}$ and a vector $|\psi> \in \mathcal{H}$:

DEFINITION 5.2.70

$|\psi>$ IS CYCLIC FOR A:

$$A\,|\psi> \quad \text{is dense in } \mathcal{H} \tag{5.2.5.141}$$

DEFINITION 5.2.71

$|\psi>$ IS SEPARATING FOR A:

$$(a|\psi> = 0 \; and \; a \in A) \Rightarrow a = 0 \tag{5.2.5.142}$$

Supposing the vector $|\psi>$ to be cyclic and separating for A let us consider the linear operator $S_{|\psi>}$ on $\mathcal{H}$ defined by the condition:

$$S_{|\psi>}a|\psi> := a^{\star}|\psi> \quad a \in A \tag{5.2.5.143}$$

The operator $S_{|\psi>}$ has a closure $\bar{S}_{|\psi>}$ that can be used to introduce the following:

DEFINITION 5.2.72

MODULAR OPERATOR W.R.T. A AND $|\psi>$:

$$\Delta_{|\psi>} := S_{|\psi>}\bar{S}_{|\psi>} \tag{5.2.5.144}$$

Let us then introduce the following:

DEFINITION 5.2.73

MODULAR CONJUGATION W.R.T. A AND $|\psi>$:

the operator $J_{|\psi>}$ occurring in the polar decomposition:

$$S_{|\psi>} = J_{|\psi>}\Delta_{|\psi>}^{\frac{1}{2}} \tag{5.2.5.145}$$

The corner stone of the Modular Theory is the following:

Theorem 5.2.17

TOMITA-TAKESAKI'S THEOREM

1.

$$\Delta^{it}_{|\psi>} \, A \, \Delta^{-it}_{|\psi>} \; = \; A \;\; \forall t \in \mathbb{R} \tag{5.2.5.146}$$

2.

$$J \, A \, J \; = \; A' \tag{5.2.5.147}$$

that, in particular, justifies the following:

DEFINITION 5.2.74

GROUP OF MODULAR AUTOMORPHISMS OF A W.R.T. $|\psi>$:
the one-parameter subgroup of AUT(A):

$$\sigma^{|\psi>}_{t}(a) \; := \; \Delta^{it}_{|\psi>} \, a \, \Delta^{-it}_{|\psi>} \tag{5.2.5.148}$$

The group of modular automorphisms $\sigma^{|\psi>}_{t}$ depends on the cyclic and separating vector $|\psi> \in \mathcal{H}$, i.e. from the normal state $\omega_{|\psi>} \in S(A)$ with associated density operator $\rho_{|\psi><\psi|}$.

If one looks at outer automorphisms, anyway, such a dependence disappears:

Theorem 5.2.18

INDEPENDENCE FROM THE STATE OF THE GROUP OF OUTER MODULAR AUTOMORPHIMS:
HP:

$|\psi_1>, |\psi_2> \in \mathcal{H}$ cyclic and separating for A

TH:

$$[\sigma^{|\psi_1>}_{t}]_{OUT(A)} \; = \; [\sigma^{|\psi_2>}_{t}]_{OUT(A)} \tag{5.2.5.149}$$

The proof of theorem5.2.18 allowed Connes to introduce the following two $\star$-isomorphisms invariants of Von Neumann algebras:

DEFINITION 5.2.75

FIRST CONNES' INVARIANT OF A:

$$Inv^{(1)}_{Connes}(A) \; := \; \bigcap_{|\psi>} Spectrum(\Delta_{|\psi>}) \tag{5.2.5.150}$$

DEFINITION 5.2.76

SECOND CONNES' INVARIANT OF A:

$$Inv_{Connes}^{(2)}(A) \ := \ \{ t \in \mathbb{R} \ : \ \sigma_t^{|\psi>} \in INN(A) \} \tag{5.2.5.151}$$

by which he classified type-III factors:

DEFINITION 5.2.77

$Type(A) \ := \ III_0$:

$$cardinality_{NC}(A) = \aleph_2 \ and \ Inv_{Connes}^{(1)}(A) = \{0,1\} \tag{5.2.5.152}$$

DEFINITION 5.2.78

$Type(A) \ := \ III_1$:

$$cardinality_{NC}(A) = \aleph_2 \ and \ Inv_{Connes}^{(1)}(A) = \mathbb{R}_+ \tag{5.2.5.153}$$

DEFINITION 5.2.79

$Type(A) \ := \ III_\lambda \ (0 < \lambda < 1)$:

$$cardinality_{NC}(A) = \aleph_2 \ and \ Inv_{Connes}^{(1)}(A) = \{ \lambda^n \, , \, n \in \mathbb{Z} \} \tag{5.2.5.154}$$

Furthermore Connes proved that:

Theorem 5.2.19

SINGLENESS OF INJECTIVE FACTORS OF EACH TYPE EXCEPT III_0:
there exist a unique injective factor of each type I_n , $n \in \mathbb{N}$, I_∞, II_1, II_∞, III_λ , $\lambda \in (0,1]$

Example 5.2.4

THE HYPERFINITE III_λ ($0 < \lambda < 1$) FACTOR

To get an intuitive insight into the structure of the noncommutative space of qubits' sequences $\Sigma_{NC}^{\infty} = R$ there is nothing better than analyzing its differences with a class of purely infinite factors, usually called the Powers factors, defined in a way very similar to that we followed in example5.1.7 to define R.

It is useful, at this purpose to introduce a suitable, compact notation concerning infinite tensor products of an algebraic probability space $(A \, , \, \omega)$:

DEFINITION 5.2.80

$$\bigotimes_{n=1}^{\infty} (A \, , \, \omega) \ := \pi_{\bigotimes_{n=1}^{\infty} \omega} (\bigotimes_{n=1}^{\infty} A)'' \tag{5.2.5.155}$$

With this notation our space of qubits' sequences may be compactly expressed as:

$$\Sigma_{NC}^{\infty} \;=\; R \;=\; \bigotimes_{n=1}^{\infty} (M_2(\mathbb{C}) \,, \tau_{unbiased}) \qquad (5.2.5.156)$$

where:

$$\tau_{unbiased}(\cdot) \;=\; Tr[\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \;\cdot] \qquad (5.2.5.157)$$

A physical realization of the one-qubit unbiased quantum probability space $(M_2(\mathbb{C}) \,, \tau_{unbiased})$ is given by a $spin 1/2$ system in thermal equilibrium at temperature $T \;=\; +\infty$, as can be seen observing that the canonical-ensemble's state:

$$\omega_{CAN}(H, \beta)(\cdot) \;:=\; Tr[\frac{e^{-\beta H}}{Tr e^{-\beta H}} \;\cdot] \qquad (5.2.5.158)$$

collapses to $\tau_{unbiased}$ when $kT \;=\; \beta^{-1} \;\rightarrow\; \infty$ for any self-adjoint, bounded from below hamiltonian operator H.

Let us now introduce the following:

DEFINITION 5.2.81

POWERS FACTORS:

$$R_{\lambda} \;:=\; \bigotimes_{n=1}^{\infty} (M_2(\mathbb{C}) \,, \omega_{\lambda}) \;\; \lambda \in (0,1) \qquad (5.2.5.159)$$

where:

$$\omega_{\lambda}(\cdot) \;:=\; Tr[\begin{pmatrix} \frac{1}{1+\lambda} & 0 \\ 0 & \frac{\lambda}{1+\lambda} \end{pmatrix} \;\cdot] \qquad (5.2.5.160)$$

It may be proved that:

$$Type(R_{\lambda}) \;=\; \lambda \;\; \forall \lambda \in (0,1) \qquad (5.2.5.161)$$

By the same considerations made in the example5.1.7 we may infer that each $R_{\lambda} \,, \, \lambda \in (0,1)$ is hyperfinite and, hence, by theorem5.2.16 and theorem5.2.19, it is the only hyperfinite, type III_{λ} factor.

Clearly, for $\lambda \in [0,1)$, the state ω_{λ} is not unbiased: for $\lambda = 0$ it is simply the pure state of density matrix $|0><0|$. Then, when λ monotonically increases from 0 to 1, it becomes a mixture of $|0><0|$ and $|1><1|$ with the bias bestowing a privilege on $|0><0|$ decreasing so that it vanishes in the limit $\lim_{\lambda \rightarrow 1} R_{\lambda} \;=\; R$.

Let us now observe that definition5.2.74 defines the group of modular automorphisms of the Von Neumann algebra $A \subseteq \mathcal{B}(\mathcal{H})$ w.r.t. a pure, normal state $\omega \;\in\; \Xi(A) \bigcap S(A)_n$. In order of generalizing it to non-pure normal states we have to introduce a generalization of the modular operator, the

spatial derivative operator and the associated **noncommutative Radon-Nikodym derivative** [Pet93], [Con94].

Given an arbitrary state $\psi \in S(A)$ let us introduce the following:

DEFINITION 5.2.82

LINEAL OF ψ:

$$D(\mathcal{H}, \psi) := \{|\xi> \in \mathcal{H} : \| a|\xi> \| \leq C_{|\xi>} \psi(a a^{\star}) \ \forall a \in A\} \qquad (5.2.5.162)$$

Considered the GNS-triplet $(\mathcal{H}_{\psi}, \pi_{\psi}, |\Psi>_{\psi}$ corresponding to the state *psi* and taken any $|\xi> \in D(\mathcal{H}, \psi)$, let us introduce the following operators:

DEFINITION 5.2.83

$R^{\psi}(|\xi>) : \mathcal{H}_{\psi} \rightarrow \mathcal{H}$:

$$R^{\psi}(|\xi>) \pi_{\psi}(a) |\Psi>_{\psi} := a|\xi> \quad a \in A \qquad (5.2.5.163)$$

DEFINITION 5.2.84

$$\Theta^{\psi}((|\xi>)) := R^{\psi}(|\xi>)(R^{\psi}(|\xi>))^{\star} \qquad (5.2.5.164)$$

Fixed a $\varphi' \in A'$:

DEFINITION 5.2.85

SPATIAL DERIVATIVE OPERATOR W.R.T. φ' AND ψ:

the positive self-adjoint operator $\Delta(\varphi', \psi)$ associated by the Form Representation Theorem to the closure of the quadratic form q:

$$q(|\xi> + |\eta>) := \varphi'(\Theta^{\psi}((|\xi>))) \qquad (5.2.5.165)$$

such that:

1. $$\| \Delta(\varphi', |\xi>)^{\frac{1}{2}} |\zeta> \|^{2} = q(|\zeta> \|) \ \forall |\zeta> \in Dom(q) \qquad (5.2.5.166)$$

2. $$Dom(q) \text{ is the core of } \Delta(\varphi', |\xi>)^{\frac{1}{2}} \qquad (5.2.5.167)$$

Given now two states $\omega_1, \omega_2 \in S(A)$:

DEFINITION 5.2.86

NONCOMMUTATIVE RADON NIKODYM DERIVATIVE OF ω_1 W.R.T. ω_2:

$$(D\omega_1 : D\omega_2)_t := \Delta(\omega_1/\varphi')^{it} \Delta(\omega_2/\varphi')^{-it} \ \ t \in \mathbb{R} \qquad (5.2.5.168)$$

where the name remarks the independence from the state φ'.

One can now generalize definition5.2.74 in the following way:

given a state $\omega \in S(A)_{norm}$:

DEFINITION 5.2.87

GROUP OF MODULAR AUTOMORPHISMS OF A W.R.T. ω:
the one-parameter subgroup of AUT(A):

$$\sigma_t^{\omega}(a) \;:=\; \Delta(\omega, \varphi')^{it} a \Delta(\omega, \varphi')^{-it} \;\; a \in A \,,\, t \in \mathbb{R} \tag{5.2.5.169}$$

We have seen how theorem5.2.16 poses some constraint on the existence of conditional expectations.

As to state-preserving conditional expectation, we have at last all the required ingredients to state Takesaki's theorem ruling the whole business:

Theorem 5.2.20

TAKESAKI'S THEOREM

HP:

$$(A \,,\, \omega) \;\; \text{algebraic probability space}$$

$$A_{accessible} \;\; W^{\star}\text{-subalgebra of A}$$

TH:

1. a **conditional expectation** $E_{\omega} \,:\, A \rightarrow A_{accessible}$ **w.r.t.** $A_{accessible}$ ω - **invariant** exists **if and only if** $A_{accessible}$ **is invariant under the modular group of** ω**, namely**:
$$\sigma_t^{\omega}(a) \;\in\; A_{accessible} \;\; \forall a \in A_{accessible} \, \forall t \in \mathbb{R} \tag{5.2.5.170}$$
2. if it exists , the **conditional expectation** $E_{\omega} \,:\, A_{accessible} \rightarrow A$ **w.r.t.** $A_{accessible}$ ω - **invariant** is unique

We have at last all the necessary technical machinery to analyze how and when the Bayesian Strategy can be applied to our problem of Statistical Inference.

It is important, first of all, to underline that the state on the complete algebra A involved in the **Bayes formula** is not the state ω, that the statistician doesn't know, but the **a priori estimation of it** $\omega_{A\ PRIORI}$.

Conseguentially, for the theorem5.2.20, the involved conditional expectation $E_{\omega_{A\ PRIORI}} \,:\, A_{accessible} \rightarrow A$ exist (and in this case is unique) under the following:

DEFINITION 5.2.88

NECESSARY AND SUFFICIENT CONDITION FOR THE FEASIBILITY OF THE BAYESIAN STATISTICAL INFERENCE:

$$\sigma_t^{\omega_{A\ PRIORI}}(a) \ \in \ A_{accessible} \ \ \forall a \in A_{accessible} \, \forall t \in \mathbb{R} \tag{5.2.5.171}$$

In the classical case such a condition is always satisfied, guaranteeing that bayesian statistical inference on finite classical probability spaces is always feasible.

This doesn't happen, instead, in the quantum case with the following fundamental consequence lucidly discovered by Miklos Redei (cfr. the cap.8 of [Red98]) and confuting the point of view exposed in [Sch01].

Theorem 5.2.21

IMPOSSIBILITY OF A SUBJECTIVISTIC BAYESIAN FOUNDATION OF QUANTUM PROBABILITY THEORY

as far as **Foundations of Probability Theory** is concerned Quantum Bayesian Theory can't be used to give a **subjectivist foundation** of Quantum Probability Theory as it happens in the classical case [Smi00].

Example 5.2.5

BAYESIAN STATISTICAL INFERENCE FOR AN EINSTEIN-PODOLSKI-ROSEN PAIR

Let us consider the Einstein-Podolsky-Rosen's setting (in its reformulation in terms of spin 1/2 given by David Böhm [Boh79], [Bel93]):

Each among Alice and Bob receive from a proper source one of the two spin 1/2 particles on an **EPR pair**.

The quantum probability space of the system is ($A := M_4(\mathbb{C})$, ω), where:

$$\rho_{\omega} \ := \ |\psi >< \psi| \tag{5.2.5.172}$$

$$|\psi > := \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} \tag{5.2.5.173}$$

$$\rho_{\omega} \ = \ \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & -\frac{1}{2} & 0 \\ 0 & -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{5.2.5.174}$$

Let us now consider Alice.

She has at her disposal only the information relative to the subalgebra $A_{accessible} := M_2(\mathbb{C})$ given by the state:

$$\omega_{accessible} = \omega|_{A_{accessible}} = \tau_2 \quad (5.2.5.175)$$

The $\tau_{unbaised}$ - conditional expectation $E_{unbaised} : A \mapsto A_{accessible}$ is, simply, the orthogonal projection on$A_{accessible}$ with respect to the following:

DEFINITION 5.2.89

HILBERT-SCHIMDT SCALAR PRODUCT ON $M_n(\mathbb{C})$:

$$< a_1 | a_2 > := \tau_n(a_1^\star a_2) \quad (5.2.5.176)$$

Considered the basis $\mathbb{E}_2 := \{e_1 := \sigma_1 , e_2 := \sigma_2 , e_3 := \sigma_3 , e_4 := \mathbb{I}\}$ of $M_2(\mathbb{C})$ and the basis $\mathbb{E}_4 := \{e_{i,j} := e_i \bigotimes e_j , i,j = 1, \cdots , 4\}$ of $M_4(\mathbb{C})$, we have clearly that:

$$E_{unbaised}(\sum_{i=1}^{4}\sum_{j=1}^{4} c_{i,j} e_{i,j}) = \sum_{i=1}^{4} c_{i,4} e_i \quad (5.2.5.177)$$

Conseguentially:

$$\omega_{A\,POSTERIORI}(\sum_{i=1}^{4}\sum_{j=1}^{4} c_{i,j} e_{i,j}) = \omega_{accessible}(E_{unbaised}(\sum_{i=1}^{4}\sum_{j=1}^{4} c_{i,j} e_{i,j})) \quad (5.2.5.178)$$

namely:

$$\omega_{A\,POSTERIORI}(\sum_{i=1}^{4}\sum_{j=1}^{4} c_{i,j} e_{i,j}) = \omega_{accessible}(\sum_{i=1}^{4} c_{i,4} e_i) \quad (5.2.5.179)$$

and so:

$$\omega_{A\,POSTERIORI}(\sum_{i=1}^{4}\sum_{j=1}^{4} c_{i,j} e_{i,j}) = \tau_2(\sum_{i=1}^{4} c_{i,4} e_i) =$$

$$\sum_{i=1}^{4} c_{i,4} \tau_2(e_i) = c_{i,4} \quad (5.2.5.180)$$

Remark 5.2.7

NONCOMMUTATIVE AXIOMATIZATIONS OF QUANTUM MECHANICS AND RELATIVITY THEORY:

Looking at definition5.2.40 one could ask what about Relativity Theory:

are we in the framework of Nonrelativistic Quantum Mechanics, of Special-relativistic Quantum Mechanics or of General Relativistic Quantum Mechanics?

The answer is that it has been formulated in order of holding in any case, adding suitable further axioms:

- assuming conjecture5.2.1 it appears natural [Con98] to suppose that General Relativistic Quantum Mechanics is based on a quantum spacetime described by a spectral triple $(A_{\hbar}\,,\,\mathcal{H}_{\hbar}\,,\,D_{\hbar})$, where the observables' algebra of quantum space-time $A_{\hbar} \subseteq \mathcal{B}(\mathcal{H}_{\hbar})$ is a Von Neumann algebra acting on the Hilbert space $\mathcal{H}_{\hbar}$.

  Let us observe that, in the classical limit $\hbar \rightarrow 0$, $A_{\hbar}$ becomes commutative, so that by Conjecture5.2.1, the spectral triple $(A_{\hbar}\,,\,\mathcal{H}_{\hbar}\,,\,D_{\hbar})$ tends to a riemannian manifold $(M\,,\,g_{Riemannian})$

  The lorentzian manifold constituing the classical space-time $(M\,,\,g_{Lorentzian})$ is then recovered by a suitable non-euclidean generalization of Wick's rotation [Wit99a], based on the analytic continuation to the complex plane, and a suitable rotation, of a **global time function** (i.e. of a function $t \in \Omega^0(M)$ such that $\nabla_a t$ is a past-directed time-like vector field, whose existence is assured by the assumption of axiom6.2.1 since **global-hyperbolicity** implies **stable-causality**) having the property that its level's surfaces Σ_t are Cauchy surfaces leading to the foliation $M = \bigcup_t \Sigma_t$ of M (cfr. the 8^{th} chapter of [Wal84]).

  Denoted by n^a the unit normal vector field to the hypersurface Σ_t and called h_{ab} the riemannian metric induced on it by g_{ab} one can choose a vector field t^a on M such that $t^a \nabla_a t = 1$ such the the **lapse function**:

$$N := -t^a n_a = (n^a \nabla_a t)^{-1} \tag{5.2.5.181}$$

  and the **shift vector**:

$$N_a := h_{ab} t^b \tag{5.2.5.182}$$

  are those for coherent flows of classical test particles adapted to the chosen **foliation**, i.e. (cfr. the sections 5.4 and 11.1 of [Pru92]):

$$N = 1 \tag{5.2.5.183}$$

$$N_a = 0 \tag{5.2.5.184}$$

  so that g_{ab} may be expressed in terms of the corresponding **syncronous (Gaussian normal) coordinates** $(x^0 = t\,,\,x^1\,,\,x^2\,,\,x^3)$ as:

$$g_{Lorentzian} = dt \bigotimes dt - h_{ij} dx^i \bigotimes dx^j \tag{5.2.5.185}$$

  Prolonging the coordinate t to the complex plane and evaluating it on the imaginary axis one results in the required riemannian manifold $(M\,,\,g_{riemannian})$.

  As the Wick's rotation's operation is always named as the passage from the **minkowskian** to the **euclidean** we will refer to the introduced not-flat generalization as to the passage from the **lorentzian** to the **riemannian**.

  Since the Universe is closed by definition,it follows by axiom5.2.3 that it is described by a strongly-continuous one-parameter group of inner automorphisms.

Conjecture5.2.1 suggests that OUT(A) plays the rule of the **quantum diffeomorphims' group** of the quantum spacetime A, while inner fluctuations of the quantum spacetime, i.e. elements of INN(A) corresponds to gauge transformations, as it is supported by the INN(A)-invariance of the minimally-coupled version of definition5.2.65.

Since the dynamics is made only by gauge transformations, one may conclude that such a picture respects Rovelli's suggestion of forgetting time [Rov88], i.e. though not following Canonical Quantum Gravity but the:

" $\cdots$ gnostic subculture of workers in quantum gravity who feel that that the structure of space and time may undergo radical changes at scales of the Planck length"; from [Ish93]

it may be catalogued in the category *"Tempus Nihil Est"* of Chris Isham's classification of different approaches to the Problem of Time in Quantum Gravity [Ish93].

- an approximation to the complete quantum theory of fields coupled with gravity is that in which one considers quantum fields on a fixed, classical space-time $(M \, , \, g_{ab})$ we will suppose to be globally-hyperbolic.

  A quantum field theory on $(M \, , \, g_{ab})$ may be defined in terms of the so called Weyl algebra A of (M, g_{ab}) and the Hadamard's states on it (for whose definition we demand to the 4^{th} chapter of [Wal94]), i.e. by the collection $\{A_O\}$ of $C^{\star}$-sub-algebras of A, one for every open subset $O \subseteq M$, with A_O representing the local observables localized on O, satisfying suitable natural conditions:

$$O_1 \subseteq O_2 \Rightarrow A_{O_1} \subseteq A_{O_2} \tag{5.2.5.186}$$

$$O_1, O_2 \text{ causally disconnected } \Rightarrow [A_{O_1} \, , \, A_{O_2}] = 0 \tag{5.2.5.187}$$

$$\begin{aligned} &\exists \{\alpha_g\} \in GR - INN[Is[(M \, , \, g_{ab})] \, , \, A] : \\ &\qquad \alpha_g(A_O) = A_{g\,O} \forall g \in Is[(M \, , \, g_{ab})] \, , \forall O \subseteq M \text{ open} \end{aligned} \tag{5.2.5.188}$$

where $Is[(M \, , \, g_{ab})]$ is the isometries'-group of $(M \, , \, g_{ab})$.

In the particular case in which $(M = \mathbb{R}^4 \, , \, \eta = \eta_{\mu\nu} dx^{\mu} \bigotimes dx^{\nu})$:

$$\eta_{\mu\nu} := \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{5.2.5.189}$$

is the Minkowski space-time, the above conditions reduce to the Haag-Kastler axioms [Haa96].

- Non-relativistic Quantum Mechanics can then be recovered taking the Inonu-Wigner's contraction $c \rightarrow +\infty$ of the isometries'-group of the minkowskian space-time, namely of the Poincaré group, thus obtaining the Galilei group (cfr. e.g. the 3^{th} chapter of [Izq95])

Remark 5.2.8

QUBITS ENTERING AND EXITING BLACK-HOLES

Since, as a matter of principle, the theory of quantum-black holes is nothing but a matter of bayesian statistical inference w.r.t. a sub-$W^{\star}$-algebra $A_{accessible}$ of the Weyl's algebra of a space-time with an event-horizon, it is a matter of Quantum Information Theory.

Our knowledges in this field are infimous, but there is a thing that have often aroused our's curiosity:

the specialists of these matters (apart from some very timid allusion in [Bek01]), speak always of **classical information** attached to certain geometrical entities, **classical information** finishing lost inside or exiting from the event-horizon though they are treating quantum systems.

It seems to us that, with this regard, the high energy physics' community have not catched the great conceptual revolution of modern Quantum Information Theory:

the irreducibility of quantum information to classical information, of the qubit to the cbit

When we will at last hear about qubits entering and exiting black-holes ?

5.3 The problem of hidden points of a noncommutative space

Let us now analyze the concept of a point in a noncommutative space.

Given an abelian $W^{\star}$-algebra A we know by theorem5.1.9 that it may be seen as (i.e. it is $\star$-isomorphic to) the $C^{\star}$-algebra $C(X(A))$ of all the continuous (w.r.t the $w^{\star} - topology$) functions on the set X(A) of its **characters** that may thus be seen as the **points** of the **commutative space** A.

We want to characterize this concept more precisely.

Given a generic **algebraic space** A:

DEFINITION 5.3.1

POINTS OF A:

$$POINTS(A) := \{\omega \in S(A) : Var(a) = 0 \text{ in } (A, \omega) \ \forall a \in A\} \tag{5.3.5.1}$$

The previous considerations may then be formalized as:

Theorem 5.3.1

ON THE POINTS OF A COMMUTATIVE SPACE:

$$A \, commutative \ \Rightarrow \ POINTS(A) = \Xi(A) = X(A) \tag{5.3.5.2}$$

Remark 5.3.1

POINTS OF A COMMUTATIVE SPACE AS DIRAC-DELTA MEASURES

Given the commutative $C^{\star}$-algebra C(X) of continuous functions over the compact, Hausdorff topological space X the points of C(X) are nothing but the Dirac delta measures over X, i.e. the states of the form:

$$\delta_{x}[f(y)] := f(x) \ \ f \in C(X) \, , \, x \in X \tag{5.3.5.3}$$

Considered a probability measure μ on X and represented the classical probability space $(X \, , \, \mu)$ as the commutative probability space $(L^{\infty}(X, \mu) \, , \, \omega_{\mu})$ one has that the projections of $L^{\infty}(X, \mu)$ are nothing but the characteristic functions of μ-measurable subsets of X forming a classical logic.

Obviously the values of $L^{\infty}(X, \mu)$'s points on the projections is given by:

$$\delta_{x}[\chi_{A}] = \begin{cases} 1 & \text{if } x \in A, \\ 0 & \text{otherwise.} \end{cases} \tag{5.3.5.4}$$

Given an algebraic probability space (A, ω):

DEFINITION 5.3.2

(A, ω) IS DETERMINISTIC:

$$\omega \in POINTS(A)$$

DEFINITION 5.3.3

(A, ω) IS CLASSICALLY-NONDETERMINISTIC:
(A, ω) is nondeterministic and A is commutative

DEFINITION 5.3.4

(A, ω) IS QUANTISTICALLY-NONDETERMINISTIC:
(A, ω) is nondeterministic and A is noncommutative

where, obviously, the form of definition5.3.3 and definition5.3.4 is owed to theorem5.2.6.

The existence of points on noncommutative spaces is inficiated by the following:

Theorem 5.3.2

INDETERMINATION'S THEOREM:

$$|E(\frac{[a,b]}{2i})| \; \leq \; \sqrt{Var(a)}\sqrt{Var(b)} \;\; \forall a,b \in A \tag{5.3.5.5}$$

PROOF:

Introduced the quantity:

$$O(a,b) \; := \; \frac{a - E(a)}{\sqrt{Var(a)}} \, + \, i \frac{b - E(b)}{\sqrt{Var(b)}} \;\; a,b \in A \tag{5.3.5.6}$$

we have clearly that:

$$O(a,b) \, O(a,b)^{\star} \; \in \; A_{+} \;\; \forall a,b \in A \tag{5.3.5.7}$$

from which the thesis immediately follows ■
Theorem5.3.2 implies that:

Corollary 5.3.1

$$(A \, , \, \omega) \; deterministic \; \Rightarrow \; (E([a \, , \, b]) \; = \; 0 \;\; \forall a,b \in A) \tag{5.3.5.8}$$

from which it follows that:

Theorem 5.3.3

FIRST VON NEUMANN'S THEOREM:
HP:

A noncommutative space

$$cardinality_{NC}(A) \,=\, \aleph_0$$

TH:

$$POINTS(A) \,=\, \emptyset$$

PROOF:

By hypothesis A is ($\star$-isomorphic to) the algebra $\mathcal{B}(\mathcal{H})$ of all bounded operator on a infinite-dimensional Hilbert-space $\mathcal{H}$.

Let us assume, for simplicity, that $\mathcal{H}$ is separable.

Fixed a complete orthonormal basis $\mathbb{E} \,:=\, \{|n>\}$ of $\mathcal{H}$ let us consider the sequence $\{P_n\}$ of projectors defined by:

$$P_n \,:=\, \sum_{k=1}^{n} |k><k| \tag{5.3.5.9}$$

We have clearly that:

$$P_0 \,\preceq\, P_1 \,\preceq\, P_2 \,\preceq\, \cdots \,\preceq\, I \tag{5.3.5.10}$$

Furthermore there exist hermitian operators $\{a_n\}$ and $\{b_n\}$ such that:

$$P_n \,=\, [a_n\,,\,b_n] \;\; \forall n \in \mathbb{N} \tag{5.3.5.11}$$

Let us then suppose ad absurdum that there exist a dispersion-free state $\omega \in POINTS(A)$.

By the corollary5.3.1 one has that:

$$\omega(P_n) \,=\, \omega([a_n\,,\,b_n]) \,=\, 0 \;\; \forall n \in \mathbb{N} \tag{5.3.5.12}$$

from which it follows that $\omega \,=\, 0$. ■

As we will now show theorem5.3.3 can be generalized to higher noncommutative cardinality.

Given an algebra A and a subalgebra $B \,\subset\, A$:

DEFINITION 5.3.5

B IS A LEFT IDEAL OF A:

$$a \in A\,,\; b \in B \;\Rightarrow\; ab \,\in\, B \tag{5.3.5.13}$$

DEFINITION 5.3.6

B IS A RIGHT IDEAL OF A:

$$a \in A \, , \, b \in B \; \Rightarrow \; ba \, \in \, B \tag{5.3.5.14}$$

DEFINITION 5.3.7

B IS A TWO-SIDED IDEAL OF A:
B is both a left ideal and a right ideal of A

Given a $C^{\star}$-algebra A:

DEFINITION 5.3.8

A IS SIMPLE:

$$\nexists B \subset A \; : \text{not-trivial two-sided ideal}$$

Given an algebraic probability space:

DEFINITION 5.3.9

$(A \, , \, \omega)$ IS SIMPLE:
A is simple

Example 5.3.1

The space $\mathcal{C}_1(\mathcal{H})$ of **trace-class operators**, the space $\mathcal{C}(\mathcal{H})$ of **infinitesimals operators**, the space $\mathcal{I}_{\alpha}(\mathcal{H})$ of **order-α infinitesimals operators** are all two-sided ideals of the $W^{\star}$-algebra $\mathcal{B}(\mathcal{H})$ of all bounded operators on an Hilbert space $\mathcal{H}$.

The rule of ideals for hidden variables issues is owed to the following:

Lemma 5.3.1

ON THE NOT-TRIVIAL IDEALS
HP:

$$A \; not-trivial \; C^{\star}-algebra \; :$$

TH:

$$POINTS(A) \neq \emptyset \; \Leftrightarrow$$
$$\exists \, J \, \text{not-trivial two-sided ideal in A} \; : \frac{A}{J} \text{ is abelian} \tag{5.3.5.15}$$

PROOF:

1. Given $\phi \in POINTS(A)$ we will prove that:

$$J := \{a \in A : \phi(a) = 0\} \tag{5.3.5.16}$$

is a not-trivial two-sided ideal such that $\frac{A}{J}$ is commutative.

Obviously J is a linear subspace of A and is a subset of A_{sa}.

Furthermore, the hypothesis of not-triviality of A implies that also A is not trivial, since the existence of an $a \in A : a \neq I$ implies that also $a - \phi(a)I \neq I$ so that $a - \phi(a)I$ is a not-trivial element of J.

Let us now show that J is an ideal:

a generic element $a \in A$ may be expressed as linear combination of self-adjoint elements:

$$a = \sum_{n} c_n x_n \; c_n \in \mathbb{C}, x_n \in A_{sa} \; \forall n \tag{5.3.5.17}$$

Given $a, b \in J$ we have, by theorem5.1.7 and the fact that ϕ is a point, that:

$$|\phi(x_n b)| \leq \phi(x_n x_n^{\star})\phi(b b^{\star}) \\ = \phi(x_n^2)\phi(b^2) = 0 \;\; \forall n \tag{5.3.5.18}$$

so that:

$$\phi(ab) = 0 \tag{5.3.5.19}$$

and hence $ab \in J$, so that it is proved that J is a left-ideal.

The proof that J is also a right-ideal is specular.

To prove, finally, that $\frac{A}{J}$ is abelian let us observe that the map $h : \frac{A}{J} \rightarrow \mathcal{C}$ defined by:

$$h([a]_{\frac{A}{J}}) := \phi(a) \tag{5.3.5.20}$$

is a $\star$ -isomorphism from $\frac{A}{J}$ to $\mathcal{C}$; in fact if $\phi(a) = \phi(b)$ then $\phi(a-b) = 0$ so that $[a]_{\frac{A}{J}} = [b]_{\frac{A}{J}}$ and, consequentially, h is invertible; furthermore:

$$h([a]_{\frac{A}{J}}, [b]_{\frac{A}{J}}) = h([ab]_{\frac{A}{J}}) = \phi(ab) = \phi(a)\phi(b) \;\; \forall a, b, \in A \tag{5.3.5.21}$$

and hence h preserves the product

2. let suppose that there exist a two-sided ideal J such that $\frac{A}{J}$ is abelian. Then, by theorem5.3.1, it follows that $POINTS(A) \neq \emptyset$.

■

immediately implying the following:

Corollary 5.3.2

INDETERMINISM OF SIMPLE ALGEBRAIC PROBABILITY SPACES

$$(A\,,\,\omega) \text{ simple } \Rightarrow (A\,,\,\omega) \text{ nondeterministic}$$

Corollary5.3.2, anyway, is only the tip of an iceberg, as is stated by the following generalization of theorem5.3.3

Theorem 5.3.4

INDETERMINISM OF NONCOMMUTATIVE PROBABILITY SPACES:
HP:

$$(A\,,\,\omega) \text{ algebraic probability space}$$

TH:

$$(A\,,\,\omega) \textit{ noncommutative } \Rightarrow (A\,,\,\omega) \textit{ nondeterministic}$$

PROOF:

Proceeding exactly as in the proof of theorem5.3.3 let us consider a sequence $\{p_n\}_{n \in \mathbb{N}}$ such that:

$$p_n \in \mathcal{P}(A) \;\; \forall n \in \mathbb{N} \tag{5.3.5.22}$$

$$p_i \preceq p_j \;\; \forall i < j \tag{5.3.5.23}$$

There will exist hermitian operators $\{a_n\}$ and $\{b_n\}$ such that:

$$p_n = [a_n\,,\,b_n] \;\; \forall n \in \mathbb{N} \tag{5.3.5.24}$$

Let us then suppose ad absurdum that there exist a dispersion-free state $\omega \in POINTS(A)$.

By the corollary5.3.1 one has that:

$$\omega(p_n) = \omega([a_n\,,\,b_n]) = 0 \;\; \forall n \in \mathbb{N} \tag{5.3.5.25}$$

from which it follows that $\omega = 0$. ■

Remark 5.3.2

UNSHARP LOCALIZATION ON A NONCOMMUTATIVE SPACE:

In the commutative case a point may be characterized through a monotonically descreasing sequence of projections.

Given, for example, the unbaised probability space of cbits' sequences $(\Sigma^{\infty}, P_{unbiased})$ let us use the numeric representation map of definition1.4.4 to visualize it as the the classical probability space $([0,1), \mu_{Lebesgue})$.

A point $x \in (0,1)$ is completelly specified by a nested sequence of measurable $(0,1)$'s subsets $\{A_n\}$ whose intersection is the singleton containing x :

$$A_i \supset A_j \ \forall i < j \tag{5.3.5.26}$$

$$\{x\} = \bigcap_{n \in \mathbb{N}} A_n \tag{5.3.5.27}$$

For example one can take:

$$A_n := (x - \frac{1}{2^n}, x + \frac{1}{2^n}) \tag{5.3.5.28}$$

Let us now look at the classical probability space $([0,1), \mu_{Lebesgue})$ as at the commutative probability space $(A := L^{\infty}([0,1), \mu_{Lebesgue}), \omega_{\mu_{Lebesgue}})$.

As we saw in the remark5.3.1 the projections of $\mathcal{P}(A)$ are nothing but the characteristic functions of measurable $[0,1)$'s subsets constituting a classical logic.

The sequence $\{A_n\}$ corresponds to the sequence of projections $\{\chi_{A_n}\}$ satisfying the condition:

$$\chi_{A_i} > \chi_{A_j} \ \forall i < j \tag{5.3.5.29}$$

The point $x \in A$, i.e the point $\delta_x \in POINTS(A)$, is then characterized by the condition:

$$\delta_x(\chi_{A_n}) = 1 \ \forall n \in \mathbb{N} \tag{5.3.5.30}$$

Given, now a noncommutative space X, one could think that, though $POINTS(X) = \emptyset$, the characterization of the concept of an X's point can be recovered generalizing the above procedure, i.e finding a monotonically increasing sequence of projections $\{p_n\}$ over X:

$$p_n \in \mathcal{P}(X) \ \forall n \in \mathbb{N} \tag{5.3.5.31}$$

$$p_i > p_j \ \forall i < j \tag{5.3.5.32}$$

and a state $\omega \in \Xi(X)$ such that:

$$\omega(p_n) = 1 \ \forall n \in \mathbb{N} \tag{5.3.5.33}$$

One could, in fact, think that in such a situation it is possible, after all, to look at the sequence $\{p_n\}$ as a sequence of propositions stating the localization in a monotonically-increasing way, so that a state ω giving value one to all these propositions, i.e. in quantum-logic language , stating the truth of all these propositions, can assume a geometrical meaning as an unsharped-localized region of the noncommutative space X.

Remark 5.3.3

ON HIDDEN POINTS OF A NONCOMMUTATIVE SPACE

Given a noncommutative space $A_{accessible}$ one could think of completing it, i.e. of considering a larger noncommutative space A of which $A_{accessible}$ is a sub-$W^{\star}$-algebra, such that $POINTS(A) \neq \emptyset$.

In such a situation the indeterminism of any noncommutative probability space (A, ω) on A could then be simply attributed to the not accessibility of the algebraic random variables belonging to $A - A_{accessible}$.

That this in not the case is stated by the following obvious corollary of theorem5.3.4:

Corollary 5.3.3

NOT EXISTENCE OF HIDDEN POINTS OF A NONCOMMUTATIVE SPACE:

$$POINTS(A) = \emptyset \ \forall A \supset A_{accessible} \tag{5.3.5.34}$$

PROOF:

Since $A_{accessible}$ is noncommutative, A is noncommutative too.

The thesis follows immediately by theorem5.3.4 ■

Though not leading to a sharp localization, one could anyway think that completions can anyway improve the unsharp localization.

If this is possible or not depends sensibly from the definition of completion one assume, as we will now show.

Given a state $\beta \in S(B)$:

DEFINITION 5.3.10

CLASSICAL PROBABILITY MEASURES WITH BARYCENTER β:

the set $M_{\beta}[S(B)]$:

$$M_{\beta}[S(B)] := \{ \mu \in M[S(B)] : \beta(b) = \int_{S(B)} \omega(b) \, d\mu(\omega) \ \forall b \in B \} \tag{5.3.5.35}$$

Given a channel $\beta \in CPU(B, A)$:

DEFINITION 5.3.11

C IS A COMPLETION-CHANNEL:

$\forall \alpha \in S(A)$, $\exists \mu \in M_{C^{\star} \alpha}[S(B)]$ such that:

- **in the completion the uncertainty descreases**, i.e.:

$$\sqrt{Var_{\alpha}(Cb)} > \sqrt{Var_{\omega}(b)} \ \forall \omega \in supp(\mu) , \forall b \in B : (Cb \in A_{sa} \, and \, \sqrt{Var_{\alpha}(Cb)} > 0) \tag{5.3.5.36}$$

- **in the completion the certainty remains certain**, i.e.:

$$\sqrt{Var_{\alpha}(Cb)} \; = \; \sqrt{Var_{\omega}(b)} \; = \; 0 \;\; \forall \omega \in supp(\mu) \, ,$$
$$\forall b \in B \, : \, (Cb \, \in A_{sa} \; and \, \sqrt{Var_{\alpha}(Cb)} \; = \; 0) \quad (5.3.5.37)$$

DEFINITION 5.3.12

C IS A DETERMINISTIC-COMPLETION-CHANNEL:

- C is a completion-channel
-

$$\sqrt{Var_{\omega}(b)} \; = 0 \;\; \forall \omega \in supp(\mu) \, ,$$
$$\forall b \in B \, : \, (Cb \, \in A_{sa} \; and \, \sqrt{Var_{\alpha}(Cb)} \; > \; 0) \quad (5.3.5.38)$$

Von Neumann himself was the first to investigate the possibility of deterministic completion channels, though only of the following particular kind:

DEFINITION 5.3.13

VON NEUMANN'S COMPLETION:
a deterministic-completion-channel of the form $\mathbb{I} \in CPU(A)$ such that:

$$cardinality_{NC}(A) \; \leq \; \aleph_0 \quad (5.3.5.39)$$

formulating the first no-go theorem on hidden variables:

Theorem 5.3.5

VON NEUMANN'S NO-GO THEOREM:

$$\{ C \; : \; \text{Von Neumann's completion} \; \} \; = \; \emptyset \quad (5.3.5.40)$$

PROOF:

It immediately follows by theorem5.3.3 ■

The generalization involved in the passage from theorem5.3.3 to theorem5.3.4 induces the following generalization of theorem5.3.3:

Theorem 5.3.6

FIRST ALGEBRAIC NO-GO THEOREM:
HP:

$$A \;\; \text{algebraic space}$$

TH:

$\mathbb{I}_A$ is a deterministic-channel completion $\Leftrightarrow$ A is commutative

PROOF:

- A commutative $\Rightarrow$ $\mathbb{I}_A$ is a deterministic-channel completion

  If A is commutative we know by theorem5.1.9 that it may be seen (i.e. it is $\star$-isomorphic to) the space $C(X(A))$ of the continuous functions over the characters, i.e. the points, of A.

  By the Riesz-Markov theorem (cfr. the section 4.4 of [Sim80]) for every state $\phi \in S(C(X))$ there exist a measure μ_ϕ on X such that:

$$\phi(f) = \int_X d\mu_\phi f \ \ \forall f \in C(X) \tag{5.3.5.41}$$

  By theorem5.3.1 if follows that:

$$supp(\mu) \subseteq POINTS(A) \tag{5.3.5.42}$$

  for which the thesis follows

- $\mathbb{I}_A$ is a deterministic-channel completion $\Rightarrow$ A commutative

  Let us assume that $\mathbb{I}_A$ is a deterministic-channel completion.

  Given $x, y \in A \ : \ x > y \leq 0$ one has, by the definition5.3.11, that for every state $\phi \in S(A)$ there exists a measure $\mu \in M[S(A)]$ such that:

$$\phi(x^2) = \int_{S(A)} d\mu(\omega)\omega(x^2) = \int_{S(A)} d\mu(\omega)\omega(x)^2 \tag{5.3.5.43}$$

$$\phi(y^2) = \int_{S(A)} d\mu(\omega)\omega(y^2) = \int_{S(A)} d\mu(\omega)\omega(y)^2 \tag{5.3.5.44}$$

  Since $\omega(x) \leq \omega(y)$, it follows that:

$$\phi(x^2) - \phi(y^2) = \int_{S(A)} d\mu(\omega)(\omega(x)^2 - \omega(y)^2) \leq 0 \tag{5.3.5.45}$$

  that implies that $x^2 \geq y^2$.

  The thesis follows immediately from the property:

$$(x \geq y \rightarrow x^2 \geq y^2 \ \forall x, y \in A) \Rightarrow A \ commutative \tag{5.3.5.46}$$

■

Let us now return to the Noncommutative Bayesian Statistical Inference Theory we have outlined in section5.2:

one could think that the process of statistical inference corresponds to an improvement in the localization on a noncommutative space.

This is not ,anyway, the case, as it is stated by the following [Red98]:

Theorem 5.3.7

SECOND ALGEBRAIC NO-GO THEOREM (BAYESIAN STATISTICAL INFERENCE DOESN'T NONCOMMUTATIVELY-LOCALIZE):
HP:

$$A \text{ noncommutative space}$$

$A_{accessible} \subset A$ sub-$W^{\star}$-algebra of A satisfying the condition of definition5.2.88

TH:

$$E_{unbaised} : A \rightarrow A_{accessible} \text{ is not a channel-completion}$$

Let us conclude this section by an analysis of John Bell's contribution to the Hidden Variables' Issue.

This involves the dicussion of an (apparentely) different kind of completion, concerning the degree oif irreducibility of noncommutative probabilities to the commutative ones.

An immediate conseguence of theorem5.2.6 is the following:

Theorem 5.3.8

IRREDUCIBILITY OF NONCOMMUTATIVE PROBABILITY TO COMMUTATIVE PROBABILITY TO ANY ORDER:
HP:

$$(A , \omega) \text{ noncommutative probability space}$$

TH:

$$\exists m \in \mathbb{N} : \text{A is irreducible to Classical Probability Theory up to } m^{th} \text{ order}$$

Remark 5.3.4

IMPOSSIBILITY OF THE OSTERWALDER-SCHRADER'S PROGRAM

A consequence of theorem5.3.8 is the impossibility of founding Quantum Field Theory on the Osterwalder-Schrader axiomatization (cfr. the sixth chapter of [Jaf87] and [Haa96]).

Indeed a quantum field theory satisfying the Osterwalder-Schrader axioms obeys the Haag-Kastler axiom's too, but the conversely doesn't hold.

This implies that the formal path-integral measures comparing in euclidean field theories cannot in principle be made always rigorous since they , mathematically rigorously, cannot always exist

One the conceptually more fascinating examples of irriducibility of Quantum Probability Theory to Classical Probability Theory to a low order is given by the EPR-stuff we already introduced in the example5.2.5.

Given the noncommutative probability space (A, ω), with:

$$A := M_2(\mathbb{C}) \bigotimes M_2(\mathbb{C}) = M_4(\mathbb{C}) \tag{5.3.5.47}$$

$$\omega(\cdot) := Tr(\rho_{|\psi><\psi|} \cdot) \tag{5.3.5.48}$$

$$|\psi> := \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} \tag{5.3.5.49}$$

$$\rho_{|\psi><\psi|} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & -\frac{1}{2} & 0 \\ 0 & -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{5.3.5.50}$$

let us consider the following noncommutative random variables:

$$q_1^A := \sigma_1 \bigotimes I = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \tag{5.3.5.51}$$

$$q_2^A := \sigma_2 \bigotimes I = \begin{pmatrix} 0 & 0 & -i & 0 \\ 0 & 0 & 0 & -i \\ i & 0 & 0 & 0 \\ 0 & i & 0 & 0 \end{pmatrix} \tag{5.3.5.52}$$

$$q_3^A := \sigma_3 \bigotimes I = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \tag{5.3.5.53}$$

$$q_1^B \;:=\; I \bigotimes \sigma_1 \;=\; \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad (5.3.5.54)$$

$$q_2^B \;:=\; I \bigotimes \sigma_2 \;=\; \begin{pmatrix} 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \end{pmatrix} \qquad (5.3.5.55)$$

$$q_3^B \;:=\; I \bigotimes \sigma_3 \;=\; \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \qquad (5.3.5.56)$$

having moments:

$$M_n(q_i^A) \;=\; M_n(q_i^B) \;=\; \begin{cases} 0 & \text{n even,} \\ 1 & \text{n odd.} \end{cases} \quad i = 1, \cdots, 3 \qquad (5.3.5.57)$$

The first joint moments of the six noncommutative random variables q_1^A , q_2^A , q_3^A , q_1^B , q_2^B , q_3^B are given by:

$$E(q_i^A q_j^A) \;=\; E(q_i^B q_j^B) \;=\; \delta_{i,j} \;\; i, j = 1, \cdots, 3 \qquad (5.3.5.58)$$

$$E(q_i^A q_j^B) \;=\; E(q_i^B q_j^A) \;=\; \begin{cases} -1 & i = j, \\ 0 & i \neq j. \end{cases} \quad i, j = 1, \cdots, 3 \qquad (5.3.5.59)$$

The contribution by John Bell was to show that [Acc88] [Str95], [Str00b]:

Theorem 5.3.9

BELL'S THEOREM:

$Q \;=\; \{q_1^A , q_2^A , q_3^A , q_1^B , q_2^B , q_3^B\}$ is irreducible to classical probability up to the $2^{th} order$

PROOF:

The simple numerical property:

$$ab \,-\, bc \,+\, ac \;\leq\; 1 \;\; \forall a, b, c \in [-1\,,\, 1] \qquad (5.3.5.60)$$

implies that:

$$|ab \,-\, bc| \;\leq\; 1 \,-\, ac \;\; \forall a, b, c \in [0, 1] \qquad (5.3.5.61)$$

$$|ab \,+\, bc| \,+\, |ad \,-\, dc| \;\leq\; 1 \,+\, ac \;\; \forall a, b, c, d \in [0, 1] \qquad (5.3.5.62)$$

$$(5.3.5.63)$$

from which it follows that it don't exist four random variables a , b , c , d defined on a classical probability space (Ω , P) such that:

$$|E(ab) - E(bc)| \leq 1 - E(ac) \quad (5.3.5.64)$$

$$|E(ab) - E(bc)| \leq 1 + E(ac) \quad (5.3.5.65)$$

$$|E(ab) - E(bc)| + |E(ad) + E(dc)| \leq 2 \quad (5.3.5.66)$$

where E denotes expectation w.r.t. the P-measure:, i.e.:

$$E(F) := \int_{\Omega} F \, dP$$

The thesis easily follows ■

Remark 5.3.5

BELL'S THEOREM DOESN'T SPEAK OF LOCALITY:

Our way of presenting Bell's result is someway provocative, in that it is completely different both from the form and from the spirit of Bell's papers [Bel93]:

Bell's theorem was intended to be and is almost always looked as [Shi00] the proof that all local hidden variables' theories imply an inequality which is incompatible with some of the predictions of Quantum Mechanics.

Such inequality, anyway, is nothing but a consequence of the fact that there does not exist a set of six classical random variables $\{c_1^A , c_2^A , c_3^A , c_1^B , c_2^B , c_3^B\}$ on a suitable classical probability space, such that:

$$M_n(c_i^A) = M_n(c_i^B) = \begin{cases} 0 & \text{if } n = 0 \text{ or } n = 2, \\ 1 & \text{if } n = 0. \end{cases} \quad i = 1, \cdots , 3 \quad (5.3.5.67)$$

$$E(c_i^A c_j^A) = E(c_i^B c_j^B) = \delta_{i,j} \;\; i,j = 1, \cdots , 3 \quad (5.3.5.68)$$

$$E(c_i^A c_j^B) = E(c_i^B c_j^A) = \begin{cases} -1 & i = j, \\ 0 & i \neq j. \end{cases} \quad i,j = 1, \cdots , 3 \quad (5.3.5.69)$$

The concept of locality appears nowhere and has nothing to do with the physical meaning of theorem5.3.9 concerning the irreducibility of entanglement to Classical Probability Theory.

Remark 5.3.6

BELL'S THEOREM AND FUNCTIONAL INTEGRALS ON SUPERSPACES:

There exist a natural reaction to theorem5.3.9, that could lead to think that there must be certainly a mistake in its proof: considered a system of two uncoupled fermionic oscillators:

$$\hat{H} := \frac{1}{2}(\hat{a}_1^\dagger \hat{a}_1 + \hat{a}_2^\dagger \hat{a}_2) \quad (5.3.5.70)$$

where:

$$\hat{a}_i^2 \ = \ (\hat{a}_i^\dagger)^2 \ = \ 0 \ \ i = 1,2 \tag{5.3.5.71}$$

$$\hat{a}_i^\dagger \hat{a}_j \ + \ \hat{a}_j \hat{a}_i^\dagger \ = \ \delta_{i,j} \ \ i = 1,2 \tag{5.3.5.72}$$

every theoretical-physicists' textbook (cfr. e.g. the section 3.5 of [ZJ93]) tell us that we can compute all its correlation functions by functional derivatives of the partition function:

$$Z[\bar{\eta}_1 \, , \, \eta_1 \, , \, \bar{\eta}_2 \, , \, \eta_2] \ := \ \int [dc_1(t) dc_2(t) d\bar{c}_1(t) d\bar{c}_2(t)] \exp[-S(c_1, c_2, \bar{c}_1, \bar{c}_2) \ + \\ \int ds \sum_{i=1}^{2} \bar{\eta}_i(s) c_i(s) + \bar{c}_i(s) \eta_i(s)] \tag{5.3.5.73}$$

with euclidean action:

$$S(c_1, c_2, \bar{c}_1, \bar{c}_2) \ := \ \int dt \sum_{i=1}^{2} \bar{c}_i(t) \dot{c}_i(t) \ - \ \bar{c}_i(t) c_i(t) \tag{5.3.5.74}$$

Isn't this fact an explicit confutation of theorem5.3.9, implying the existence of the six classical random variables $\{ c_1^A \, , \, c_2^A \, , \, c_3^A \, , \, c_1^B \, , \, c_2^B \, , \, c_3^B \}$ we spoke about in the remark5.3.5?

The reason why this is not the case is that the euristic measure of equation5.3.5.73 cannot be defined in a mathematically rigorous way.

Indeed, though being at the basis of many exciting mathematical results such as the proof of the Atiyah-Singer Index Theorem by the computation of the index of the Dirac operator D on a spin-manifold $(M \, , \, g)$ as the path-integral:

$$Index(D) \ := \ \int_{p.b.c.} [dx][d\psi] \exp[- \int_0^\beta dt L] \tag{5.3.5.75}$$

where:

$$L \ := \ \frac{1}{2} g_{\mu,\nu} \dot{x}^\mu \dot{x}^\nu \ + \ \frac{1}{2} g_{\mu\nu} \psi^\mu \frac{D\psi^\mu}{Dt} \tag{5.3.5.76}$$

is the supersymmetric lagrangian of a spin-$\frac{1}{2}$ fermion living on $(M \, , \, g)$ [Alv95], a rigorous mathematical formalization of functional integration on superspaces (going beyond informal time-splitting procedures such as that of the fifth chapter of [Wit92]) doesn't exist yet.

It may be worth mentioning the possibility that it could require an extension of the Kolmogorov's Axiomatization of Probability rather than simply an application of it, and could in this way converge to Quantum Probability Theory, as the section5.3 of [Khr99] and the intellectual path of its author could suggest

5.4 Irreducibility of Quantum Computational Complexity Theory to Classical Computational Complexity Theory

Chapter 6

Quantum algorithmic randomness: where are we?

6.1 The unpublished ideas of Sidney Coleman and Andrew Lesniewski

The first people who began to investigate in a sistematic way the interrelations between Quantum Theory and the notion of algorithmic randomness was certainly Paul Benioff in a serie of 1970's papers [Ben73], [Ben74], [Ben77], [Ben78] in which he extensively analyzed the algorithmic randomness status of the sequence of outcomes of quantum measurements.

Benioff's intention was not, anyway, that of characterizng a notion of quantum-algorithmic-randomness, but that of extracting from Quantum Physics a new definition of classical-algorithmic randomness.

Indeed, in those years, the great scientific revolution concerning the incommensurability of quantum information and classical information (we underlined in the example 5.1.1 and in the remark5.1.9) was not happened yet.

A very similar kind of investigation was then pursued by Sidney Coleman and Andrew Lesniewski who tried to extend previous considerations by Hartle, as well as by Sam Guttman [Gut95], [Mit01]

Unfortunately Coleman and Lesniweski never published their thought that is accessible only from the exposition of it made by John Preskill in the section3.6 of his wonderful lecture notes [Pre98] as well as from the electronic correspondence of Christopher Fuchs he gently gave to collectivity's disposition (cfr. pagg.24-30 as well as pagg.106-110 of [Fuc01]).

The starting point is the following analysis by Hartle [Har68]:

the only point of the standard Copenhagen's axiomatization of Quantum Mechanics in which the term $<<$ *probability* $>>$ appears is the **Postulate of Reduction**, stating that a measurement of an observable $\hat{A} := \sum_a a|a><a|$ on a quantum system prepared in the state $|\psi> := \sum_a |a><a|\psi>$ has the following effects:

1. $$Probability[measurement's\, outcome \;=\; a] \;=\; |<a|\psi>|^2 \quad (6.1.6.1)$$

2. if the measuremnt's outcome a occurs, then the state's system collapses istantaneously to the state $|a>$

where we have considered, for simplicity, the case when there is no degeneration.

Hartle observed that the **Issue of the Interpretation of Probability** may be made to disappear from the axiomatization of Quantum Mechanics in the following way:

1. one replaces the Postulate of Reduction with the weaker **Postulate of Eigenstates**:

   If we prepare a quantum state $|a>$ such that $\hat{A}|a>= a|a>$, and then immediately measure $\hat{A}$, the outcome of the measurement is a with certainty

2. the case of measurements performed in a state that is not an eigenstate of the measured observable is reconducted to the **Postulate of Eigenstates** by the assumption of a frequentistic interpretation of probability:

   suppose we want to make a statement about the probability of obtaining the result $|\uparrow_z>$ when we measure σ_z in the state :

   $$|\psi> = \; a|\uparrow_z> + b|\downarrow_z> \quad (6.1.6.2)$$

   Hartle imagines that one prepares an infinite number of copies, so that the state is:

   $$|\psi^{(\bigotimes \infty)}> := \bigotimes_{n=1}^{\infty} |\psi> \quad (6.1.6.3)$$

   and imagines that one measures σ_z for each of the copies.

   Introduced the **average spin operator**:

   $$\bar{\sigma}_z \; := \; \lim_{n \to +\infty} \frac{1}{n} \sum_{i=1}^{n} \bar{\sigma}_z^{(i)} \quad (6.1.6.4)$$

   Hartle claims that $|\psi^{(\bigotimes n)}>$ becomes an eigenstate of $\bar{\sigma}_z$ with eigenvalue $|a|^2 - |b|^2$ for $n \to \infty$.

   Then he appeals to the **Postulate of Eigenstates** to infer that a measurement of $\bar{\sigma}_z$ will yeld the result $|a|^2 - |b|^2$ with certainty, and that the fraction of all the spins that point up is, therefore, $|a|^2$.

   In this sense $|a|^2$ is the probability that the measurement of σ_z yelds the outcome $|\uparrow_z>$.

As an application of Hartle's strategy, let us suppose , for example, that:

$$| \uparrow_x^{(\bigotimes n)} > := \bigotimes_{i=1}^{n} \frac{1}{\sqrt{2}} (| \uparrow_z > + | \downarrow_z >) \tag{6.1.6.5}$$

One has that:

$$< \uparrow_x^{(\bigotimes n)} | \bar{\sigma}_z | \uparrow_x^{(\bigotimes n)} > = 0 \tag{6.1.6.6}$$

$$< \uparrow_x^{(\bigotimes n)} | \bar{\sigma}_z^2 | \uparrow_x^{(\bigotimes n)} > = \frac{1}{n} \tag{6.1.6.7}$$

Thus, taking the limit $n \rightarrow +\infty$, one concludes that $\bar{\sigma}_z$ has vanishing dispersion about its mean value so that, at least in this sense, $| \uparrow_x^{(\bigotimes \infty)} >$ is an "eigenstate" of $\bar{\sigma}_z$ with eigenvalue zero.

Coleman and Lesniewski has generalized Hartle's ideas observing that indeed one can require that the sequence $\cdot_i \lambda_i$, where λ_i is the result of the measurement of the operator σ_z^i, satisfies not only the Law of Randomness of 1-Borel normality, but all the Laws of randomess, i.e. that it is Martin Löf - Solovay - Chaitin random.

So they introduce an orthogonal projection operator $\hat{\Pi}_{random}$ that acting on a state $|\psi>$ that is an eigenstate of each $\sigma_z^{(i)}$ satisfies:

$$\hat{\Pi}_{random} |\psi> = |\psi> \tag{6.1.6.8}$$

if the sequence of eigenvalues of $\sigma_z^{(i)}$ is algorithmically-random, and:

$$\hat{\Pi}_{random} |\psi> = 0 \tag{6.1.6.9}$$

if the sequence of eigenvalues of $\sigma_z^{(i)}$ is not algorithmically-random.

Preskill reports that Coleman and Lesniewski discovered that eq.6.1.6.8 and eq.6.1.6.9 properties, together with the condition that $\hat{\Pi}_{random}$ is an orthogonal projection, are not sufficient to determine how $\hat{\Pi}_{random}$ acts on all $\mathcal{H}_2^{\bigotimes \infty}$, but that, with additional technical constrains, it exists, it is unique, and has the property that:

$$\hat{\Pi}_{random} | \uparrow_x^{\bigotimes \infty} > = 1 \tag{6.1.6.10}$$

These considerations seems to us rather strange, since, according to us, the operator $\hat{\Pi}_{random}$ may be simply defined as:

DEFINITION 6.1.1

COLEMAN-LESNIEWSKI OPERATOR:

$$\hat{\Pi}_{random} := \int_{CHAITIN(\Sigma^{\infty})} dP_{unbaised} |\bar{x} >< \bar{x}| \tag{6.1.6.11}$$

but than one has that:

$$\hat{\Pi}_{random} | \uparrow_{x}^{\bigotimes \infty} >$$

$$= \hat{\Pi}_{random} \bigotimes_{i=1}^{\infty} [\frac{1}{\sqrt{2}} (|0> + |1>)$$

$$= (\lim_{n \rightarrow \infty} \frac{1}{2^{\frac{n}{2}}}) \hat{\Pi}_{random} (|0^{\infty}> + |1^{\infty}>) = 0 \quad (6.1.6.12)$$

Introduced the following notion:

DEFINITION 6.1.2

COLEMAN RANDOM SEQUENCES OF QUBITS:

$$COLEMAN - RANDOM(\mathcal{H}_{2}^{\bigotimes \infty}) := \{ |\psi> \in \mathcal{H}_{2}^{\bigotimes \infty}) : \hat{\Pi}_{random} |\psi> = |\psi> \} \quad (6.1.6.13)$$

it would be clear why, according to our point of view, such a notion is completelly misleading as to the characterization of quantum algorithmic randomness:

as we extensively discussed in section5.1, since the right space of qubits' sequences is the noncommutative space Σ_{NC}^{∞} and not the Hilbert space $\mathcal{H}_{2}^{\bigotimes \infty}$, the space of algorithmically-random sequences of qubits is a set of objects of the form:

$$RANDOM(\Sigma_{NC}^{\infty}) \subset \Sigma_{NC}^{\infty} \quad (6.1.6.14)$$

and not a set of the form:

$$RANDOM(\mathcal{H}_{2}^{\bigotimes \infty}) \subset \mathcal{B}(\mathcal{H}_{2}^{\bigotimes \infty}) \quad (6.1.6.15)$$

as $COLEMAN - RANDOM(\mathcal{H}_{2}^{\bigotimes \infty})$.

Demanding to remark5.1.7 and remark5.1.8 for a complete analysis, let us briefly recall that the passage from $\Sigma_{NC}^{\star}$ to Σ_{NC}^{∞} corresponds to a genuine increasing of **noncommutative cardinality** by one step, with the resulting effect of **continuous dimension** and, hence, **the lost of atomicity** of the underlying quantum logic, while the passage from $\mathcal{B}(\mathcal{H}_{2}^{\star})$ to $\mathcal{B}(\mathcal{H}_{2}^{\infty})$ corresponds to an increasing of **commutative cardinality** by one step, that is different from the correct required increasing of **noncommutative cardinality** by one step.

From a logico-mathematical point of view, this can be seen introducing the following:

DEFINITION 6.1.3

COLEMAN PROPOSITIONS:

$$CQP := \{ |\psi><\psi| : |\psi> \in COLEMAN - RANDOM(\mathcal{H}_{2}^{\bigotimes \infty}) \} \quad (6.1.6.16)$$

Clearly any Coleman quantum proposition is an **atomic quantum propositions** of the weak quantum logic $\mathcal{L}(\mathcal{H}_2^{\bigotimes \infty})$.

The effects of erroneously supposing that the quantum logic of qubits' sequences has atomic propositions may be appreciated by the following:

Remark 6.1.1

THE HALTING-PROBABILITY'S COLEMAN ATOMIC PROPOSITION WOULD SOLVE THE COMMUTATIVE ENTSCHEIDUNGPROBLEM

Let us consider the following Coleman quantum proposition:

$$p_{\Omega_U} := |\Omega_U >< \Omega_U| \tag{6.1.6.17}$$

where, according to definition1.3.9, Ω_U denotes the Halting Probability w.r.t. the Chaitin universal computer U.

Let us, then, introduce the **qubits' sequence operator**:

$$\hat{q}^{\bigotimes \infty} := \bigotimes_{n \in \mathbb{N}} \hat{q} \tag{6.1.6.18}$$

where $\hat{q}$ is the qubit operator defined in eq.5.1.5.31. The measurement of $\hat{q}^{\bigotimes \infty}$ in the state $|\Omega_U >$ results in the solution of the (C_Φ - classical, i.e. commutative) Enstcheidungproblem (as David Hilbert indicated the problem of determining whether or not a given formula of the (Classical) Predicate Calculus is valid [Dav65], [Odi89]).

We see, then, that the predicate p_{Ω_U} encodes the solution of the Commutative Entsheidungsproblem.

So we would have that the Quantum Propositional Calculus admits an **atomic** proposition (from which other not-atomic i.e. not-elementary, propositions may be constructed logically-connecting it with other propositions through the connectives $\bigvee, \bigwedge, \perp$), that, just alone, implies a violation of the Church-Turing Thesis.

Assuming the Church-Turing Thesis, we have then to reject such a situation.

Let us explain, by the way, more precisely the meaning of the expression Commutative Enschteidungsproblem we used:

the impossibility of developing all Mathematical-Logics simply by the distributive orthocomplemended lattice of Classical Predicate Calculus appears only when one wants to take into account quantifications. In this case, even restricting the analysis to First Order Theories in which one predicate cannot have other predicates or functions as arguments and quantification on predicates or functions is forbidden, one has to pass to Classical Formal Systems, their models and so on.

Also the Classical Predicate Calculus may, of course, be then embedded in such a more sophisticate language:

there exist many ways of axiomatize it as a classical formal system, and the general theory of formal systems may be applied to it to conclude that, as a formal system (in any way we axiomatized it), Classical Predicate Calculus is consistent though, as we have seen, undecidable.

As far as Quantum Logic is concerned, many people, and we among them, tried to go beyond Quantum Predicate Calculus (i.e. the theory of orthocomplemented orthomodular lattices) to deveop a general theory of Quantum Formal Systems, the first attempts being of Von Neumann himself:

> *"Dear Doctor Silsbee, It is with great regret that I am writing these lines to you, but I simply cannot help myself. In spite of very serious attempts to write the article " Logics of Quantum Mechanics" I find it it completely impossible to do it at this time. As you may know, I wrote a paper on this subject with Garrett Birkhoff in 1936 ("Annals of Mathematics", vol. 37 , pp. 823-843) and I have thought a good deal on the subject since. My work on continuous geometry , on which I gave the Amer. Math. Soc. Colloqiuim lectures of 1937, comes to a considerable extent from this source. Also a good deal concerning the relationship between strict- and probability logics (upon which I touched briefly in the Henry Joseph Lecture) and on the extension of this "Propositional calculus" work to "logic with quantifiers" (which I never discussed in public)"* (letter to Doctor Solbee ; July 2, 1945 ; cfr. [vN01])

Personally we tried to develop:

1. a quantum corrispective of John Mc Carthy's LISP [Car60], i.e. more precisely, of Chaitin's version of it in which the evaluation operator *"eval"* of syntax:

   eval S-expression

   is replaced by a time-constrained [Cha98] version of it, whose syntax:

   try time-limit S-expression

   specifies the time-interval after which the computation halts furnishing as output the partial computation performed [1]

   We studied a new language, that we called the quantum-LISP, defined by the replacement of the instruction *"try"* with a new instruction *"quantum try"* with sintax:

   quantum-try time-limit quantum-S-expression

   where a **quantum-S-expression** is a list of the form:

   $$((S - expression_G \; S - expression_H) \; (a \; b)) \qquad (6.1.6.19)$$

[1] Such a time-constraining is necessary since, otherwise, the request of evaluating a formal axiomatic system would never halt since, for all the not-trivial formal systems, the inferential chain of theorem-proving is infinite

with $a, b \in \mathbb{C}$ $|a|^2 + |b|^2 = 1$.

Under the command of eq.6.1.6.19 the computer chooses at random one value of a binary random variable h such that:

$$Prob(h = \frac{1}{2}) = |a|^2 \tag{6.1.6.20}$$

$$Prob(h = -\frac{1}{2}) = |b|^2 \tag{6.1.6.21}$$

and then operates as follows:

- if occurs $h = \frac{1}{2}$ then it sets the **halt-qubit-list** to (10) and operates as Chaitin-LISP would do under the instruction:

  try time-limit $S - expression_G$

- if occurs $h = -\frac{1}{2}$ then it sets the **halt-qubit-list** to (01) and operates as Chaitin-LISP would do under the instruction:

  try time-limit $S - expression_H$

The idea underlying such a definition of the quantum-try instruction is to make it equivalent to a Deutsch's quantum Turing machine in which the periodic monitoring of the halting-qubit occurs at temporal-steps of time-interval [Deu85].

By the impossibility of having a fair random generator extensively discussed in section5.4 Quantum-LISP is not implementable on a classical computer and, for practical purposes, must be replaced with a Virtual-quantum-LISP, i.e. a language completelly identical to Quantum-LISP, but for the fact that the fair random generator is replaced with a PRG.

2. proceeding euristically, we tried to characterize the notion of a **quantum Post systems** associated to a classical Post system [Odi89] $\mathcal{G} := (\Sigma, A, Q)$ with the **axioms' set** $A \subset \Sigma^{\star}$ and **productions' set** Q as a triple $\hat{\mathcal{G}} := (\mathcal{H}_{\Sigma}, \mathcal{H}_{A}, \hat{Q})$, where $\mathcal{H}_{\Sigma} = \mathcal{H}_2^{\bigotimes \star}$, $\mathcal{H}_A$ is an Hilbert sub-space of $\mathcal{H}_{\Sigma}$, while $\hat{Q}$ is the set of the **quantum productions**, i.e. operators on $\mathcal{H}_{\Sigma}$ acting as the productions Q of $\mathcal{G}$ on the computational basis.

   A theorem of a quantum Post system is then defined as an element of $\mathcal{H}_2^{\star}$ reachable by a vector belonging to $\mathcal{H}_A$ by a finite number of application of suitable quantum productions giving rise to a plethora of logical-mathematical notions specularizing the classical ones.

We then discovered that formalizations of the theory of Quantum Formal Systems already existed in the literature: in 1996 Philiph Maymin introduced a quantum analogue of Alonzo Church's Lambda Calculus [May96], an idea already independentely (and in a completely different way) developed by David Finkelstein in the section 14.3.7 of his monograph [Fin97]. In 1997 Christopher

Moore and James P. Crutchfield introduced quantum analogues of the whole Chomsky hierarchy [Cru97].

A similar idea was concretelly implemented in his Masters Thesis by Bernard Öemer who developed QCL: an high-level, architecture independent programming language for quantum computing whose interpreter is downloadable from the author's homepage [Ö98]; the syntactic structure of a QCL program is described by a context-free grammar, in a way concisely explained in the section4.19.4 of [Pau01].

A step forward in the formalization of what a General Theory of Quantum Formal Systems has been done, according to us, by Paul Benioff [Ben98] who, introducing (with the usual generalization on the computational basis) a quantum analogue of a toy-formal-system by Raymond M. Smullyian (cfr. the first chapter of [Smu92]) discusses not only its **syntax** but also its **semantic**.

This is something new since, up to date, interpretations and models has been studied by the Quantum Logic Community only at the Quantum Propositional Calculus' level .

Now, exactly as the consideration of quantifications requires, in the classical case, to give up the simple lattice-theoretic Classical Propositional Calculus passing to the more sophisticated language of Classical Formal Systems and arriving, on this way, to axiomatize Classical Propositional Calculus itself formalizing its Entscheidungsproblem (that we call the Commutative Entscheidungsproblem) and discovering its unsolvability, we think the same must happen as to Quantum Propositional Calculus, whose Enstcheidungsproblem will be called the **Noncommutative Enstcheidungsproblem** from here and beyond.

These preliminary, euristic considerations concerning **quantum formal systems** will be discussed, anyway, more explicitly in section6.2 where we will extensively discuss the quantum extension of the duality:

languages versus automata

and the consequential characterization of the notion of **quantum formal system** obtained using such a duality at the correct level of Moore's generalization of Chomsky's hierarchy.

6.2 Karl Svozil's invention of Quantum Algorithmic Information Theory

In 1995 Karl Svozil first introduced the idea that the irreducibility of Quantum Information Theory to the classical one implies the necessity of developing a quantum analogue of Classical Algorithmic Information Theory, namely Quantum Algorithmic Information Theory, irreducible to the classical theory [Svo96].

Given a quantum computer Q, i.e. a quantum-mechanical physical system with Hilbert space $\mathcal{H}_2^{\star}$ Svozil affords the first issue:

have the programs of Q to be coded in cbit or qubits?

To obtain the quantum analogue of **prefix algorithmic entropy**, Svozil claims, their lengths must satisfy the Kraft's Inequality; but if we allowed Q's programs to be qubits' strings instead of cbits' strings, than the Kraft sum would diverge.

As we will see this a key point, discussed also by Paul Vitanyi [Vit99], [Vit01] in his rediscovering of Svozil's results and lying at the basis of the objections André Berthiaume, Wim van Dam and Sophie Laplante moved to Vitanyi [vDSL00] in their rediscovering of what Svozil had already discussed years before.

The condition that the programs of Q are classical may be easily formalized observing that any map:

$$Q \in \overset{\circ}{MAP} (\Sigma^{\star} , \mathcal{H}_2^{\bigotimes \star}) \tag{6.2.6.1}$$

may be equivalentely seen as a map:

$$Q \in \overset{\circ}{MAP} (\mathbb{E}_{\star} , \mathcal{H}_2^{\bigotimes \star}) \tag{6.2.6.2}$$

identifying $\Sigma^{\star}$ with the computational basis $\mathbb{E}_{\star}$.

Assuming that the quantum computer is a **closed system** Q will be clearly nothing but the restriction to $\mathbb{E}_{\star}$ of an **inner automorphism** of $\mathcal{B}(\mathcal{H}_2^{\star})$.

Assumed the prefix-free condition:

$$HALTING(Q) \text{ is prefix-free} \tag{6.2.6.3}$$

Svozil introduces the following:

DEFINITION 6.2.1

QUANTUM ALGORITHMIC INFORMATION OF $|\psi>$ W.R.T. Q:

$$I_Q(|\psi>) := \begin{cases} \min\{\vec{x} \in HALTING(Q) \ : \ Q(\vec{x}) = |\psi>\} & \text{if } \exists \vec{x} \in HALTING(Q) \ : \ Q(\vec{x}) = |\psi> , \\ +\infty & \text{otherwise.} \end{cases} \tag{6.2.6.4}$$

Then Svozil considers the definition of a quantum analogue of Chaitin's Halting Probability.

To see how Svozil implements such a notion it is necessary, first of all, to discuss his analysis of the Halting Problem for Quantum Computers, i.e. his analysis of Quantum Diagonalization.

Diagonalization is a proof's technique introduced by Cantor to prove that $cardinality(2^{\mathbb{N}}) > \aleph_0$.

It may be formalized in the following way:

Theorem 6.2.1

DIAGONALIZATION'S THEOREM:

HP:

$$A \ \ set$$

$$R \subseteq A \times A \quad \text{binary relation on A}$$

$$D := \{a \in A : (a,a) \notin R\} \quad \text{diagonal set for R} \tag{6.2.6.5}$$

$$R_a := \{b \in A : (a,b) \in R\} \ \ a \in A$$

TH:

$$D \neq R_a \ \ \forall a \in A$$

PROOF:

Suppose ad-absurdum that:

$$\exists \bar{a} \in A \ : \ D = R_{\bar{a}} \tag{6.2.6.6}$$

i.e.:

$$\exists \bar{a} \in A \ : \ D = \{b \in A \ : \ (\bar{a}, b) \in R\} \tag{6.2.6.7}$$

Let us now consider the following question:

$$\bar{a} \in D \, ?$$

- if the answer to the question in eq.6.2 is **yes** it follows by eq.6.2.6.5 that $(\bar{a}, \bar{a}) \notin R$ that, by eq.6.2.6.7, implies that $\bar{a} \notin D$ that is asburdum
- if the answer to the question in eq.6.2 is **no** it follows by eq.6.2.6.5 that $(\bar{a}, \bar{a}) \in R$ that, by eq.6.2.6.7, implies that $\bar{a} \in D$ that is again asburdum

■

Cantor's argument runs than as follows:

Theorem 6.2.2

CANTOR'S THEOREM:

$$cardinality(2^{\mathbb{N}}) > \aleph_0 \tag{6.2.6.8}$$

PROOF:

Let us suppose ad absurdum that $2^{\mathbb{N}}$ is countable. Then there exists a a way of enumerating all members of $2^{\mathbb{N}}$ as:

$$2^{\mathbb{N}} = \{R_0, R_1, R_2, \cdots\} \tag{6.2.6.9}$$

Introduced the relation on $\mathbb{N}$ as:

$$R := \{(i,j) \in \mathbb{N} \times \mathbb{N} : j \in R_i\} \tag{6.2.6.10}$$

the thesis immediately follows applying to R the theorem6.2.1 ■

Let us now pass to partial recursive functions and let us introduce the following two sets:

DEFINITION 6.2.2

FIRST SELF-REFERENTIAL SET:

$$SR_1 := \{i \in \mathbb{N} : i \in \mathcal{W}_i\} \tag{6.2.6.11}$$

DEFINITION 6.2.3

SECOND SELF-REFERENTIAL SET:

$$SR_2 := \{(i,j) \in \mathbb{N} \times \mathbb{N} : i \in \mathcal{W}_j\} \tag{6.2.6.12}$$

Cantor's diagonalization argument immediately leads to the following importan theorems:

Theorem 6.2.3

COMBINATORIAL CORE OF THE UNDECIDABILITY RESULTS:

$$SR_1 \text{ is r.e. but not recursive}$$

PROOF:

We have that:

$$x \in SR_1 \Leftrightarrow \varphi_x(x) \downarrow \tag{6.2.6.13}$$

But theorem1.1.1 tells us that there exist a partial recursive φ such that:

$$\varphi(x) = \varphi_x(x) \tag{6.2.6.14}$$

and hence:

$$SR_1 = HALTING(\varphi) \tag{6.2.6.15}$$

So SR_1, being the halting set of a partial recursive function, is a r.e. set.

The fact that SR_1 is not recursive follows immediately by applying theorem1.1.1 to the relation SR_2. ■

Theorem 6.2.4

UNSOLVABILITY OF THE HALTING PROBLEM:

SR_2 is r.e. but not recursive

PROOF:

We have that:

$$(i,j) \in SR_2 \Leftrightarrow \varphi_j(i) \downarrow \tag{6.2.6.16}$$

But theorem1.1.1 tells us that there exist a partial recursive φ such that:

$$\varphi(i) = \varphi_j(i) \tag{6.2.6.17}$$

and hence:

$$SR_2 = HALTING(\varphi) \tag{6.2.6.18}$$

So SR_2, being the halting set of a partial recursive function, is a r.e. set.

Let us then suppose by absurdum that SR_2 is recursive. Since:

$$x \in SR_1 \Leftrightarrow (x\,,\,x) \in x \in SR_2 \tag{6.2.6.19}$$

this implies that SR_1 is not recursive too, contradicting theorem6.2.3. ■

Remark 6.2.1

THE FIRST SELF-REFERENTIAL SET AND RUSSELL'S PARADOX

Bertrand Russell's Paradox is certainly the most famous example of the many subtlities that appear in the formalization of **classes**, i.e. of **sets** whose elements are **sets** themselves.

It runs as follows: considered the set:

$$A := \{x : x \notin x\} \tag{6.2.6.20}$$

one has that:

$$x \in A \Leftrightarrow x \notin x \tag{6.2.6.21}$$

and thus:

$$A \in A \Leftrightarrow A \notin A \qquad (6.2.6.22)$$

that is nonsense.

Let us now observe that the set $\mathbb{N} - SR_1$ resembles Russell's set A: it is the set of numbers not belonging to the r.e. set they code.

But the is no paradox here because Russel's argument simply shows that such a set is not r.e. itself.

Remark 6.2.2

PROGRAMMATION AND META-PROGRAMMATION

The meaning of theorem6.2.4 may be appreciated taking into account the concrete programmation on the (classical, deterministic) computers we use every day, observing that, by Church-Turing Thesis, the specific hardware nature of the consided computer is irrilevant.

We can divide the set of all programming languages for a generic computer in two classes, according to if they admit **meta-programmation** or not.

By meta-programmation we mean the ability of programs to deal with that particular kind of **objects** made by program themselves.

Indeed the more logico-mathematically featured programming languages deal whith only one structure of objects (e.g. **lists** in Mac Carthy's LISP [Car60] or **expressions** in Wolfram's Mathematica).

So they automatically admit **meta-programmation** since programs and the other objects on which they operate are of the same (unique) structure.

What is important to observe is that the **meta-programmation ability** realizes exactly that link between **language** and **meta-language** that we indicated in the remark1.1.1 as the door leading (or better allowing) self-reference.

We can now explain the diagonalization argument lying behind theorem6.2.4 in the following more concrete way [Svo93], [Wey94], [Pap98]:

Let us suppose, for example to enter a Mathematica session.

We could thus think that it is possible, using the meta-programming in a clever way, to define, through a suitable Mathematica expression:

$$In[1] := HALT[p_{-}, x_{-}] := \cdots \qquad (6.2.6.23)$$

a function HALT[p,x] that, when called, returns a cbit having the value True or False according if, respectively, Mathematica halts or doesn't halt under the input p[x]

If such a Mathematica expression HALT[p,x] existed it could be used to construct the following:

DEFINITION 6.2.4

DIAGONAL EXPRESSION:

$$In[2] := DIAGONAL[x_{-}] := (Label[start] ; If[Halt[x, x] == True , Goto[start] , True) \qquad (6.2.6.24)$$

Notice what DIAGONAL[x] does: if the HALT program decides that the program x would halt if presented with itself as input, then DIAGONAL(x) loops forever; otherwise it gives as output True and then halts.

From the function DIAGONAL[x] we could, then, construct the following Mathematica expression:

DEFINITION 6.2.5

$$In[3] \;:=\; PARADOX \;:=\; DIAGONAL[DIAGONAL] \tag{6.2.6.25}$$

Let us now give to Mathematica the following input:

$$In[4] \;:=\; PARADOX \tag{6.2.6.26}$$

Will Mathematica halt giving the output Out[4] or not?

It will do it iff the input HALT[DIAGONAL,DIAGONAL] gives as output False; in other words Mathematica halts if and only if it doesn't halt. That is a contradiction.

So we must conclude that the only hypothesis that started us on this path is false, i.e. that there it doesn't exist any Mathematical expression that put at the place of the dots in eq.6.2.6.23 make the expression HALT[p,x] to be defined so that it outputs 1 if the Mathematica expression p[x] halts and zero otherwise.

Remark 6.2.3

TIME-CONSTRAINED HALTING FUNCTION:

Let us observe that a time-constrained version of the halting function, i.e. a Mathematica expression $HALT[p, x, T]$ that outputs True if Mathematica halts under the input p[x] in less or equal than T seconds and outputs False otherwise, can be implemented as follows:

$$In[1] \;:=\; HALT[p_{-}\,,\,x_{-}\,,\,T_{-}] \;:=\; If[TimeConstrained[p[x], T] \neq \$Aborted\,,\,True\,,\,False] \tag{6.2.6.27}$$

Let us observe, anyway, that while a dialog of the form:

$$In[2] \;:= HALT[p, x, T] \tag{6.2.6.28}$$
$$Out[2] \;:= True \tag{6.2.6.29}$$

assures us that also the impossible HALT[p,x], if existed, would give us True as output, a dialog of the form:

$$In[2] \;:= HALT[p, x, T] \tag{6.2.6.30}$$
$$Out[2] \;:= False \tag{6.2.6.31}$$

tells us nothing because it is possible that there exist a time $t > T$ such that:

$$In[3] \;:= HALT[p, x, t] \tag{6.2.6.32}$$
$$Out[3] \;:= True \tag{6.2.6.33}$$

So the expression HALT[p,x,t] can't be used to solve the Halting Problem.

Svozil has analyzed what happens when one supposes that the halting-degree of freedom is codified by a qubit:

$$|Halt> := c_{True}|True> + c_{False}|False> \in \mathcal{H}_2 \quad (6.2.6.34)$$

$$|False> := |0> \quad (6.2.6.35)$$

$$|True> := |1> \quad (6.2.6.36)$$

$$(6.2.6.37)$$

instead of by the cbit:

$$c_{halting} \in \Sigma \quad (6.2.6.38)$$

$$False := 0 \quad (6.2.6.39)$$

$$True := 1 \quad (6.2.6.40)$$

we can rephrase his analysis replacing the halting Mathematica expression HALT[p,x] such that:

$$(\, In[n] := Halt[p,x]\,) \Rightarrow (\, Out[n] := \begin{cases} True & \text{if } p[x] \neq\uparrow , \\ False & \text{otherwise.} \end{cases}) \quad (6.2.6.41)$$

with an analogue expression QHALT[p,x] such that:

$$(\, In[n] := QHalt[p,x]\,) \Rightarrow (\, Out[n] := \begin{cases} |True> & \text{if } p[x] \neq\uparrow , \\ |False> & \text{otherwise.} \end{cases}) \quad (6.2.6.42)$$

Let us then suppose that it is possible to implement such an object by a suitable input of the form:

$$In[1] := QHALT[p\_ , x\_] := \cdots \quad (6.2.6.43)$$

If such a Mathematica expression HALT[p,x] exists it can be used to construct quantum analogues of the **diagonal expression** of definition6.2.4:

DEFINITION 6.2.6

QUANTUM DIAGONAL EXPRESSION OF FIRST KIND:

$$In[2] := QDIAGONAL1[x\_] := (Label[start]; If[QHalt[x,x] == |True>, Goto[start], True) \quad (6.2.6.44)$$

DEFINITION 6.2.7

QUANTUM DIAGONAL EXPRESSION OF SECOND KIND:

$$In[2] := QDIAGONAL2[x\_] := (Label[start]; If[QHalt[x,x] == |True>, Goto[start], |True>) \quad (6.2.6.45)$$

DEFINITION 6.2.8

QUANTUM DIAGONAL EXPRESSION OF THIRD KIND:

$$In[2] \ := \ QDIAGONAL3[x\_] \ := \ If[QHalt[x,x] == |True>, |False>, |True>] \quad (6.2.6.46)$$

as well as quantum analogues of the paradox function of definition6.2.5:

DEFINITION 6.2.9

QUANTUM PARADOX EXPRESSION OF FIRST KIND:

$$In[3] \ := \ QPARADOX1 \ := \ QDIAGONAL1[QDIAGONAL1] \quad (6.2.6.47)$$

DEFINITION 6.2.10

QUANTUM PARADOX EXPRESSION OF SECOND KIND:

$$In[3] \ := \ QPARADOX2 \ := \ QDIAGONAL2[QDIAGONAL2] \quad (6.2.6.48)$$

DEFINITION 6.2.11

QUANTUM PARADOX EXPRESSION OF THIRD KIND:

$$In[3] \ := \ QPARADOX1 \ := \ QDIAGONAL1[QDIAGONAL1] \quad (6.2.6.49)$$

Does the diagonalization proof of the not-existence of HALT[p,x] hold also as to $QHALT1[p,x]$, $QHALT2[p,x]$, $QHALT3[p,x]$?

Let us start analyzing QDIAGONAL1[x]: if the QHALT program decides that the program x would halt if presented with itself as input, then DIAGONAL(x) loops forever;otherwise it gives as output True and then halts.

Up to the identification of Σ with the computational basis $\mathbf{E}_2$ of $\mathcal{H}_2$, the Mathematica QDIAGONAL1[x] is equivalent to DIAGONAL, giving rise to the same diagonalization argument as to QPARADOX1.

Let us then pass to QDIAGONAL2[x] whose action is the following: if the QHALT program decides that the program x would halt if presented with itself as input, then DIAGONAL(x) loops forever; otherwise it gives as output $|True>$ and then halts.

Let us then look at what we expect Mathematica should output under the input QPARADOX2: it halts outputting $|True>$ iff QHALT[QDIAGONAL2,QDIAGONAL2] outputs $|False>$ so that once again QDIAGONAL2 halts on itself iff it doesn't halt on itself reproducing once again the paradox.

As a conclusion, the consideration of definition6.2.9 and definition6.2.7 prove the impossibility of substituting the dots in eq.6.2.6.43 so that the implemented Mathematica function behaves as eq.6.2.6.43 proving that QHALT cannot exist too.

Svozil, instead, doesn't arrive to this conclusion, since he considers only QDIAGONAL3[x] whose action is the following: if the QHALT program decides that the program x would halt if presented with itself as input, then

QDIAGONAL3[x] outputs $|False>$; otherwise it gives as output $|True>$ and then halts.

Since QDIAGONAL3 halts on every input, PARADOX3 simply outputs $|False>$ so that, indeed, it can't be used to infer by diagonalization the impossibility of QHALT.

Let us observe, by the way, that:

$$(In[n] \, := \, QDIAGONAL3[|True>]) \, \Rightarrow \, (Out[n] \, = \, |False>) \quad (6.2.6.50)$$

$$(In[n] \, := \, QDIAGONAL3[|False>]) \, \Rightarrow \, (Out[n] \, = \, |True>) \quad (6.2.6.51)$$

If QDIAGONAL3 was such that:

$$QDIAGONAL3[c_{True}|True> + c_{False}|False>] \, = \, c_{True} QDIAGONAL3[|True>] + QDIAGONAL3[|False>] \;\; \forall c_{True}, c_{False} \in \mathbb{C} \, : \, |c_{True}|^2 \, + \, |c_{False}|^2 \, = \, 1$$

its restriction to inputs of the form $c_{True}|True> + c_{False}|False>$ could indeed be represented by the NOT gate $\hat{\sigma}_x \, := \, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Anyway this is not the case, since:

$$(c_{False} \neq 0 \, \Rightarrow \, QDIAGONAL3[c_{True}|True> + c_{False}|False>] \, = \, |True>) \quad \forall c_{True}, c_{False} \in \mathbb{C} \, : \, |c_{True}|^2 \, + \, |c_{False}|^2 \, = \, 1 \quad (6.2.6.52)$$

We have seen in remark6.2.3 that a time-constrained version HALT[p,x,t] of the halting program may indeed be easily defined.

This fact involves some subtility owing to the following [Cha95]:

Theorem 6.2.5

ON HALTING NOW OR NEVER AGAIN:

$$\exists c \in \mathbb{R}_{+} \, : \quad U(\vec{x}) \text{ has not yet halted at time } \Sigma(|\vec{x}| + c) \, \Rightarrow \, U(\vec{x}) \, = \uparrow \quad (6.2.6.53)$$

where $\Sigma(n)$ is the busy-beaver function of definition1.4.2, whose proof lies on the following [Cha95]:

Lemma 6.2.1

BOUND ON THE HALTING TIME:
HP:

$$\vec{x} \in \Sigma^{\star} \, : \, U(\vec{x}) \downarrow$$

$$t_{HALTING} \, := \, \min\{ t \in \mathbb{R}_{+} \, : \text{U has already halted on } \vec{x} \text{ at time t} \}$$

TH:

$$\exists c \in \mathbb{R}_{+} \ : \ I(t_{HALTING}) \ \leq \ |\vec{x}| \ + \ c$$

Theorem6.2.5 would indeed seem to contradict what we said in the remark6.2.3 because it would seem to tell us that there exist indeed a **dead-line-time function** $(p,x) \stackrel{f}{\rightarrow} d[p,x]$ such that by a dialog of the form:

$$In[n] \ := HALT[p,x,d[(p,x)]] \tag{6.2.6.54}$$

$$Out[n] \ := False \tag{6.2.6.55}$$

(where HALT[p,x,T] is the time-constrained halting function of eq.6.2.6.27) one could infer that p doesn't halt on x.

The function $HALT[p,x,f[(p,x)]]$ would then seem to solve the Halting Problem, since defining:

$$HALT[p_{-}\ ,\ x_{-}] \ := \ HALT[p,x,d[(p,x)]] \tag{6.2.6.56}$$

HALT[p,x] behaves exactly as the required halting predicate.

The bug in such a reasoning is owed to the following:

Theorem 6.2.6

NOT-RECURSIVITY OF THE BUSY-BEAVER FUNCTION:

$$\Sigma(n) \ \notin \ REC - MAP(\mathbb{N},\mathbb{N}) \tag{6.2.6.57}$$

Theorem6.2.6 implies that the **dead-line-time function** function $(p,x) \stackrel{f}{\rightarrow} f[p,x]$ is itself not-recursive, so that it cannot be implemented by an input of the form:

$$d[p_{-}\ ,\ x_{-}] \ := \ \cdots \tag{6.2.6.58}$$

for a suitable substitution of the dots at the r.h.s. of eq.6.2.6.58 as it would be required for the Mathematica implementation of the halting predicate in eq.6.2.6.56 to be complete.

Anyway, at this point, one could object that it would be sufficient to succeed in implementing an **overestimated-dead-line-time-function**:

$$overestd[p_{-}\ ,\ x_{-}] \ := \ \cdots \tag{6.2.6.59}$$

such that:

$$overestd[p\ ,\ x] \ \geq \ d[p\ ,\ x] \ \ \forall \text{ Mathematica expression p , x} \tag{6.2.6.60}$$

in order that:

$$HALT[p_{-}\ ,\ x_{-}] \ := \ HALT[p,x,overestd[(p,x)]] \tag{6.2.6.61}$$

behaves in the required way, implementing algorithmically the halting predicate.

The bug in this reasoning is owed to the following (cfr. the section8.3 of [Svo93]):

Theorem 6.2.7

THE BUSY BEAVER RUNS QUICKER THAN RECURSIVE FUNCTIONS:

$$\forall f \in REC(\mathbb{N}, \mathbb{N}) \; \exists N \in \mathbb{N} \; : \; \Sigma(n) \; > \; f(n) \;\; \forall n > N \tag{6.2.6.62}$$

that implies that there is no way of substituting the dots in eq.6.2.6.59 so that eq.6.2.6.60 is satisfied.

C. Calude, M.J. Dinneen and K. Svozil consider, finally, the situation in which on Mathematica has been implemented a time-travel-algorithm: $TimeTravel[t_1, t_2]$ that (giving suitable input to suitable hardware) allows to cause the instantaneous time-travel:

$$t = t_1 \; \rightarrow \; t = t_2 \tag{6.2.6.63}$$

verified inside Mathematica by the dialog:

$$In[n] \; := \; before \; = \; AbsoluteTime[\,]; \, TimeTravel[t_1, t_2]; \\ after \; = \; AbsoluteTime[\,]; \, \{before \, , \, after\} \tag{6.2.6.64}$$

$$Out[n] \; := \; \{t_1 \, , \, t_2\} \tag{6.2.6.65}$$

Though we are not interested here in the details of such an hardware, it may be worth to observe that the existence of $TimeTravel[t_1, t_2]$ is not incompatible with General Relativity, if one assume that it is founded only on the Cauchy-Problem for Einstein's equation, as it is proved by the well-known Gödel's solution (cfr. the section5.7 of [Ell73]):

$$spacetime_{Gödel} \; := \; (\mathbb{R}^4 \, , g_{Gödel} \; := \; -dt \bigotimes dt \; + \; dx \bigotimes dx \; + \\ dz \bigotimes dz \; - \frac{1}{2} \exp(2\sqrt{2}\omega x) dy \bigotimes dy \; - \; 2 \exp(\sqrt{2}\omega x) dt \bigotimes dy) \tag{6.2.6.66}$$

for a pressure-free perfect-fluid's matter-distribution with energy momentum tensor $T_{ab} \; = \; \rho u_a u_b$, where the matter density ρ and the normalized four-velocity vector u_a are such that:

$$u_0^a \; := \; \delta_0^a \tag{6.2.6.67}$$

$$4 \, \pi \, \rho \; = \; \omega^2 \; = \; -\Lambda \tag{6.2.6.68}$$

where Λ is the cosmological constant, has closed time-like curves. Indeed the censorship of causality violations is usually added in the Foundations of General Relativity in the following way (cfr. the cap.8 and the cap.12 of [Wal84] and the cap.8 of [Wal94]):

given a space-time $(M \, , \, g_{ab})$ time-orientable, i.e. such that the light-cone in any point may be divided in its future and past halves in a way varying smoothly with the point:

DEFINITION 6.2.12

CHRONOLOGICAL FUTURE OF $p \in M$:

$$I^+(p) \ := \ \{q \in M \ : \exists \text{ a future-directed time-like curve } \lambda : [0,1] \to M : \lambda(0) = p\,,\, \lambda(1) = q\} \quad (6.2.6.69)$$

DEFINITION 6.2.13

CHRONOLOGICAL PAST OF $p \in M$:

$$I^-(p) \ := \ \{q \in M \ : \exists \text{ a past-directed time-like curve } \lambda : [0,1] \to M : \lambda(0) = p\,,\, \lambda(1) = q\} \quad (6.2.6.70)$$

DEFINITION 6.2.14

CAUSAL FUTURE OF $p \in M$:

$$J^+(p) \ := \ \{q \in M \ : \exists \text{ a future-directed causal curve } \lambda : [0,1] \to M : \lambda(0) = p\,,\, \lambda(1) = q\} \quad (6.2.6.71)$$

DEFINITION 6.2.15

CAUSAL PAST OF $p \in M$:

$$J^-(p) \ := \ \{q \in M \ : \exists \text{ a past-directed causal curve } \lambda : [0,1] \to M : \lambda(0) = p\,,\, \lambda(1) = q\} \quad (6.2.6.72)$$

DEFINITION 6.2.16

CHRONOLOGICAL PAST OF $S \subset M$:

$$I^-(S) \ := \ \bigcup_{p \in S} I^-(p) \quad (6.2.6.73)$$

DEFINITION 6.2.17

CHRONOLOGICAL FUTURE OF $S \subset M$:

$$I^+(S) \ := \ \bigcup_{p \in S} I^+(p) \quad (6.2.6.74)$$

DEFINITION 6.2.18

CAUSAL PAST OF $S \subset M$:

$$J^-(S) \ := \ \bigcup_{p \in S} J^-(p) \quad (6.2.6.75)$$

DEFINITION 6.2.19

CAUSAL FUTURE OF $S \subset M$:

$$J^{+}(S) := \bigcup_{p \in S} J^{+}(p) \tag{6.2.6.76}$$

DEFINITION 6.2.20

$S \subset M$ IS ACHRONAL:

$$I^{+}(S) \bigcap S = \emptyset \tag{6.2.6.77}$$

Given an achronal, closed set $S \subset M$:

DEFINITION 6.2.21

$$D^{+}(S) := \{ p \in M : \gamma \text{ inextendible future causal curve through p } \Rightarrow Im(\gamma) \bigcap S \neq \emptyset \} \tag{6.2.6.78}$$

DEFINITION 6.2.22

$$D^{-}(S) := \{ p \in M : \gamma \text{ inextendible past causal curve through p } \Rightarrow Im(\gamma) \bigcap S \neq \emptyset \} \tag{6.2.6.79}$$

DEFINITION 6.2.23

DOMAIN OF DEPENDENCE OF $S \subset M$:

$$D(S) := D^{+}(S) \bigcap D^{-}(S) \tag{6.2.6.80}$$

DEFINITION 6.2.24

$S \subset M$ IS A CAUCHY SURFACE:

$$D(S) = M \tag{6.2.6.81}$$

We will say that:

DEFINITION 6.2.25

(M , g_{ab}) IS GLOBALLY-HYPERBOLIC:

$$\exists S \subset M \; Cauchy - surface \tag{6.2.6.82}$$

The impossibility of $TimeTravel[t_1 , t_2]$ may be derived only assuming the following suppletive Roger Penrose's:

AXIOM 6.2.1

AXIOM OF STRONG COSMIC CENSORSHIP:

$$(M, g_{ab}) \text{ physical space-time } \Rightarrow (M, g_{ab}) \text{ globally hyperbolic} \qquad (6.2.6.83)$$

If axiom6.2.1 is required to guarantee the correctness of the Cauchy's problem for Einstein's equation is not yet clear [Chr00].

Closing this little parenthesis on the possibility of $TimeTravel[t_1 \, , \, t_2]$ the key observation by Calude, Dinnen and Svozil is that one could use it, substantially, to slow the increasing with time of the busy beaver function $\Sigma(t)$ in order to surpass it recursively.

Let us suppose, for example, that we and our computer on which it is running our Mathematica session, are enclosed into a big box free-falling in the Gödel's space-time of eq.6.2.6.66.

Threating the whole box as a massive particle of mass m, General Relativity Theory tells us that its motion is described by the action:

$$S[q(\tau)] \; := \; -m \int_{\tau_1}^{\tau_2} d\tau \sqrt{g_{ab}^{Gödel} \frac{dq^a(\tau)}{d\tau} \frac{dq^b(\tau)}{d\tau}} \qquad (6.2.6.84)$$

whose invariance under reparametrization of the paths leads to the existence of the primary first-class constraint (the mass-shell condition) (cfr. [Tei92] for a general presentation of the Theory of Dirac Constraints and [Giv01],[Sal98] for its mathematical recasting in the framework of Symplectic Geometry):

$$H \; = \; p_a g_{Gödel}^{ab} p_b \, + \, m^2 \; \approx_{Dirac} \; 0 \qquad (6.2.6.85)$$

identifying a coisotropic submanifold $S \subset \mathbb{R}^8$, called the **constraint surface**, of the phase space $\mathbb{R}^8$.

The space of all the **global-observables** of the box is $C^{\infty}(S_{red})$, where S_{red} is the reduced phase-space defined as the quotient of S w.r.t. the gauge orbits; no element of it corresponds to time, since, from the own reparametrization invariance of the action6.2.6.84, it follows that, as to the **exophysical** point of view (cfr. the 6^{th}-chapter of [Svo93]) the box is a system with no time [Rov88].

So a gauge-fixing is required; we will choose the gauge $\tau \, = \, t$.

Anyway, as to the **endophysics** of we and the computer enclosed in the box, the things are different: the internal-clock of the computer by which Mathematica computes the function AbsoluteTime[ ] selects the particular coordinate system $(t \, , \, x \, , \, y \, , \, z \,)$ measuring the coordinate t.

On receiving the input $TimeTravel[t_1 \, , \, t_2]$ Mathematica tells to the hardware device to act on the whole box in order of giving to it a suitable initial condition $q^a(\tau = 0) \, , \frac{dq^a}{d\tau}(\tau = 0)$ function of $t_1 \, , \, t_2$ so that the successive free-fall motion of the box along a closed time-like curve realizes the required transition $t = t_1 \; \rightarrow \; t = t_2$.

It should be noted, anyway, that the possibility exists that such a process, for time-delaying such to allow to surpass recursively the busy-beaver-function, may be not effectively implementable, though we must confess we don't understand how this could happen.

Remark 6.2.4

GÖDEL AGAINTS GÖDEL:

The funny think of such a use of the Gödel's spacetime to overpass the busy beaver function is that is a sort of fight Gödel against Gödel, i.e. Gödel's solution of Einstein's Equation against Gödel's First Undecidability Theorem.

Demanding to [Odi89] and [Dav65] for details, Gödel's First Undecidability Theorem may be informally stated in the following way:

Every formal system which is sufficiently rich (i.e. contains Peano's Arithmetics), consistent(i.e. no false result may be proved by it) and recursively axiomatizable is not only ***incomplete****, i.e. there exist well-formed formulas in it that are nor provable neither refutable, but also* ***undecidable****, i.e. the set of its theorems is not recursive*

Such a theorem may be inferred by the Unsolvability of the Halting Problem, namely by theorem6.2.4, by simply observing that the decidability of the involved classical formal system would allow to prove or disprove any formula of the form $<< i \in \mathcal{W}_j >>$.

Calude, Dinnen and Svozil (cfr. [Svo00] as well as the final section of [Pau01]) have recently analyzed the quantum analogue of this issue.

Their arguments is centered around the following:

Conjecture 6.2.1

ON THE DYNAMICAL EVOLUTION OF THE HALTING QUBIT:

HP:

Q quantum computer with unitary dynamics, whose **halting state** is specified by a halting qubit:

$$|Halt > (t) \; := \; a_{True}(t)|True > \, + a_{False}(t)|False > \in \; \mathcal{H}_2$$
$$a_{True}(t) \, , \, a_{False}(t) \in \mathbb{C} : |a_{True}(t)|^2 \, + \, |a_{False}(t)|^2 = 1 \quad (6.2.6.86)$$

such that:

$$Prob[\text{Q has halted at time t}] \; = \; |a_{True}(t)|^2$$
$$Prob[\text{Q has not halted yet at time t}] \; = \; |a_{False}(t)|^2$$

with the initial condition at $t \, = \, 0$:

$$|a_{True}(0)|^2 \; = \; |a_{False}(0)|^2 \; = \; \frac{1}{2}$$

TH:

In the worst case $|a_{True}(t)|^2$ decades temporally as:

$$\exists c \in \mathbb{R}_+ \ : \ |a_{True}(t)|^2 \ \propto \ \frac{1}{\Sigma(I(t)+c)}$$

that they claim to follow from lemma6.2.1 and the unitarity of Q's dynamics. Given for granted the conjecture6.2.1 let us observe that:

1. Classical Computation may be seen as the particular case of Quantum Computation in which no superposition of vectors of the computational basis $\mathbf{E}_\star$ occur.
2. as to the **computability-issue** , **deterministic computation** and **classically-probabilistic computation** are equivalent (cfr. e.g. the 6^{th} chapter of [Gab95]) [2]
3. the monitoring of the halting-qubit gives a probabilistic-algorithm for solving the Halting Problem

Also assuming that the informal arguments supporting conjecture6.2.1 may be rigorously formalized, what constitues, according to our modest opinion, the weaker point in the Calude - Dinnen - Svozil's attach to what Calude calls the *Turing's barrier* lies in a not enough sharp specification of their **halting protocol**.

Considered the Hilbert space $\mathcal{H}_2^{\bigotimes \star} \bigotimes \mathcal{H}_2^{Halting}$, to be affected by the halting status of Q, the halting-qubit system H must be someway coupled to the computer so that, assuming the compound system (computer + halting flag) to be closed, its unitary dynamics starting from a disentangled state of the form $\frac{1}{\sqrt{2}}(|True> + |False>) \bigotimes |\vec{x}>$ will entangle them, so that:

1. the computer will evolve as an open system (i.e. trough a suitable CPU-map of $\mathcal{B}(\mathcal{H}_2^{\bigotimes \star})$) contradicting the assumed unitarity of Q
2. the halting flag will evolve as an open system (i.e. through a suitable CPU-map of $\mathcal{B}(\mathcal{H}_2^{Halting})$ and hence, in particular, the halting state won't continue to be pure contradicting eq.6.2.6.86

The problem is similar to that concerning the consistence of Deutsch's halting protocol for Quantum Turing Machines that what questioned by Myers [Mye97] with the argument that, ought to the entanglement between the **halting qubit** and the **tape's and internal state's sector**, would cause the periodic monitoring of the halting qubit to spoil the computation.

[2] It is important, with this respect, not to make confusion between **classically-nondeterministic computability** and **classically probabilistic computability**: in terms of acceptance of a given input **classically-nondeterministic computability** requires that there exist at least one computational path leading to an accepting state, while **classically probabilistic computability** averages on all the computational paths requiring that the input is accepted with probability greater than one half.

Unfortunately, part of the literature generated by Myers' objection [Oza98b], [Pop98], [Dan98], [Oza98c] called the issue with the misleading name of ***"the Quantum Halting Problem of Quantum Turing Machines"***, an erroneous denomination, since the the true **Quantum Halting Problem** is the problem of finding a quantum algorithm that receiving as input an other quantum algorithm, tell us if it halts or not.

The correct name of the discussed problem is ***"the consistence of the Halting Protocol of Quantum Turing Machines***.

In the same way, the problem concerning our objection to the Calude-Dinnen-Svozil's argument for solving the **Classical Halting Problem** through a quantum computer may be called: ***"the consistence of the Calude-Dinnen-Svozil's Halting Protocol"***.

The difference between such a problem and the problem of the consistence of the Halting Protocol of Quantum Turing Machines, is that in the latter case a periodic monitoring of the quantum qubit is involved, while in the former case, in any repetition of the computation, it occurs only one measurement of the halting qubit.

For this reason the problem of the consistence of the Calude-Dinnen-Svozil's Halting Protocol cannot be be simply resolved in terms of quantum nondemolition (QND) measurements (for which cfr. [Tho83] and the 12^{th} chapter of [Per95]) as was made by Ozawa in [Oza98b].

A possible solution could consist, mimicking the alternative halting protocol for Quantum Turing Machines proposed by Ozawa in [Oza98c] inglobing the halting qubit in the quantum-state-register's Hilbert space, to identify the halting-qubit's Hilbert space $\mathcal{H}_2^{Halting}$ with the one qubit-sector of $\mathcal{H}_2^{\star}$ by posing:

$$|True> := |1> \tag{6.2.6.87}$$
$$|False> := |0> \tag{6.2.6.88}$$

Such a strategy requires, first of all, that we replace the initial condition of eq.6.2 for the halting-qubit with:

$$|a_{True}(0)|^2 = 0 \tag{6.2.6.89}$$
$$|a_{False}(0)|^2 = 1 \tag{6.2.6.90}$$

Whether the double rule that one qubit sector of $\mathcal{H}_2^{\star}$ would assume can be in some way managed consistentely is not, anyway, clear.

Remark 6.2.5

DIRAC QUANTIZATION OF THE BOX IN GÖDEL'S SPACETIME

As a matter of curiosity it may be finally interesting to consider the quantum analogue of the gedanken experiment in Gödel spacetime previously introduced.

We can think to describe quantistically the massive box containing we and the computer, exploiting the Dirac quantization of the action of eq.6.2.6.84 (cfr. the 13^{th} chapter of [Tei92] and [Kir01] for its mathematical recasting in the framework of Symplectic Geometry, i.e. in terms of Geometric Quantization):

introduced the canonical operators:

$$(\hat{x}^{\mu}\psi)(x) := x^{\mu}\psi(x) \tag{6.2.6.91}$$

$$(\hat{p}_{\mu}\psi)(x) := -i\frac{\partial}{\partial x^{\mu}}\psi(x) \tag{6.2.6.92}$$

on the Hilbert space $\mathcal{H} := L^2(\mathbb{R}^8, d\vec{x})$, the subspace of physical states $\mathcal{H}_{physical} \subset \mathcal{H}$ is given by:

$$\mathcal{H}_{physical} := Ker(-\triangle_{g_{Gödel}} + m^2) \tag{6.2.6.93}$$

where Δ_g denotes the Laplace-Beltrami operator of the (pseudo)riemannian metric g.

The scalar product in $\mathcal{H}_{physical}$ depends on the choice of a gauge and is defined in terms of a suitable self-adjoint operator $\hat{O}$:

$$<\psi_1|\psi_2>_{physical} := <\psi_1|\hat{O}|\psi_2> \quad |\psi_1>, |\psi_2>\in \mathcal{H} \tag{6.2.6.94}$$

having the effect of restricting the integral to the physical degrees of freedom.

With the gauge-fixing $\tau = t$, what the classical analysis of overpassing the busy beaver function becomes under quantization of the box ?

Clearly such a treatment should be considered as the one-particle approximation of the quantum field theory of a Klein-Gordon field on Gödel's space time whose consistence requires the involved energies are less than the mass-gap of the theory [Wit99a].

It should be mentioned that while our previous formalization of Calude-Dinnen-Svozil's classical considerations is accademical since the assumpution of axiom6.2.1 or weaker forms of it is rather compelling from a physical point of view, the possibility of time-machines when Quantum Mechanics is taken into account is a strongly debated issue about which we have no competence and about which we demand to [Nah01].

Considered again the quantum computer Q of definition6.2.1 Svozil have introduced the following quantities:

DEFINITION 6.2.26

UNIVERSAL QUANTUM ALGORITHMIC PROBABILITY OF $|\psi>\in \mathcal{H}_2^{\bigotimes \star}$:

$$P_Q(|\psi>) := \sum_{\vec{x}\in\Sigma^{\star}} 2^{-\frac{|\vec{x}|}{2}} | <True|Q(\vec{x})|^2 \tag{6.2.6.95}$$

DEFINITION 6.2.27

UNIVERSAL QUANTUM HALTING AMPLITUDE:

$$\Omega_Q := \sum_{\vec{x}\in\Sigma^{\star}} 2^{-\frac{|\vec{x}|}{2}} | <True|Q(\vec{x})|^2 \tag{6.2.6.96}$$

The next step of Svozil's contribution has been the conjecture (cfr. the 17^{th} open problem of the list [Cal96]) that in Quantum Algorithmic Information Theory it should be possible to formulate undecidability theorems analogues to the two classical ones by Chaitin.

Let us then formalize the previously informally introduced notions of **classical formal systems** and **quantum formal systems** in the following way:

DEFINITION 6.2.28

CLASSICAL FORMAL SYSTEM:
an r.e. set:

$$CFS \; := \; \{(\vec{a}_i \, , \vec{T}_i)\}_{i \in I} \tag{6.2.6.97}$$

where:

$$card(I) \in \mathbb{N} \tag{6.2.6.98}$$

$$\vec{a}_i \, , \vec{T}_i \in \Sigma^{\star} \;\; \forall i \in I \tag{6.2.6.99}$$

Given a classical formal system $CFS \; := \; \{(\vec{a}_i \, , \vec{T}_i)\}_{i \in I}$ the meaning of definition6.2.28 is the following: every couple $(\vec{a}_i \, , \vec{T}_i)$ is a **rule of inference** of CFS stating that the theorem (indexed by the string) $\vec{T}_i$ may be deduced from the **axiom** (indexed by the string) $\vec{a}_i$.

According to this interpretation we will express the fact that the couple of strings $(\vec{a}_i \, , \vec{T}_i)$ belongs to CFS by the notation $\vec{a} \vdash_{CFS} \vec{T}$.

We are now ready for the following:

Theorem 6.2.8

FIRST CHAITIN'S UNDECIDABILITY THEOREM:
HP:

CFS classical formal system with a unique axiom $\vec{a} \in \Sigma^{\star}$
TH:

$$\exists \, c_{CFS}^{(1)} \in \mathbb{R}_{+} \; : \; [\,(a \vdash_{CFS} I(\vec{x}) > n) \; \Rightarrow \; (I(\vec{x}) > n)\,] \; \Rightarrow \; [\,(a \vdash_{CFS} I(\vec{x}) > n) \; \Rightarrow \; n \, < \, I(\vec{a}) + c_{CFS}^{(2)}] \tag{6.2.6.100}$$

PROOF:

Consider the following Chaitin computer C:

for $\vec{u}, \vec{v} \in \Sigma^{\star}$ such that:

$$U(\vec{u}\,,\,\lambda) \;=\; string(k)\; and\, U(\vec{v}\,,\,\lambda) \;=\; \vec{a} \tag{6.2.6.101}$$

put:

$C(\vec{u}\cdot\vec{v},\lambda) \;:=\;$ the first string $\vec{s}$ that can be shown in CFS to have algorithmic information greater than $k+|\vec{v}|$.

Among the possible inputs for C we may find the minimal self-delimiting descriptions for $string(k)$ and $\vec{a}$, i.e.:

$$u \;=\; (string(k))^{\star}\;,\; \vec{v} \;=\; \vec{a}^{\star} \tag{6.2.6.102}$$

having algorithmic information $I(string(k))\,,\, I(\vec{a})$ respectively.

If $C(\vec{u}\cdot\vec{v}\,,\,\lambda) \;=\; \vec{s}$, then:

$$I_C(\vec{s}) \;\leq\; |\vec{u}\cdot\vec{v}| \;\leq\; |(string(k))^{\star}|\,|\vec{a}^{\star}| \tag{6.2.6.103}$$

On the other hand, for some constant d:

$$k+|\vec{a}^{\star}| \;<\; I(\vec{s}) \;\leq\; |(string(k))^{\star}\,\vec{a}^{\star}| \,+\, d \tag{6.2.6.104}$$

We therefore get the following crucial inequalities:

$$k+I(\vec{a}) \;<\; I(\vec{s}) \;\leq\; I(string(k))+I(\vec{a})+d \tag{6.2.6.105}$$

This implies:

$$k \;<\; I(string(k))+d \;=\; O(\log k) \tag{6.2.6.106}$$

which can be true only for finitely many values of the natural k.

Pick now $c_F \;=\; k$, where k is the value that violates the above inequality. We have proven that $\vec{s}$ cannot exist for $k \;=\; c_F$ ■

Remark 6.2.6

FIRST CHAITIN'S UNDECIDABILITY THEOREM AND BERRY'S PARADOX:

Theorem6.2.8 has a deep conceptual meaning, suggesting that the mathematical phenomenon of undecidability may have an information-theoretic nature:

in facts it tells us that a classical formal system CFS have an explicative power ruled by its classical algorithmic information I(CFS), in that it cannot be used to prove that some object has classical algorithmic information substantially greater than itself.

Exactly as the proof of Gödel's First Undecidability Theorem starts from a self-reference's paradox, i.e the Liar Paradox:

$$<< \textit{This statement is false} >>$$

by:

1. its modification in a form:

   $$<< \textit{This statement is unprovable} >>$$

   that it is no more paradoxical (since assuming that statement is indeed true and, hence, unprovable, no contradiction arises)

2. its formalization as as statement of Arithmetics by Gödel numbering

the proof of theorem6.2.8 lies on another self-reference's paradox, i.e the Berry's paradox:

$$<< \textit{Let x be the least number that cannot be defined in less than 16 words} >>$$

(whose paradoxical nature lies on the fact that such a statement determines x by 15 words).

Let us now consider the sequence $\bar{\Omega} := \{\Omega_n\}_{n \in \mathbb{N}}$ of the binary digits of the nonterminating dyadic expansion of the Halting Probability $\Omega := \Omega_U$ w.r.t. to the fixed universal Chaitin computer, i.e.:

$$\bar{\Omega} := (\mathcal{N}|_{\Sigma^\infty - \Sigma^\star})^{-1}(\Omega) \qquad (6.2.6.107)$$

One has that:

Theorem 6.2.9

SECOND CHAITIN'S UNDECIDABILITY THEOREM:
HP:

$CFS := \{(\vec{a}_i, \vec{T}_i)\}_{i \in I}$ classical formal system whose axiom's set $A := \{\vec{a}_i\}_{i \in I}$ is such that:

$$(A \vdash_{CFS} << \Omega_n = i >> \Rightarrow \Omega_n = i) \ \forall i \in \Sigma, \forall n \in \mathbb{N} \qquad (6.2.6.108)$$

and whose theorems' set $T := \{\vec{T}_i\}_{i \in I}$ is r.e.
TH:

$$\exists c^{(2)}_{CFS} \in \mathbb{N}_+ : \\ [(A \vdash_{CFS} << \cdot_{k=1}^{n} \Omega_{i_k} = \vec{x} >>) \Rightarrow (n < I(CFS) + c^{(2)}_{CFS} >>)] \\ \forall i_1, \cdots, i_n \in \mathbb{N}, \forall \vec{x} \in \Sigma^n \qquad (6.2.6.109)$$

PROOF:

If T provides k different cbits of Ω, then it gives us a covering $Cover_k$ of measure 2^{-k} which includes Ω.

Let us enumerate T until k cbits of Ω, $\Omega_{i_1}, \cdots, \Omega_{i_k}$ $i_1 < i_2 < \cdots < i_k$ are determined.

Put:

$$\begin{aligned} Cover_k \; := \; \{x_1 \Omega_{i_1}, x_2 \Omega_{i_2}, \cdots, x_k \Omega_{i_k} : x_1, x_2, \cdots, x_k \in \Sigma^\star \\ |x_1| := i_1 - 1, |x_2| := i_2 - i_1, |x_k| := i_k - i_{k-1}\} \subset \Sigma^\star \end{aligned} \quad (6.2.6.110)$$

By construction $Cover_k$ is a covering; furthermore:

$$P_{unbiased}(Cover_k \, \Sigma^\infty) \; = \; \frac{2^{i_k} - k}{2^{i_k}} \; = \; 2^{-k} \quad (6.2.6.111)$$

So T yelds infinitely many cbits of Ω, contradicting theorem1.4.4 ■

Remark 6.2.7

USING THE DIGITS OF Ω TO DECIDE ALL THE FINITELY REFUTABLE CONJECTURES:

To appreciate the meaning of theorem6.2.9 let us observe that the knowledge of $\vec{\Omega}(n)$, $n \in \mathbb{N}$ allows to solve the halting problem for all the programs of length less or equal to n, as can be proved in the following way:

since:

$$\Omega \; \in \; (\mathcal{N}(\vec{\Omega}(n)0^\infty), \mathcal{N}(\vec{\Omega}(n)0^\infty) + 2^{-n} \quad (6.2.6.112)$$

one can simply make a sistematic search through all programs the eventually halts until enough halting programs $p_{i_1}, p_{i_2} \cdots p_{i_k}$, of length, respectively, $l_{i_1}, l_{i_2} \cdots l_{i_k}$, such that:

$$\sum_{j=1}^{k} 2^{-l_{i_j}} \; > \; \mathcal{N}(\vec{\Omega}(n)0^\infty) \quad (6.2.6.113)$$

But then observe eq.6.2.6.113 assure us that the collection of programs $p_{i_1}, p_{i_2} \cdots p_{i_k}$ contains all the halting programs of length less or equal to n.

We saw in remark6.2.4 that the Recursive Unsolvability of the Halting Problem implies Gödel's First Undecidability Theorem.

With the same argument involved in such a proof one may immediately infer that the solution of the n-length Halting Problem furnished by the knowledge of $\vec{\Omega}(n)$ implies the decision of all finitely refutable conjectures that can be expressed by at most n cbits.

Remark 6.2.8

ON THE CONSTANTS IN CHAITIN'S UNDECIDABILITY THEOREM:

The recent LISP implementation by Chaitin of his undecidability theorems [Cha98] shows constructively that two numbers $c_{CFS}^{(1)}$ and $c_{CFS}^{(2)}$ are concretelly computable (he computes them !).

It must be observed, anyway, that $c^{((1)}_{CFS}$ and $c^{(2)}_{CFS}$ depend also on the fixed Chaitin Universal computer U. Allowing U to vary we will have to denote them by $c^{(1)}_{CFS,U}$ and $c^{(2)}_{CFS,U}$.

Let us consider, in particular, the classical formal system ZFC giving foundations to Mathematics:

Robert Solovay has recentely proved that [Sol00]:

Theorem 6.2.10

SECOND SOLOVAY'S THEOREM:

HP:

ZFC is consistent

TH:

$$\exists \, U \text{ universal Chaitin computer } \ : \ c^{(2)}_{CFS,U} \, = \, 0$$

Most of the conceptual deepness of theorem6.2.9 lies on its link with the tenth of the celebrated list of 23 unsolved problem David Hilbert presented in 1900 at the Second International Congress of Mathematics in Paris he considered would have been the germs of the incoming new century.

Given a polynomial $P(x \, , \, y_1, \cdots , y_m)$ with integer coefficients (an $\mathbb{N}$-polynomial from here and beyond):

DEFINITION 6.2.29

SOLUTIONS' SET OF P:

$$SOL(P) \; := \; \{ x \in \mathbb{N} \, : \, P(x \, , \, y_1, \cdots , y_m) \, = \, 0 \text{ for some } y_1, \cdots , y_m \, \in \, \mathbb{N} \} \tag{6.2.6.114}$$

DEFINITION 6.2.30

HILBERT'S TENTH PROBLEM:

to construct an algorithm $HILBERT10[P]$ that receiving as input an $\mathbb{N}$-polynomial P outputs:

$$HILBERT10[P] \; := \; \begin{cases} True & \text{if } SOL(P) \neq \emptyset, \\ False & \text{otherwise.} \end{cases} \tag{6.2.6.115}$$

Considered now a set $S \, \subseteq \, \mathbb{N}$:

DEFINITION 6.2.31

S IS DIOPHANTINE:

$$\exists\, P\, \mathbb{N} - polynomial \;:\; S \,=\, SOL(P) \qquad (6.2.6.116)$$

The intellectual path of thirty years by Martin David, Hilary Putnam and Julia Robinson was completed by Yuri Matiyasevich in 1970 through the proof of the following [Mat01]:

Theorem 6.2.11

MATIJASEVIC'S THEOREM:

$$S\, Diophantine \;\Leftrightarrow\; S\, r.e. \qquad (6.2.6.117)$$

from which immediately follows that:

Corollary 6.2.1

the Hilbert's Tenth Problem is recursively-unsolvable.

Let us now consider exponential $\mathbb{N}$-polynomials, i.e. polynomials built not only by addition and multiplications, but also by exponentiations.

DEFINITION 6.2.32

S IS EXPONENTIAL-DIOPHANTINE:

$$\exists\, P\, exponential - \mathbb{N} - polynomial \;:\; S \,=\, SOL(P) \qquad (6.2.6.118)$$

Theorem6.2.11 immmediately implies that:

Corollary 6.2.2

$$S\, exponential - Diophantine \;\Leftrightarrow\; S\, r.e. \qquad (6.2.6.119)$$

It is possible, anyway, to prove a stronger result; introduced the following:

DEFINITION 6.2.33

S IS SINGLE-FOLD EXPONENTIAL DIOPHANTINE:

$S \,=\, SOL(P)$, where the exponential-Diophantine-polynomial $P(x\,,\, y_1, \cdots, y_m)$ is such that:

$$\forall x \in S\; \exists\,!(y_1, \cdots, y_m) \in \mathbb{N}^m \;:\; P(x\,,\, y_1, \cdots, y_m) \,=\, 0 \qquad (6.2.6.120)$$

one has that:

Theorem 6.2.12

JONES-MATIJASEVIC'S THEOREM:

$$S\, single - fold - exponential - Diophantine \;\Leftrightarrow\; S\, r.e. \qquad (6.2.6.121)$$

Theorem6.2.12 allows to prove the following:

Theorem 6.2.13

LINK BETWEEN THE HALTING PROBABILITY AND HILBERT'S TENTH PROBLEM:

$\exists\ P(n\,,\,x\,,\,y_1,\cdots,y_m)$ exponential-Diophantine-polynomial such that for every $k \in \mathbb{N}$ the equation:

$$P(n\,,\,x\,,\,y_1,\cdots,y_m) \tag{6.2.6.122}$$

has an infinite number of solutions iff the k^{th} bit of Ω is 1

PROOF:

One has obviously that:

$$\mathcal{N}|_{\Sigma^{\infty}-\Sigma^{\star}} \ \in\ \mathbb{Q}\ \ \forall n \in \mathbb{N} \tag{6.2.6.123}$$

Furthermore:

$$<<\ (\vec{\Omega}(k))_m\ =\ 1\ >> \in REC(\mathbb{N})\ \ \forall n,k \in \mathbb{N}\,:\, m < n \tag{6.2.6.124}$$

where we have followed the convention introduced in section1.1 of identifying **unary predicates** with the sets of the elements satisfying them.

But then, using theorem6.2.12, one gets an equation:

$$P(n\,,\,x\,,\,y_1,\cdots,y_m)\ =\ 0 \tag{6.2.6.125}$$

having:

- one solution $y_1,\cdots,y_m$ if the n^{th} cbit of $\vec{\Omega}(k)$ is 1
- no solution $y_1,\cdots,y_m$ if the n^{th} cbit of $\vec{\Omega}(k)$ is 0

The number of different m-ples of natural numbers which are solution of eq.6.2.6.125 is therefore infinite iff the n^{th} cbit of the base-2 expansion of Ω is 1. ■

The first step forward the derivation of quantum amalogues of Chaitin's Undecidability Theorems is to develop the theory of **Noncommutative Formal Systems** expanding the short preliminary considerations presented in section6.1.

Gereralizing the classical case one is led to the following:

DEFINITION 6.2.34

NONCOMMUTATIVE FORMAL SYSTEM:

a set:

$$NCFS\ :=\ \{(\vec{a}_i\,,\,\vec{\alpha}_i)\}_{i \in I} \tag{6.2.6.126}$$

where:

$$card(I) \in \mathbb{N} \tag{6.2.6.127}$$

$$\vec{a}_i\,,\,\vec{T}_i \in \Sigma_{NC}^{\star}\ \ \forall i \in I \tag{6.2.6.128}$$

Given a noncommutative formal system $NCFS := \{(\vec{a}_i , \vec{T}_i)\}_{i \in I}$ the meaning of definition6.2.34 is specular to the commutative case: every couple $(\vec{a}_i , \vec{T}_i)$ is a **rule of inference** of NCFS stating that the theorem (indexed by) $\vec{T}_i$ may be deduced from the **axiom** (indexed by) $\vec{a}_i$.

Again we will express the fact that the couple of strings $(\vec{a}_i , \vec{T}_i)$ belongs to CFS by the notation $\vec{a} \vdash_{NCFS} \vec{T}$.

Before trying to derive undecidability results quantifying the explicative power of a quantum formal system by its quantum algorithmic information, let us analyze a bit definition6.2.34 from the point of view of Moore's generalization of **Chomsky's Hierarchy** and of the **duality languages versus automata**.

Following the first chapter of [Pau01] let us start from the following:

DEFINITION 6.2.35

CLASSICAL REWRITING SYSTEM:
a couple of the form (Σ , P) where P is a finite subset of $\Sigma^{\star} \times \Sigma^{\star}$ whose elements are called the **productions** of (Σ , P).

Given a classical rewriting system $\gamma := (\Sigma , P)$ let us introduce the following intuitive notation for productions:

$$(\vec{x} \rightarrow \vec{y}) := (\vec{x} , \vec{y}) \in P \qquad (6.2.6.129)$$

Given two words $\vec{x} , \vec{y} \in \Sigma^{\star}$:

DEFINITION 6.2.36

$\vec{x}$ IMMEDIATELY IMPLIES $\vec{y}$ IN γ ($\vec{x} \Rightarrow_{\gamma} \vec{y}$):
$\exists \vec{x}_1 , \vec{x}_2 , \vec{u} , \vec{v} \in \Sigma^{\star}$:

$$\vec{u} \rightarrow \vec{v} \qquad (6.2.6.130)$$
$$\vec{x} = \vec{x}_1 \vec{u} \vec{x}_2 \qquad (6.2.6.131)$$
$$\vec{y} = \vec{x}_1 \vec{v} \vec{x}_2 \qquad (6.2.6.132)$$
$$(6.2.6.133)$$

DEFINITION 6.2.37

IMPLICATION'S RELATION OF γ ($\Rightarrow_{\gamma}$)
the symmetric and transitive closure of γ

DEFINITION 6.2.38

PURE GRAMMAR:
a therne $G := (\Sigma , P , \vec{a})$ such that:

- (Σ , P) is a rewriting system
- $\vec{a} \in \Sigma^{\star}$ is called the **axiom** of G

Given a pure grammar $G := (\Sigma , P , \vec{a})$:

DEFINITION 6.2.39

LANGUAGE GENERATED BY G:

$$L(G) := \{\vec{x} \in \Sigma^\star : \vec{a} \Rightarrow_\gamma^\star \vec{x}\} \tag{6.2.6.134}$$

DEFINITION 6.2.40

CHOMSKY'S GRAMMAR:
a quintuple $G := (N , T , S , P)$ such that:

- N and T are disjoint finite alphabet called, respectively, the **nonterminating alphabet** and the **terminating alphabet**
- $S \in N$ is called the **axiom** of G
- P is a finite subset of $(N \bigcup T)^\star \cdot N \cdot (N \bigcup T) \cdot (N \bigcup T)^\star$ called the **productions' set** of G

As for pure grammars $\vec{u} \rightarrow \vec{v}$ will stand for $(\vec{u} , \vec{v}) \in P$.
Given a Chomsky grammar $G := (N , T , S , P)$ and two words $\vec{x} , \vec{y} \in (N \bigcup T)^\star$:

DEFINITION 6.2.41

$\vec{x}$ IMMEDIATELY IMPLIES $\vec{y}$ IN G ($\vec{x} \Rightarrow_G \vec{y}$):
$\exists \vec{x}_1 , \vec{x}_2 \in (N \bigcup T)^\star , \vec{u} \rightarrow \vec{v} \in P$ such that:

$$\vec{u} \Rightarrow \vec{v} \tag{6.2.6.135}$$
$$\vec{x} = \vec{x}_1 \vec{u} \vec{x}_2 \tag{6.2.6.136}$$
$$\vec{y} = \vec{x}_1 \vec{v} \vec{x}_2 \tag{6.2.6.137}$$
$$\tag{6.2.6.138}$$

The implication $\Rightarrow_G^\star$ is then defined as the symmetric and transitive closure of $\Rightarrow_G$ exactly as for pure grammars.

DEFINITION 6.2.42

$\vec{x} \in (N \bigcup T^\star)$ IS A SENTENTIAL FORM IN G:

$$S \Rightarrow_G^\star \vec{x} \tag{6.2.6.139}$$

DEFINITION 6.2.43

LANGUAGE GENERATED BY G:

$$L(G) := \{\vec{x} \in T^\star : S \Rightarrow_G^\star \vec{x}\} \tag{6.2.6.140}$$

Remark 6.2.9

LANGUAGES GENERATED BY PURE GRAMMARS AND CHOMSKY GRAMMARS

Comparing definition6.2.43 with definition6.2.39 it is essential to observe that the language generated by a Chomsky grammars contains only sentential forms that are strings over the terminating alphabet.

DEFINITION 6.2.44

G IS CONTEXT-SENSITIVE:

$$|\vec{u}| \leq |\vec{v}| \ \forall \vec{u} \to \vec{v} \in P \tag{6.2.6.141}$$

DEFINITION 6.2.45

G IS CONTEXT-FREE:

$$\vec{u} \in N \ \forall \vec{u} \to \vec{v} \in P \tag{6.2.6.142}$$

DEFINITION 6.2.46

G IS LINEAR:

$$\vec{u} \in N \, and \, \vec{v} \in T^{\star} \bigcup T^{\star} \cdot N \cdot T^{\star} \ \forall \vec{u} \to \vec{v} \in P \tag{6.2.6.143}$$

DEFINITION 6.2.47

G IS REGULAR:

$$\vec{u} \in N \, and \, \vec{v} \in T \bigcup T \cdot N \cdot \{\lambda\} \ \forall \vec{u} \to \vec{v} \in P \tag{6.2.6.144}$$

DEFINITION 6.2.48

FINITE LANGUAGES:

$$FIN := \{L \subset A^{\star} : \max(card(A), card(L)) < \infty\} \tag{6.2.6.145}$$

DEFINITION 6.2.49

REGULAR LANGUAGES:

$$REG := \{L(G) : G \text{ regular Chomsky grammar}\} \tag{6.2.6.146}$$

DEFINITION 6.2.50

LINEAR LANGUAGES:

$$LIN := \{L(G) : G \text{ linear Chomsky grammar}\} \tag{6.2.6.147}$$

DEFINITION 6.2.51

CONTEXT-FREE LANGUAGES:

$$CF := \{L(G) : G \text{ context-free Chomsky grammar}\} \tag{6.2.6.148}$$

DEFINITION 6.2.52

RECURSIVELY ENUMERABLE LANGUAGES:

$$RE := \{L(G) : G \text{ Chomsky grammar}\} \tag{6.2.6.149}$$

One has that:

Theorem 6.2.14

CHOMSKY'S HIERARCHY:

$$FIN \subset REG \subset LIN \subset CF \subset CS \subset RE \tag{6.2.6.150}$$

There exist a natural duality among languages and computing devices; Given a language L and a computing device D:

DEFINITION 6.2.53

D ACCEPTS L:
the final internal state of D under the input x belongs or not a subset of accepting states of D's set of internal states according to whether the word x belong or not to the language L

Such a duality between languages and automata induces a hierarchy of different kinds of computing devices able to accept the various kinds of languages in Chomsky's hierarchy:

LANGUAGES	AUTOMATA
regular	finite
linear	one-turn pushdown
context-free	pushdown
context-sensitive	linear-bounded
recursively enumerable	Turing

Remark 6.2.10

CHURCH'S THESIS AND CHOMSKY'S HIERARCHY
Reasoning in an opposite way from the usual one, i.e. looking at the notion of **recursivity** as a derived notion induced from the primary notion of **recursive enumerability** defining a recursive function as a function having an r.e. graph, one can look at Church's thesis as the statement that Chomsky's hierarchy stops with recusively enumerable languages, i.e. that there doesn't exist a grammar more powerful than Chosmky's grammar as to effective generation of languages is concerned.

The duality between languages and automata identifies Turing Machines,as the more powerful computational device for accepting languages.

While we will define Turing machines in section8.1, we won't introduce the other less powerful computational devices for which we demand to [Wey94], [Pap98] (and to the Mathematica packages developed by Jaime Rangel Mondragón [Mon99] for their concrete implementation on computer).

What it is relevant to our purposes is to observe that under noncommutative generalization both the duality languages-automata and the existence of Chomsky's hierarchy in the degree in generating power of grammar preserve, as it has been shown by Christopher Moore [Cru97].

Before of trying to use theorem6.2.34 to derive quantum analogues of theorem6.2.8 and theorem6.2.9, one should check whether the naife definition6.2.34 is correct from the point of view of the quantum Chomsky' hierarchy, i.e. if it raelly characterizes those qwuantum languages that are generated by quantum Chomsky grammars.

This is a conditio sine qua non, since only in this case the definition6.2.34 is the mathematical-logic counterpart, via the languages-automata-duality, of the computational device formalizing Quantum Computation, i.e. the Quantum Turing Machine we will introduce in section8.1

6.3 Yuri Manin's suggestion at the June 1999 Bourbaki seminar

6.4 Paul Vitanyi's Quantum Kolmogorov complexity

6.5 The objection by Berthiaume van Dam and Laplante to Vitanyi

6.6 Peter Gacs' quantum algorithmic entropy

6.7 The algorithmic approach to Quantum Chaos Theory: quantum algorithmic information versus quantum dynamical entropies

Chapter 7

Typical properties in Quantum Probability Theory

7.1 Conformism in Quantum Probability Theory

The approaches to Quantum Algorithmic Information Theory by Karl Svozil, by Paul Vitanyi, by Berthiaume van Dam and Laplante and by Paul Gacs have a thing in common: they deal with **strings of qubits**.

Starting from strings of qubit is seen, indeed, as simpler, the case of sequences of qubits being seen as a derived, more complicate issue to be derived in a second time by the case of strings.

As we stressed in the remark1.4.1, anyway, a sharp distinction between regularity and randomness in the classical case is impossible for strings but only for sequences.

This is essentially owed to the fact that theorem2.2.1, whose importance we underlined in the remark 3.3.1, holds only for sequences.

So, despite of appearances, as to algorithmic randomness the analysis of **sequences** is greatly conceptually clearer and simpler than that of **strings**.

This implies that the same happens as to quantum algorithmic randomness where a quantum analogue of theorem4.2.2 can hold only in the case of sequences.

As a conclusion, as to the characterization of **quantum algorithmic randomness**, one has to start from **sequences of qubits** and not from **strings of qubits**.

This was indeed the attitude of the approach by Coleman and Lesniewski, who, anyway, failed in individuating the correct space of qubits' sequences, with the consequences we reported in the remark6.1.1.

Our objective here consists in trying of characterizing the correct notion of an **algorithmic random sequence of qubits** by formulating a suitable quantum analogue of the approach pursued in chapter3.

Given a noncommutative collectivity S_{NC} made of $N := n^2 \in \mathbb{N}$ noncommutative people:

$$cardinality_{NC}(S_{NC}) = n^2 \tag{7.1.7.1}$$

(i.e. $S_{NC} = M_n(\mathbb{C})$) our objective is to define a **typical property** of S_{NC}.

We will have to face a certain number of issues conceptually based on the double nature of a Von Neumann algebra:

- as a commutative set
- as a noncommutative set

as we stressed in the remark5.1.2.

The first issue we have to deal with is the following:

FIRST ISSUE: Have we to consider ordinary, commutative, properties or noncommutative properties?

We shall try to answer the following question following both the alternatives and comparing them:

1. Properties have to be considered as classical, i.e. ordinary, predicates over S_{NC}.

   Thus an other subproblem arises:

   SECOND ISSUE: How have one to count the number of the elements of S_{NC} having a given property ?

   Mimicking the classical case one would be tempted to consider the quantity:

   $$cardinality(\{x \in S_{NC} \, : \, p(x) \; holds\}$$

   But this doesn't seem to be such a good idea, as can be seen considering, for example, the predicate:

   $$p_{unitarity}(x) := << x^{\star} x = x x^{\star} = I >> \tag{7.1.7.2}$$

   and observing that obviously:

   $$cardinality(\{x \in S_{NC} \, : \, p_{unitarity}(x) \; holds\}) = \aleph_1^{\frac{n^2}{2}} = \aleph_1 = \aleph_1^{n^2} = cardinality(S_{NC}) \tag{7.1.7.3}$$

   So one infers that to count the number of elements having a given property one has to use noncommutative cardinality.

   This, anyway, requires the restriction to properties such that the subset of all the elements of S_{NC} having such a property is a sub-factor of S_{NC}.

Example 7.1.1

MATRICES WITH CONSTRAINED FIRST ENTRY:

Let us consider the following family of predicates:

$$p_{\text{first entry not y}}(x) \ := << x_{1,1} \ \neq \ y >> \quad y \in \mathbb{C} \tag{7.1.7.4}$$

We would be tempted to say that the majority of people in S_{NC} have this property so that it must be considered a **majoritary property** of S_{NC}.

But if votes are counted by noncommutative cardinality, this may be true only if $y = 0$, since the set $\{x \in S_{NC} \ : \ p_{\text{first entry not y}}(x) \ holds\}$ is not a subfactor of S_{NC} for every $y \neq 0$ and conseguentially:

$$cardinality_{NC}(\{x \in S_{NC} \ : \ p_{\text{first entry not y}}(x) \ holds\}) \ = \uparrow \quad \forall y \neq 0 \tag{7.1.7.5}$$

Let us consider, for example, the unitarity predicate of eq.7.1.7.2 for which we have that:

$$cardinality_{NC}(\{x \in S_{NC} \ : \ p_{unitarity}(x) \ holds\} \ = \ \frac{N}{2} \tag{7.1.7.6}$$

Thus we conclude that $p_{unitarity}$ is neither a **majoritary property** nor a **minoritary property**.

Let us consider, instead, the following predicate:

$$p_{\text{traceless skew-adjoint}}(x) \ := << x^{\star} \ = \ -x \ and \ \tau_{unbaised}(x) = 0 >> \tag{7.1.7.7}$$

Since:

$$cardinality_{NC}(\{x \in S_{NC} \ : \ p_{\text{traceless skew-adjoint}}(x) \ holds\}) \ = \ \frac{N-1}{2} \tag{7.1.7.8}$$

we conclude that $p_{\text{traceless skew-adjoint}}$ is a **minoritary property** of S_{NC}, so that its negation $p^{\perp}_{\text{traceless skew-adjoint}}$ is a **majoritary property**.

As in the commutative case a typical properties is then defined as a property $p(\cdot)$ such that:

$$cardinality_{NC}(\{x \in S_{NC} \ : \ p_(x) \ holds\}) \ \gg \ \frac{N}{2} \tag{7.1.7.9}$$

This is the case, for example, of the property $p_{\text{first entry not 0}}$ we introduced in example7.1.1 provided $N \gg 1$, where, as in the commutative case, the informality of such a notion derives from the informal nature of the **very greater than** ordering relation.

Let us now consider an infinite countable noncommutative community $cardinality_{NC}(S_{NC}) = \aleph_0$. As in the commutative case the same notion of a **majoritary property** loses its meaning.

Exactly as in the classical case, anyway, one has that for an infinite uncountable noncommutative community the notion of a typical property may be defined provided S_{NC} admits an unbiased noncommutative probability distribution $\tau_{unbaised}$, i.e. provided $Type(S_{NC}) = II_1$: in this case a **typical property** is defined as a property holding $\tau_{unbaised}$-almost everywhere

2. Properties have to be considered as noncommutative propositions over S_{NC}, i.e. as elements of the quantum logic $QL(S_{NC})$ of S_{NC}.

   The set of typical properties of a noncommutative probability space of the form (S_{NC} , ω) will then be subset of $\mathcal{P}(S_{NC})$ and, clearly, won't satisfy the distributive law as to conjunction and disjunction of its elements.

Let us now formalize these considerations, demanding to the remark5.1.2 for their conceptual foundations.

Given a noncommutative probability space (A , ω):

DEFINITION 7.1.1

COMMUTATIVE PREDICATES OVER A:

$$\mathcal{P}_C(A) := \{p(x) \text{ statement concerning } x \in A\} = MAP(X, \{0,1\}) \tag{7.1.7.10}$$

DEFINITION 7.1.2

NONCOMMUTATIVE PREDICATES OVER A:

$$\mathcal{P}_{NC}(A) := \mathcal{P}(A) \tag{7.1.7.11}$$

Example 7.1.2

COMMUTATIVE AND NONCOMMUTATIVE PREDICATES OVER THE ONE QUBIT ALPHABET

Given the one qubit alphabet $\Sigma_{NC} = M_2(\mathbb{C})$, let us consider the following commutative predicates:

$$\begin{aligned}
p_{normality}(x) &:= << xx^\star = x^\star x >> \\
p_{hermitianicity}(x) &:= << x = x^\star >> \\
p_{positivity}(x) &:= << \exists y : x = yy^\star >> \\
p_{projectivity}(x) &:= << x = x^\star = x^2 >> \\
p_{unitarity}(x) &:= << xx^\star = x^\star x = I >>
\end{aligned}$$

belonging to the classical logic $(\Sigma_{NC} , \leq_C , \perp_C)$.

Let us observe that:

$$p_{projectivity} \leq_C p_{positivity} \leq_C p_{hermitianicity} \leq_C p_{normality} \quad (7.1.7.12)$$
$$p_{projectivity} \leq_C p_{unitarity} \leq_C p_{normality} \quad (7.1.7.13)$$

so that the neither **orthomodularity** nor the **modularity** of $(\Sigma_{NC}, \leq_C, \perp_C)$ would be by itself sufficient to guarantee, for example, that:

$$p_{hermitianicity}(x) \bigvee (p_{positivity}(x) \bigwedge p_{projectivity}(x)) = (p_{hermitianicity}(x) \bigvee p_{positivity}(x)) \bigwedge (p_{hermitianicity}(x) \bigvee p_{projectivity}(x)) \ \forall x \in M_2(\mathbb{C}) \quad (7.1.7.14)$$

that may inferred only by **distributivity**.

One has clearly that:

$$\mathcal{P}_{NC}(\Sigma_{NC}) = \mathcal{P}(\Sigma_{NC}) = \{x \in \Sigma_{NC} : p_{projectivity}(x) \ holds\} \quad (7.1.7.15)$$

A not-trivial projection has the form:

$$p_{\vec{n}} := \frac{1}{2}(I + \vec{\sigma} \cdot \vec{n}) \ \vec{n}^2 = 1 \quad (7.1.7.16)$$

and, in the physical realization of Σ_{NC} as a spin $\frac{1}{2}$ system, corresponds to the statement:

<< a measurement of $\vec{\sigma}$ in the direction $\vec{n}$ gives outcome $+1$ with certainty >>

or, more concisely:

<< the spin point in the direction $\vec{n}$ >>

assuming with Einstein Podolski and Rosen [Ros83] that:

"If, without in any way disturbing a system, we can predict with certainty (i.e. with probability equal to unity) the value of a physical quantity, then there exist an element of physical reality corresponding to this physical quantity"

A simple calculation shows that the rules of the game are:

1. $$p_{\vec{n}}^{\perp} = p_{-\vec{n}} \ \forall \vec{n} \quad (7.1.7.17)$$

2. $$p_{\vec{n}_1} \bigvee p_{\vec{n}_2} = 0 \ \forall \vec{n}_1 \neq \vec{n}_2 \quad (7.1.7.18)$$

3. $$p_{\vec{n}_1} \bigwedge p_{\vec{n}_2} = 1 \ \forall \vec{n}_1 \neq \vec{n}_2 \quad (7.1.7.19)$$

whose meaning is [Thi01]:

1. We are sure that $\vec{\sigma}$ does not point in the direction $\vec{n}$ only if it points to $-\vec{n}$
2. The sharpest proposition which is implied by both $<<$ $\vec{\sigma}$ points to $\vec{n}_1$ $>>$ and $<<$ $\vec{\sigma}$ points to $\vec{n}_2$ $>>$ is the tautology $<<$ the spin points somewhere $>>$
3. The proposition $<<$ $\vec{\sigma}$ points to $\vec{n}_1 \, and \, \vec{n}_2$ $>>$ is always false

They immediately imply the violation of the distributive law:

$$p_{\vec{n}_1} \bigvee (\vec{n}_2 \bigwedge \vec{n}_3) \; = \; p_{\vec{n}_1} \bigvee 0 \; = \; p_{\vec{n}_1}$$
$$\neq \; (p_{\vec{n}_1} \bigvee p_{\vec{n}_2}) \bigwedge (p_{\vec{n}_1} \bigvee p_{\vec{n}_3}) \; = \; 1 \bigwedge 1 \; = \; 1 \;\; \forall \vec{n}_1 \neq \vec{n}_2 \neq \vec{n}_3 \quad (7.1.7.20)$$

Given a classical probability space $CPS \; := \; (X \, , \, \mu)$ and a commutative predicate over X $p(x) \, \in \, \mathcal{P}_C(X)$ let us introduce its fibre in zero:

$$N_p \; := \; \{ x \in X \; : \; p(x) \; = \; 0 \} \quad (7.1.7.21)$$

Looking at definition3.1.1 it is clear that:

$$p \in \mathcal{P}_{TYPICAL}(CPS) \; \Leftrightarrow \; \mu(N_p) \; = \; 0 \quad (7.1.7.22)$$

Let us now look at CPS as the commutative probability space $(A \; := \; L^{\infty}(X \, , \mu), \omega_{\mu}(\cdot) \; := \int_X d\mu \cdot)$.

We have clearly that:

$$p \in \mathcal{P}_{TYPICAL}(CPS) \; \Leftrightarrow \; \chi_{N_p} \in \mathcal{P}_{NC}(A) \quad (7.1.7.23)$$

so that we can express $\mathcal{P}_{TYPICAL}(CPS)$ as:

$$\mathcal{P}_{TYPICAL}(CPS) \; = \; \{ p \in \mathcal{P}_{NC}(A) \; : \; \omega(p) \; = \; 0 \} \quad (7.1.7.24)$$

Given an algebraic probability space $APS \; := \; (A \, , \, \omega)$, each of the two possible answers given to the FIRST ISSUE suggests a natural noncommutative generalization of the definition3.1.3:

1. looking at commutative properties of A one is lead to introduce the following:

   DEFINITION 7.1.3

   $S \; \subset A$ IS A NULL SET OF APS:

   $$E(a) \; = \; 0 \;\; \forall a \in S \quad (7.1.7.25)$$

   DEFINITION 7.1.4

TYPICAL COMMUTATIVE PROPERTIES OF APS:

$$\mathcal{P}_{C}^{TYPICAL}(APS) \equiv \{ p \in \mathcal{P}(A) : \{a \in A : p(a) \text{ doesn't hold } \} \text{ is a null set of APS}\} \tag{7.1.7.26}$$

2. looking at noncommutative properties of A one is led to introduce the following:

   DEFINITION 7.1.5

   TYPICAL NONCOMMUTATIVE PROPERTIES OF APS:

$$\mathcal{P}_{NC}^{TYPICAL}(APS) = \{p \in \mathcal{P}_{NC}(A) : \omega(p) = 0\} \tag{7.1.7.27}$$

Let us now try to formalize the idea of randomness as satisfaction of all typical properties, following again both the streets:

1. **DEFINITION 7.1.6**

   SET OF THE KOLMOGOROV COMMUTATIVELY-RANDOM ELEMENTS OF APS:

$$KOLMOGOROV - RANDOM_{C}(APS) := \{ a \in A : p(a) \; holds \; \forall p \in \mathcal{P}_{C}^{TYPICAL}(APS)\} \tag{7.1.7.28}$$

2. **DEFINITION 7.1.7**

   SET OF THE KOLMOGOROV NONCOMMUTATIVELY-RANDOM ELEMENTS OF APS:

$$KOLMOGOROV - RANDOM_{NC}(APS) := \bigvee_{p \in \mathcal{P}_{C}^{TYPICAL}(APS)} p \tag{7.1.7.29}$$

The efficacy of such a formalization will be investigated in section7.4.

7.2 Constraint on infinite noncommutatively-independent tosses of a quantum coin

We know by theorem2.2.1 that the correct notion of $NC_M - C_\Phi$-randomness, namely Martin-Löf Solovay-Chaitin randomness, satisfies the following intuitive condition:

CONSTRAINT 7.2.1

ON THE NOTION OF A RANDOM SEQUENCE ON THE COMMUTATIVE ALPHABET Σ :

*Making infinite **independent** trials of the experiment consisting on tossing a **classical coin** we must obtain an algorithmically-random sequence with probability one*

So a reasonable strategy to obtain informations about the correct definition of a random sequence of qubits would consist in:

- formulating an analogous constraint in terms of an infinite sequence of experiments consisting in tossing a quantum coin
- identifying the information that such a constraint gives on the correct way of of defining an algorithmically-random sequence of qubits

In the constraint7.2.1 the commutative random variables c_i and c_j on the commutative probability space $(L^\infty(\Sigma^\infty, P_{unbiased}), \tau_{unbiased})$ representing the results of the classical-coin tossings at times, respectively, $i, j \in \mathbb{N}$, are assumed to be **independent**:

$$\tau_{unbiased}(c_i^n c_j^m) = \tau_{unbiased}(c_i^n)\, \tau_{unbiased}(c_j^m) \quad \forall n, m \in \mathbb{N} \quad (7.2.7.1)$$

By theorem5.2.4 this implies that:

$$[\, c_i \, , \, c_j \,] \; = \; 0 \quad (7.2.7.2)$$

Let us now consider the quantum situation and let us adopt the terminology introduced in example5.1.7 and example5.2.4.

The quantum coin tossing at time $i \in \mathbb{N}$ will be described by the noncommutative random variable c_i associated, in the passage from $A_{\mathbb{Z}}$ to $R = \bigotimes_{n=0}^{\infty}(M_2(\mathbb{C}) \, , \, \tau_2)$, to a noncommutative random variable on the noncommutative probability space $(A_{\{i\}} \, , \, \tau_{\{i\}})$.

By theorem5.2.5 we have that:

$$c_i \; and \; c_j \text{ are independent } \; \forall i, j \in \mathbb{N} \quad (7.2.7.3)$$

Remark 7.2.1

COMMUTATIVE INDEPENDENCE VERSUS NONCOMMUTATIVE INDEPENDENCE

The adoption of the classical, commutative notion of independence in a quantum context is of great physical relevance, lying at the heart of one of the most important features of Quantum Physics, both foundationally and for applications: **entanglement**.

Anyway, from a conceptual viewpoint, it is reasonable to expect that in Noncommutative Probability Theory there must exist a notion of non-commutative independence according to which there may exist noncommutatively-independent random variables that don't commute among themselves.

Among the many proposals the more radical is Dan Voiculescu's Free Probability Theory [Pet00] according to which the own fact that two random variables commute and thus has some kind of algebraic interrelation among them is seen as a lack of genuine noncommutative-independence among them.

To introduce Free Probability Theory it is necessary to introduce some notions concerning free groups [Zie98].

Given a group G and a subsets of its $\chi \in G$:

DEFINITION 7.2.1

χ IS A SYSTEM OF GENERATORS OF G:
the smallest subgroup of G containing χ in G

DEFINITION 7.2.2

RANK OF G:

$$d(G) := \min\{cardinality(\chi)\, \chi \text{ system of generators of G}\} \qquad (7.2.7.4)$$

Given a system of generators χ of G let us consider an alphabet $\hat{\chi}$ such that there exist a bijection $b : \hat{\chi} \to \chi$.

Let us adopt capital letters $X, Y, Z, A, B, C, \cdots$ to denote elements of $\hat{\chi}$ and the corresponding small letters $x, y, z, a, b, c, \cdots$ for the corresponding elements of χ.

DEFINITION 7.2.3

WORD OVER $\hat{X}$ OF LENGTH $k \in \mathbb{N}_+$ ($|W| = k$)):
a formal expression:

$$W := W(\hat{\chi}) = \prod_{i=1}^{k} X_i^{\epsilon_i} \quad X_i \in \hat{\chi}, \epsilon_i \in \{-1, 1\} \forall i \in \{1, 2, \cdots, k\} \qquad (7.2.7.5)$$

DEFINITION 7.2.4

THE WORD $W(\hat{\chi})$ REPRESENTS THE ELEMENT $g \in G$:

$$g \;=\; W(\hat{\chi}) \;=\; \prod_{i=1}^{k} X_i^{\epsilon_i} \tag{7.2.7.6}$$

Given two words $W(\hat{\chi}) = g$ and $V(\hat{\chi}) = h$ representing respectively the elements g and h of G:

DEFINITION 7.2.5

PRODUCT OF $W(\hat{\chi})$ and $V(\hat{\chi})$:

$$W(\hat{\chi})V(\hat{\chi}) \;=\; gh \in G \tag{7.2.7.7}$$

DEFINITION 7.2.6

INVERSE WORD OF $W(\hat{\chi}) \;=\; \prod_{i=1}^{k} X_i^{\epsilon_i}$:

$$W(\hat{\chi})^{-1} \;:=\; \prod_{i=1}^{k} X_{k-i}^{-\epsilon_{k-i}} \tag{7.2.7.8}$$

Obviously if $W(\hat{\chi})$ represents $g \in G$ then $W(\hat{\chi})^{-1}$ represents $g^{-1} \in G$.

We will denote the **trivial word**, namely the thy word consisting of no letters and representing the identity $e \in G$ as I.

DEFINITION 7.2.7

PEAK:

a word of the form:

$$X^{\epsilon}X^{-\epsilon} \;\; X \in \hat{\chi}\,,\, \epsilon \in \{-1, 1\} \tag{7.2.7.9}$$

Given two words V and W:

DEFINITION 7.2.8

V AND W ARE FREELY EQUIVALENT:

$$V \;\equiv\; W \quad \text{V may be obtained by W inserting or deleting peaks} \tag{7.2.7.10}$$

DEFINITION 7.2.9

THE WORD $R(\hat{\chi}) \;:=\; X_1^{\epsilon_1} \cdots X_k^{\epsilon_k}$ IS A RELATOR W.R.T. χ AND G:

$$x_1^{\epsilon_1} \cdots x_k^{\epsilon_k} \;=\; 1 \quad \text{in G} \tag{7.2.7.11}$$

Given a system of relators $\mathcal{R}$:

DEFINITION 7.2.10

$\mathcal{R}$ IS A SYSTEM OF DEFINING RELATORS W.R.T. χ AND G:
every relator is a consequence of those in $\mathcal{R}$, i.e. is freely-equivalent to a word:

$$L_1(\hat{\chi})R_1(\hat{\chi})^{\eta_1}L_1(\hat{\chi})^{-1}\cdots L_k(\hat{\chi})R_k(\hat{\chi})^{\eta_1}L_k(\hat{\chi})^{-1} \quad R_j(\hat{\chi}) \in \mathcal{R}\,,\, \eta_j \in \{-1,1\}\, L_j(\hat{\chi}) \text{ word} \tag{7.2.7.12}$$

DEFINITION 7.2.11

PRESENTATION OF G:
a couple (χ , $\mathcal{R}$) such that:

- χ is a generating system of G
- $\mathcal{R}$ is a system of defining relators w.r.t. G and χ

Since to assign a presentation of a group is equivalent to assigning it, the fact that (χ , $\mathcal{R}$) is a presentation of the group G is usually indicated as:

$$G \ = < \chi|\mathcal{R} > \tag{7.2.7.13}$$

DEFINITION 7.2.12

G IS FINITELY GENERATED:

$$dim(G) \ < \ \aleph_0 \tag{7.2.7.14}$$

DEFINITION 7.2.13

G IS FINITELY PRESENTED:

$$G \ = < \chi|\mathcal{R} > \tag{7.2.7.15}$$

$$cardinality(\chi) \ < \ \aleph_0 \tag{7.2.7.16}$$

$$cardinality(\mathcal{R}) \ < \ \aleph_0 \tag{7.2.7.17}$$

Given a finitely presented group $G \ = < \chi|\mathcal{R} >$:

DEFINITION 7.2.14

WORD PROBLEM OF G:
the problem of determining if an arbitrary word in the elements of χ defines, as a consequence of $\mathcal{R}$, the identity element

DEFINITION 7.2.15

G IS A FREE GROUP:

$$G \ = < \chi|- > := < \chi|\emptyset > \tag{7.2.7.18}$$

i.e. if it has a presentation free of defining relators.
In particular:

DEFINITION 7.2.16

$$F_{n} \; := \; \text{free group} \; : d(F_{n}) \, = \, n \tag{7.2.7.19}$$

DEFINITION 7.2.17

FREE BASIS OF F_n:

$$\{ g_{1} \, , \, \cdots \, , \, g_{n} \} \; : \; F_{n} \; = < g_{1}, \cdots , g_{n} | - > \tag{7.2.7.20}$$

Remark 7.2.2

FREENESS AS ALGEBRAIC INDEPENDENCE

The fact that there doesn't exist any algebraic relation among the elements of a free-basis $\{g_1, \cdots, g_n\}$ of $F_n \; = < g_1, \cdots , g_n | - >$ up to their membership to F_n may be interpreted as a condition of algebraic independence among them.

Remark 7.2.3

RANDOM WALKS ON FREE GROUPS

Let us consider a drunk living in a D-dimensional space $\mathbb{R}^D$, exiting at time $t \; = \; 0$ from the tavern located in the origin and beginning to walk completelly at random, making at each temporal step $n \in \mathbb{N}$ one step of unit length.

Introduced the unit versors $\vec{v}^{(i)} \; \in \; \mathbb{R}^D \; i = 1, \cdots , D$:

$$\vec{v}^{(i)}_{j} \; := \; \delta_{i,j} \;\; i,j = 1, \cdots , D \tag{7.2.7.21}$$

and the **near-neighbourhood matrix**:

$$J_{\vec{x},\vec{y}} \; := \; \sum_{i=1}^{D} \delta_{\vec{x},\vec{y}+\vec{v}^{(i)}} \tag{7.2.7.22}$$

we have clearly that the probability $P_t(\vec{x})$ that at the temporal step $t \in \mathbb{N}$ he is located in the lattice site $\vec{x} \; \in \; \mathbb{Z}^D$ satisfies the conditions:

$$P_{t}(\vec{x}) \; = \; \frac{1}{2D} \sum_{\vec{y} \in \mathbb{Z}^{D}} J_{\vec{x},\vec{y}} P_{t-1}(\vec{y}) \tag{7.2.7.23}$$

$$P_{0}(\vec{x}) \; = \; \delta_{\vec{x},\vec{0}} \tag{7.2.7.24}$$

Introduced the Fourier-transform of the $P_t(\vec{x})$:

$$P_{t}(\vec{x}) \; = \; \int_{[-\pi,\pi]^{D}} \frac{d\vec{p}}{(2\pi)^{D}} e^{i \vec{p} \cdot \vec{x}} \tilde{P}_{t}(\vec{p}) \tag{7.2.7.25}$$

$$\tilde{P}_{t}(\vec{p}) \; = \; \sum_{\vec{x} \in \mathbb{Z}^{D}} e^{-i \vec{p} \cdot \vec{x}} P_{t}(\vec{x}) \tag{7.2.7.26}$$

eq.7.2.7.23 implies that:

$$\tilde{P}_t(\vec{p}) \;=\; (\frac{1}{D}\sum_{i=1}^{D}\cos(p_i))^t \qquad (7.2.7.27)$$

To analyze the asympotic situation at large distances w.r.t. the lattice spacing and for long times, it is convenient to rescale and times using a lattice spacing a rather then 1 and a time interval τ rather than 1.

After the substitutions:

$$t \;\to\; \frac{t}{\tau} \qquad (7.2.7.28)$$

$$\vec{x} \;\to\; \frac{\vec{x}}{a} \qquad (7.2.7.29)$$

$$\vec{k} \;\to\; a\vec{k} \qquad (7.2.7.30)$$

one obtains that:

$$P_t(\vec{x}) \;=\; a^D \int_{[-\frac{\pi}{a},\frac{\pi}{a}]^D} \frac{d\vec{p}}{(2\pi)^D} e^{i\vec{p}\cdot\vec{x}} (\frac{1}{D}\sum_{i=1}^{D}\cos(a\,p_i))^{\frac{t}{\tau}} \qquad (7.2.7.31)$$

Let us now take the limit as a and τ go to zero keeping the distance and time intervals fixed.

Following , for simplicity, the informal approach of [Dro89a] let us consider a volume $\Delta\vec{x}$ which is large w.r.t. the elementary lattice volume a^D but which is also sufficiently small to ensure that P remain nearly constant within $\Delta\vec{x}$; this last requirement is fulfilled if $\frac{t}{\tau}$ is also large.

This permits to introduce a probability density $p(\vec{x},t)$ defined as:

$$p(\vec{x},t)\Delta\vec{x} \;:=\; \sum_{\vec{x}'\in\vec{x}+\Delta\vec{x}} P(\vec{x}',t) \;\approx\; \frac{\Delta\vec{x}}{a^D}P(\vec{x},t) \qquad (7.2.7.32)$$

so that:

$$p(\vec{x},t) \;=\; \lim_{a,\tau\to 0}\int_{[-\frac{\pi}{a},\frac{\pi}{a}]^D} \frac{d\vec{p}}{(2\pi)^D} e^{i\vec{p}\cdot\vec{x}} (\frac{1}{D}\sum_{i=1}^{D}\cos(a\,p_i))^{\frac{t}{\tau}} \qquad (7.2.7.33)$$

This limit is not trivial only when a and τ vanish in such a way that the ratio $\frac{\tau}{a^2}$ is kept fixed, as shown by the expansion of the cosine:

$$(\frac{1}{D}\sum_{i=1}^{D}\cos(a\,p_i))^{\frac{t}{\tau}} \;=\; (1-\frac{a^2}{2D}\vec{p}^2+o(\frac{1}{a},\frac{1}{\tau}))^{\frac{t}{\tau}} \;\to\; e^{-t\vec{p}^2} \qquad (7.2.7.34)$$

in which the time scale has been fixed using:

$$\tau \;=\; \frac{a^2}{2D} \qquad (7.2.7.35)$$

Hence:

$$p(\vec{x},t) \;=\; \int \frac{d\vec{p}}{(2\pi)^D} \exp[-t\vec{p}^2 + i\vec{x}\cdot\vec{p}] \;=\; \frac{1}{(4\pi t)^{\frac{D}{2}}} \exp(-\frac{\vec{x}^2}{4t}) \qquad (7.2.7.36)$$

Fixed the notation for gaussian distributions in the following way:

DEFINITION 7.2.18

D-DIMENSIONAL GAUSSIAN MEASURE OF MEAN $\vec{m}$ AND COVARIANCE MATRIX $\hat{C}$:

the probability measure on $\mathbb{R}^d$ of halting-set $\mathcal{F}_{Borel}$ with density:

$$gauss(D,\vec{m},\hat{C};\vec{x}) \;:=\; \frac{1}{(2\pi)^{\frac{D}{2}}} \exp[-\frac{1}{2}(\vec{x}-\vec{m}) \cdot \hat{C}^{-1}(\vec{x}-\vec{m})] \qquad (7.2.7.37)$$

we see that the asympotic probability distribution of the drunk's position is $gauss(D,\vec{0},\frac{\hat{I}}{2\sqrt{t}};\vec{x})$.

Up to translation and rescaling the essence of the asymptotic behaviour of the random walk is thus encoded in the following:

DEFINITION 7.2.19

STANDARD GAUSSIAN MEASURE:

the probability measure on $\mathbb{R}$ of halting-set $\mathcal{F}_{Borel}$ with density $gauss_{STANDARD} := g(1,0,1;x)$

i.e. by the sequence $M_n[gauss_{STANDARD}]$ of its moments:

Theorem 7.2.1

GAUSSIAN MOMENTS:

$$M_n[gauss_{STANDARD}] \;:=\; \int_{-\infty}^{+\infty} dx x^n gauss_{STANDARD}(x) \;=\; \begin{cases} (2m-1)!! & \text{if } n = 2m \,,\, m \in \mathbb{N}, \\ 0 & \text{otherwise.} \end{cases} \qquad (7.2.7.38)$$

$M_{2m}[gauss_{STANDARD}]$ has an intuitive combinatorial meaning: it is the **number of pair partitions** of a set of $2m$ elements.

Let us now consider another drunk making a random walk on the free group of rank D $F_D \;=<g_1,\cdots,g_D|->$, starting at time $t \;=\; 0$ from the tavern located in the identity element e, going in one step from g to h g with probability:

$$Prob[g \;\rightarrow\; hg] \;=\; \begin{cases} \frac{1}{2D} & \text{if } h \in \{g_1\,,\,\cdots\,,g_n\,,\,g_1^{-1}\,,\,\cdots\,,\,g_n^{-1}\}, \\ 0 & \text{otherwise.} \end{cases} \qquad (7.2.7.39)$$

Let us now recall that to any discrete group G one can associate the following Hilbert space:

DEFINITION 7.2.20

HILBERT SPACE OF G:
the Hilbert space $(l^2(G)\,,\,<\cdot|\cdot>)$ such that:

- $$l^2(G) \;:=\; \{\xi \,:\, G \to \mathbb{C} \,:\, \sum_{g \in G} |\xi(g)|^2 \;<\; +\infty\} \tag{7.2.7.40}$$

- $$<\xi|\eta> := \sum_{g \in G} \xi(g)\eta^{\star}(g) \;\; \xi, \eta \in l^2(G) \tag{7.2.7.41}$$

Furthermore there exist natural action representations of G on the Hilbert space $l^2(G)$:

DEFINITION 7.2.21

LEFT REGULAR REPRESENTATION OF G ON $l^2(G)$:

$$(L_g\xi)(\eta) \;:=\; \xi(g^{-1}h) \;\; \xi \in l^2(G), g, h \in G \tag{7.2.7.42}$$

DEFINITION 7.2.22

RIGHT REGULAR REPRESENTATION OF G ON $l^2(G)$:

$$(R_g\xi)(\eta) \;:=\; \xi(hg) \;\; \xi \in l^2(G), g, h \in G \tag{7.2.7.43}$$

from which one can define two Von Neumann algebras associated to G:

DEFINITION 7.2.23

(LEFT) GROUP VON NEUMANN ALGEBRA OF G:

$$\mathcal{L}(G) \;:=\; \{L_g\,,\, g \in G\}^{''} \tag{7.2.7.44}$$

DEFINITION 7.2.24

(RIGHT) GROUP VON NEUMANN ALGEBRA OF G:

$$\mathcal{R}(G) \;:=\; \{R_g\,,\, g \in G\}^{''} \tag{7.2.7.45}$$

Introduced the following notation for the Kronecker's deltas on G looking them as function on the second argument:

$$\delta_g(h) \;:=\; \delta_{gh} \;\; g, h \in G \tag{7.2.7.46}$$

it may be proved [Pet00] that the state $\tau \in \mathcal{L}(G)$ defined as:

$$\tau(a) \;:= <a\delta_e\,,\,\delta_e> \;\;\; a \in \mathcal{L}(G) \tag{7.2.7.47}$$

is a faithful, normal tracial state on $\mathcal{L}(G)$.

Returning at last to our drunk random walking on F_D let us introduce the following noncommutative random variables over the noncommutative probability space $(\mathcal{L}(F_D)\,,\,\tau)$:

$$a_i \;:=\; \frac{1}{\sqrt{2}}(L_{g_i} + L_{g_i^{-1}}) \;\; i = 1, \cdots, D \tag{7.2.7.48}$$

and let us observe that, by eq.7.2.7.39, the probability that the drunk is again at the tavern at the temporal step t may be expressed as the following expectation value over the noncommutative probability space:

$$P_t(e) \;=\; E((\sum_{i=1}^{D} a_i)^t) \forall t \in \mathbb{N} \tag{7.2.7.49}$$

whose asympotic behaviour is given by:

$$P_{2t}(e) \;\approx\; \frac{1}{(2\pi)^D} \frac{1}{t+1} \binom{2\,t}{t} \tag{7.2.7.50}$$

So, exactly as the asymptotic return-to-tavern probability for the drunk living in the D-dimensional euclidean space is governed by the gaussian distribution, the asymptotic return-to-tavern probability for the drunk living living in the D-rank free group is ruled by the probability measure on the real line having vanishing odd moments and even moments given by the **Catalan numbers**:

$$C_n \;:=\; \frac{1}{n+1} \binom{2n}{n} \tag{7.2.7.51}$$

namely the **standard semicircle measure**, according to the following:

DEFINITION 7.2.25

SEMICIRCLE MEASURE OF MEAN m AND VARIANCE $\frac{r^2}{4}$:

the probability measure on $\mathbb{R}$ with halting set $\mathcal{F}_{Borel}$ and density:
$sc(m, r; x) \;:=$

$$\begin{cases} \frac{2}{\pi r^2}\sqrt{r^2 - (x-m)^2} & \text{if } m - r \leq x \leq m + r, \\ 0 & \text{otherwise.} \end{cases} \tag{7.2.7.52}$$

DEFINITION 7.2.26

STANDARD SEMICIRCLE MEASURE:

the probability measure on $\mathbb{R}$ with halting set $\mathcal{F}_{Borel}$ and density $sc_{STANDARD} := sc(0, 2; x)$

One has indeed the following:

Theorem 7.2.2

SEMICIRLE MOMENTS:

$$M_n[sc_{STANDARD}] := \int_{-\infty}^{+\infty} dx x^n sc_{STANDARD}(x) = \begin{cases} C_{2\,m} & \text{if } n = 2m \,,\, m \in \mathbb{N}, \\ 0 & \text{otherwise.} \end{cases} \quad (7.2.7.53)$$

The moments of the semicircle distribution, namely the Catalan numbers, have a combinatorial meaning similar to that of the gaussian moments: $M_{2m} = C_{2m}$ is the n**umber of non-crossing pair partitions** of a linearly ordered set of 2m objects (let's say the 2m-letters' alphabet Σ_{2m}), according to the following:

DEFINITION 7.2.27

THE PARTITION $\mathcal{V} := \{V_1, \cdots, V_s\}$ OF Σ_n IS NON-CROSSING:

$$(V_i = \{v_1, \cdots, v_p\} \, and \, V_j = \{w_1, \cdots, w_q\}) \Rightarrow$$
$$(w_m < v_1 < w_{m+1} \Leftrightarrow w_m < v_p < w_{m+1} \; m = 1, \cdots, q-1) \quad (7.2.7.54)$$

Let us now observe that what rules the asympotic behaviour of the drunk living in the D-dimensional euclidean space is the Central Limit Theorem of Classical Probability Theory, stating that the probability distribution:

$$\frac{x_1 + \cdots + x_n}{\sqrt{n}}$$

of a collection of identically distributed, independent random variables tends to the gaussian distribution when $n \to \infty$.

In the same way what rules the asympotic behaviour of the drunk living in the D-ranked free group is a noncommutative central limit theorem stating that the average:

$$\frac{a_1 + \cdots + a_n}{\sqrt{n}}$$

is a noncommutative random variable whose distribution, for $n \to \infty$, tends to the semicircle distribution.

Given a free group $F = < \chi | - >$ and a word W over χ:

DEFINITION 7.2.28

W IS REDUCED:

W doesn't contain peaks

An important problem of free groups is the solvability of their word problem

Theorem 7.2.3

SOLUTION OF THE WORLD PROBLEM OF FREE GROUPS:
each element of F_n is represented by a unique reduced word

Let us consider again the collection of noncommutative random variables $\{a_i\}$ on the noncommutative probability space $(\mathcal{L}(F_n), \tau)$ introduced in the remark7.2.3 on discussing the random walk on F_n and the noncommutative central limit theorem governing its asymptotic behaviour: its a collection of mutually-noncommuting random variables so that, by theorem5.2.4, they are certainly not independent.

Formalizing the kind of algebraic independence of such a collection, inherited from the free structure of F_n, one arrives to the following:

given a noncommutative probability space (A, ω) and a family $\{A_i\}_{i \in I}$ of subalgebras of A:

DEFINITION 7.2.29

THE SUBALGEBRAS $\{A_i\}_{i \in I}$ ARE FREE:

$$\forall n \in \mathbb{N}, \forall i(1), \cdots, i(n) \in I \, : \, i(k) \neq i(k+1) \, (1 \leq k \leq n-1)$$
$$a_k \in A_{i(k)} \, , \, \omega(a_k) = 0 \, 1 \leq k \leq n \, \Rightarrow \omega(a_1 a_2 \cdots a_n) \, = \, 0 \quad (7.2.7.55)$$

Clearly definition7.2.29 is a generalization of the simpler case in which $I = \mathbb{N}$ and each $\{A_i\} = span(\{a_i\})$, in which freeness implies the following useful result:

Theorem 7.2.4

THE VANISHING EXPECTATION VALUE OF A PRODUCT OF CENTERED FREE RANDOM VARIABLES

HP:

$(A \, , \, \omega)$ noncommutative probability space

$\{a_1 \, , \, \cdots \, , \, a_n\}$ n^{th}-ple of free random variables

TH:

$$E(\sum_{i=1}^{n} a_i \, - \, E(a_i)) \, = \, 0$$

PROOF:

The family of subalgebras $\{A_i\}_{i=1}^{n}$ spanned by every $a_i \, i = 1, \cdots n$ may be ordered in a way such that $a_k \in A_{i(k)}$ with $i(k) \neq i(k+1) \, k = 1, \cdots , n-1$.

Furthermore one has clearly that:

$$E(a_i - E(a_i)) \; = \; 0 \;\; i = 1, \cdots , n \tag{7.2.7.56}$$

So the freness condition implies the thesis. ■

We know that the independence of a collection $\{a_1 \, , \cdots , a_n\}$ of random variables on an algebraic probability space $(A \, , \omega)$ may be seen as a rule for deriving the joint-moment $E(\prod_{i=1}^{n} a_i)$ for the collection of expectation values $\{E(a_1) \, , \cdots , E(a_n)\}$ according to:

$$E(\prod_{i=1}^{n} a_i) \; = \; \prod_{i=1}^{n} E(a_i) \tag{7.2.7.57}$$

Also freeness may be seen in this way, but with a different way of computing the joint moments:

Corollary 7.2.1

HP:

$(A \, , \, \omega)$ noncommutative probability space

$\{a_1 \, , \, \cdots \, , \, a_n\}$ n^{th}-ple of free random variables

TH:

$$E(\prod_{i=1}^{n} a_i) \; = \; \sum_{i=1}^{n} \sum_{1 \leq k_1 \leq \cdots \leq k_r \leq n} (-1)^{r+1} E(a_{k_1}) \cdots E(a_{k_r}) E(a_1 \cdots \hat{a}_{k_1} \cdots \hat{a}_{k_r} \cdots a_n)$$

where $\hat{}$ indicates terms that are omitted.

Example 7.2.1

FREENESS VERSUS INDEPENDENCE FOR A COUPLE OF NONCOMMUTATIVE RANDOM VARIABLES

Given two free algebraic random variables $a \, , \, b$ on a noncommutative probability space $(A \, , \omega)$, Corollary7.2.1 implies that:

$$E(a \, b) \; = \; E(a)E(b) \; = \; E(b \, a) \tag{7.2.7.58}$$

exactly as one would have if a and b were independent.

Anyway one has that:

$$E(a\,b\,a\,b) \;=\; E(a^2)E(b)^2 \,+\, E(a)^2E(b^2) \,-\, (E(a))^2(E(b))^2 \qquad (7.2.7.59)$$

and:

$$E(ab^2a) \;=\; E(a^2)E(b^2) \qquad (7.2.7.60)$$

The latter identity shows in particular that free relation precludes commutativity.

Indeed one has that:

Corollary 7.2.2

ON THE VANISHING VARIANCE OF FREE COMMUTING RANDOM VARIABLES:

$$(a, b \text{ free } \; and \; [a\,,\,b] = 0) \;\Rightarrow\; (Var(a) = 0 \; or \; Var(b) = 0) \qquad (7.2.7.61)$$

PROOF:

By Corollary7.2.1 and commutativity one has that:

$$E((a - E(a)I)^2\,(b - E(b)I)^2) \;=\; 0 \qquad (7.2.7.62)$$

from which the thesis immediately follows. ■

Example 7.2.2

THE FREE FLAVOUR OF THE QUBITS' STRINGS' HILBERT SPACE

Fock spaces have a deep connection with freeness we want here to stress, starting from the following:

Theorem 7.2.5

FOCK SPACES AS HILBERT SPACES OF FREE GROUPS

HP:

$$\mathcal{H} \;:\; \text{ Hilbert space } \;:\, dim(\mathcal{H}) = n$$

TH:

$$\mathcal{F}(\mathcal{H}) \; = \; l^2(F_n)$$

that implies, in particular, that the qubit-strings' Hilbert space is nothing but the Hilbert space of the 2-ranked free group:

$$\mathcal{H}_2^{\bigotimes \star} \; = \; l^2(F_2) \tag{7.2.7.63}$$

Let us formalize a bit the analysis of Fock spaces, considering as prototype the qubit-strings' Hilbert space we are mainly interested to.

DEFINITION 7.2.30

VACUUM VECTOR OF $\mathcal{H}_2^{\bigotimes \star}$:
the unit vector $|\Phi>$ such that:

$$\mathcal{H}_2^{\bigotimes 0} \; = \; \mathbb{C}|\Phi> \tag{7.2.7.64}$$

DEFINITION 7.2.31

(QUBITS') NUMBER OPERATOR:
the positive self-adjoint operator $\hat{N}$ on $\mathcal{F}_S(\mathcal{H}_2)$ such that $\mathcal{H}_2^{\bigotimes n}$ is an eigen-subspace corresponding to the eigenvalue n ($n \in \mathbb{Z}^+$).

Given $|\psi> \in \mathcal{H}_2$:

DEFINITION 7.2.32

CREATION OPERATOR W.R.T. $|\psi>$:

$$c^\star(|\psi>)|\eta> := \begin{cases} |\psi> & \text{if } |\eta> = |\Phi> \, , \\ |\psi> \bigotimes |\eta> & \text{if } <\eta|\Phi> = 0. \end{cases} \tag{7.2.7.65}$$

DEFINITION 7.2.33

DISTRUCTION OPERATOR W.R.T. $|\psi>$:
the operator $c(|\psi>)$

Let us now consider the noncommutative probability space $(\mathcal{B}(\mathcal{H}_2^{\bigotimes \star}), \omega(\cdot) := Tr[\rho_{|\Phi><\Phi|} \cdot])$.

One has that:

Theorem 7.2.6

FREENESS OF CREATION AND DISTRUCTION OPERATORS OF A FAMILY OF ORTHOGONAL STATES

HP:

$$\{|h_i> \in \mathcal{H}_2\}_{i \in I} \ : < h_i | h_j > = \ 0 \ \forall i \neq j$$

TH:

$$\{c(|h_i>)^{\star} \, , \, c(|h_i>)\}_{i \in I} \text{ are in free-relation}$$

Remark 7.2.4

UNSOLVABLE WORD PROBLEMS AND FREENESS:

Yet in the middle fifthies W.W. Boone and P.S. Novikov discovered the existence of groups with recursively-unsolvable word-problem.

This happens, for example, for the group $G \ = < \mathcal{X} | \mathcal{R} >$:

$$\mathcal{X} \ := \ \{a, b, d, e, p, q, r, t, k\} \tag{7.2.7.66}$$

$$\begin{gathered} \mathcal{R} \ := \ \{p^{10}a \ = \ ap \, , \, p^{10}b \ = \ bp \, , \, p^{10}c \ = \ cp \, , \, p^{10}d \ = \ dp \, , \, p^{10}e \ = \ ep \\ qa \ = \ aq^{10} \, , \, qb \ = \ bq^{10} \, , \, qc \ = \ cq^{10} \, , \, qd \ = \ dq^{10} \, , \, qe \ = \ eq^{10} \\ ra \ = \ ar \ = \ rb \ = \ br \ = \ rc \ = \ cr \ = \ rd \ = \ dr \ = \ re \ = \ er \\ pacqr \ = \ rpcaq \ = \ p^2adq^2r \ = \ rp^2daq^2 \ = \ p^3bcq^3r \ = \ rp^3cbq^3 \\ p^4bdq^4r \ = \ rp^4dbq^4 \, , \, p^5ceq^5r \ = \ rp^5ecaq^5 \\ p^6deq^6r \ = \ rp^6edbq^6 \, , \, p^7cdcq^7r \ = \ rp^7cdceq^7 \\ p^8caaaq^8r \ = \ rp^8aaaq^8 \, , \, p^9daaaq^9r \ = \ rp^9aaaq^9 \\ pt \ = \ tp \, , \, qt \ = \ tq \, , \, pk \ = \ kp \, , \, qk \ = \ kq \, , \, k(aaa)^{-1}t(aaa) \ = \ (aaa)^{-1}t(aaa)k\} \end{gathered} \tag{7.2.7.67}$$

Considered the noncommutative probability space $(\mathcal{L}(G) \, , \, \tau)$, couldn't the unsolvability of the word problem of G result in the recursive undecidability of freeness for a suitable collection of noncommutative random variables?

Since we have seen that there exist (at least) two possibilities of formulating a quantum analogue of the constraint7.2.1 we will pursue both:

1. insisting in adopting the notion of **independence** also in the quantum case, we arrive at the following:

   CONSTRAINT 7.2.2

   INDEPENDENCE-CONSTRAINT ON THE NOTION OF A RANDOM SEQUENCE ON THE NONCOMMUTATIVE ALPHABET Σ_{NC} :

   Making infinite ***independent*** *trials of the experiment consisting on tossing a* ***quantum coin*** *we must obtain an algorithmically-random sequence of qubits with certainty*

Let us try to formalize this analysis; denoted by $RANDOM(\Sigma_{NC}^{\infty})$ the space of algorithmically-random sequences of qubits, exactly as constraint7.2.1 results in the condition:

$$p_{\text{Chaitin randomness}} \in \mathcal{P}_{C}^{TYPICAL}[(\Sigma^{\infty}, \tau_{unbaised})] \quad (7.2.7.68)$$

where:

$$p_{\text{Chaitin randomness}}(\bar{x}) := << \bar{x} \in RANDOM(\Sigma^{\infty}) >> \quad (7.2.7.69)$$

the constraint7.2.2 results in the condition:

$$p_{\text{noncommutative randomness}} \in \mathcal{P}_{C}^{TYPICAL}[(\Sigma_{NC}^{\infty}, \tau_{unbaised})] \quad (7.2.7.70)$$

where:

$$p_{\text{noncommutative randomness}}(\bar{x}) := << \bar{x} \in RANDOM(\Sigma_{NC}^{\infty}) >> \quad (7.2.7.71)$$

2. assuming that the sequence of quantum coin tosses must be **free** instead of **independent**, one must give up the sequence $\{c_i\}$ replacing it with a sequence $\{\tilde{c}_i\}$ of free random variables.

   The more natural way of doing this is passing through the notion of **free product** of noncommutative probability spaces.

   Given two groups $G_1 := < \chi_1 | \mathcal{R}_1 >$ and $G_2 := < \chi_2 | \mathcal{R}_2 >$:

   DEFINITION 7.2.34

   FREE PRODUCT OF G_1 AND G_2:

$$G_1 * G_2 := \frac{< \chi_1 \bigcup \chi_2 | \mathcal{R}_1 \bigcup \mathcal{R}_2 >}{\mathcal{R}_1 \bigcap \mathcal{R}_2} \quad (7.2.7.72)$$

   Example 7.2.3

   FINITE FREE GROUPS AS FREE PRODUCTS

   The set $\mathbb{Z}$ may be seen as the 1-rank free group:

$$\mathbb{Z} = F_1 = < \Sigma_1 | - > \quad (7.2.7.73)$$

   The higher rank free groups may be obtained simply by free products:

$$F_n = *_{i=1}^{n} \mathbb{Z} \quad (7.2.7.74)$$

   A different equivalent way of characterizing free products is through the so called Universality Property; let us recall that (cfr. the second chapter of [Gri99]) given a group G:

DEFINITION 7.2.35

COMMUTATOR SUBGROUP OF G:

$$[G\,,G] \;:=\; \{[x,y] \;:=\; xyx^{-1}y^{-1}\,,\, x,y \in G\} \qquad (7.2.7.75)$$

Theorem 7.2.7

UNIVERSALITY PROPERTY FOR DIRECTS SUMS OF GROUPS

$$G \;=\; \bigoplus_{i \in I} G_i \;\Leftrightarrow\; \forall \{\varphi_i : G_i \to G\}_{i \in I} \text{ family of homomorphims } \;:\; [\varphi_j(x_j)\,,\,\varphi_k(x_k)] = e\,\forall j \neq k$$
$$\exists ! \varphi \bigoplus_{i \in I} G_i \;\to\; G \;:\; \varphi \circ i_i \;=\; \varphi_i \quad (7.2.7.76)$$

Replacing in theorem7.2.7 the range of the homomorphisms from G to its commutator subgroup G' and removing the commutativity condition, one results in the following:

Theorem 7.2.8

UNIVERSALITY PROPERTY FOR FREE PRODUCTS OF GROUPS:

$$G \;=\; *_{i \in I} G_i \;\Leftrightarrow\; \exists \{i_i : G_i \to G\}_{i \in I} \text{ family of homomorphims } :$$
$$(\forall \{\varphi_i : G_i \to G'\}_{i \in I} \text{ family of homomorphims}$$
$$\exists ! \varphi *_{i \in I} G_i \;\to\; G \;:\; \varphi \circ i_i \;=\; \varphi_i) \quad (7.2.7.77)$$

The free product of algebras may be introduces in a similar way (cfr. the third chapter of [Opr94]):

given a family of algebras $\{A_i\}_{i \in I}$ and an algebra A

DEFINITION 7.2.36

A IS THE FREE PRODUCT OF $\{A_i\}_{i \in I}$ ($A \;:=\; *_{i \in I}\{A_i\}$):

$$\exists \{i_i : A_i \to A\}_{i \in I} \text{ family of homomorphims with } i_i(I) = I :$$
$$\forall B\, algebra\,,\, \forall \{\varphi_i : A_i \to B\}_{i \in I} \text{ family of homomorphims: } f_i(I) = I$$
$$\exists ! h : A \mapsto B \; homomorphism \;:\; h \circ i_i \;=\; f_i \quad (7.2.7.78)$$

Definition7.2.36 constructs the free product in the category of algebras.

The definition of free product in the category of Von Neumann algebras requires the free product of algebra must be endowed of a rule concerning involution and a norm. Furthermore a completion procedure must be carried off.

While the rule concerning involution will be explicitly specified in the through the theorem we are going to introduce , we won't discuss the other sophisticated technicalities concerning the norm and the completion, demanding the interested reader to the section7.1 of [Pet00].

Let us consider two algebraic probability spaces (A_1 , φ_1) and (A_2 , φ_2). Decomposed A_i as $A_i = \mathbb{C}I \bigoplus A_i^0$, where:

$$A_i^0 := \{a_i \in A_i : \varphi_i(a) = 0\} \tag{7.2.7.79}$$

it may be proved that:

Theorem 7.2.9

DIRECT SUM EXPANSION OF THE FREE PRODUCT ALGEBRA:

$$\begin{gathered} A_1 * A_2 = \mathbb{C}I \oplus \bigoplus\{A_{i(1)}^0 \bigotimes A_{i(2)}^0 \bigotimes \cdots \bigotimes A_{i(n)}^0 : \\ i(k) \in \{1,2\}, 1 \leq k \leq n\, , i(k) \neq i(k+1) 1 \leq k \leq n-1\, , n \in \mathbb{N}\} = \\ = \mathbb{C}I \bigoplus A_1^0 \bigoplus A_2^0 \bigoplus (A_1^0 \bigotimes A_2^0) \\ \bigoplus (A_2^0 \bigotimes A_1^0) \bigoplus (A_1^0 \bigotimes A_2^0 \bigotimes A_1^0) \bigotimes (A_2^0 \bigotimes A_1^0 \bigotimes A_2^0) \bigotimes \\ \bigotimes (A_1^0 \bigotimes A_2^0 \bigotimes A_1^0 \bigotimes A_2^0) \\ \bigoplus (A_2^0 \bigotimes A_1^0 \bigotimes A_2^0 \bigotimes A_1^0) \bigoplus \cdots \end{gathered} \tag{7.2.7.80}$$

Let us explicitly analyze the products' structure of $A_1 * A_2$:

if $a_i \in A_i^0$ $i \in \{1,2\}$, then their product $a_1 \cdot a_2$ is $a_1 \bigotimes a_2 \in A_1^0 \bigotimes A_2^0$.

More generally:

$$\begin{gathered} (x = \bigotimes_{k=1}^{n} a_k\, , a_k \in A_{i(k)}^0\, , i(k) \in \{1,2\}, 1 \leq k \leq n) \; and \; (y = \bigotimes_{l=1}^{m} b_l \\ b_l \in A_{j(l)}^0\, , j(l) \in \{1,2\}, 1 \leq l \leq m) \; and \\ (i(n) \neq j(1)) \Rightarrow x \cdot y = \bigotimes_{k=1}^{n} a_k \bigotimes \bigotimes_{l=1}^{m} b_l \end{gathered} \tag{7.2.7.81}$$

If $i(n) = j(1)$, anyway, $x \cdot y$ can't be obtained simply concatenating the two tensor products, since, in this case it is not true, in general, that $a_n b_1 \in A_{i(n)}^0$; precisely, decomposed $a_n b_1$ as:

$$a_n b_1 = \lambda I + a \quad a \in A_{i(n)}^0 \tag{7.2.7.82}$$

one has that:

$$x \cdot y = \bigotimes_{k=1}^{n-1} a_k \bigotimes a \bigotimes_{l=2}^{m} b_l + \lambda \bigotimes_{k=1}^{n-1} a_k \bigotimes_{l=2}^{m} b_l \tag{7.2.7.83}$$

The promised definition of the involution in the $W^{\star}$-algebra $A_1 * A_2$ is straightforward:

$$x^{\star} = \bigotimes_{k=1}^{n} a_{n-k} \tag{7.2.7.84}$$

Example 7.2.4

FREE PRODUCT OF GROUPS VON NEUMANN ALGEBRAS

Given two discrete groups G_1 and G_2 the left (right) group Von Neumann algebra w.r.t. their free product is equal to the free product of their left (right) group Von Neumann algebras, i.e.:

$$\mathcal{L}(G_1 * G_2) = \mathcal{L}(G_1) * \mathcal{L}(G_2) \tag{7.2.7.85}$$

$$\mathcal{R}(G_1 * G_2) = \mathcal{R}(G_1) * \mathcal{R}(G_2) \tag{7.2.7.86}$$

Let us now introduce the following:

DEFINITION 7.2.37

FREE PRODUCT OF THE ALGEBRAIC PROBABILITY SPACES (A_1 , φ_1) AND (A_2 , φ_2):

$$(A_1 , \varphi_1) * (A_2 , \varphi_2) := (A_1 * A_2 , \varphi) \tag{7.2.7.87}$$

with:

$$\varphi(\lambda I + \sum \bigotimes_{k=1}^{n} a_k) := \lambda \tag{7.2.7.88}$$

The free product $*_{i \in I}(A_i , \varphi_i)$ of an arbitrary collection $\{(A_i , \varphi_i)\}$ of algebraic probability spaces may then be easily obtained by definition7.2.37 by iteration.

Each A_i is embedded in $*_{i \in I} A_i$ by the following:

DEFINITION 7.2.38

CANONICAL EMBEDDING of A_i IN $*_{i \in I} A_i$:

the map $i_i : A_i \mapsto *_{i \in I} A_i$:

$$i_i(a_i) := \varphi_i(a_i) I \bigoplus (a_i - \varphi_i(a_i) I) \tag{7.2.7.89}$$

Exactly as the notion of independence of classical random variables may be based on the notion of product of classical probability spaces, the notion of freeness of algebraic random variable may be based on the notion of free product of noncommutative probability spaces through the following:

Theorem 7.2.10

FREENESS THROUGH FREE PRODUCT OF ALGEBRAIC PROBABILITY SPACES:

HP:

$$(A \, , \, \varphi) \text{ noncommutative probability space}$$

$$\{A_i\}_{i \in I} \text{ family of subalgebras of A}$$

$$(B \, , \, \omega) \; := \; *_{i \in I}(A_i \, \varphi_{| \, A_i})$$

TH:

$$\{A_i\}_{i \in I} \text{ are free } \Leftrightarrow \varphi(\prod_{k=1}^{n} a_k) \; =$$

$$\omega(\prod_{k=1}^{n} i_{i(k)}(a_k)) \;\; a_k \in A_{i(k)} \, , \, i(k) \in I \, , \, i(k) \neq i(k+1) \, , \, 1 \leq k \leq n-1 \, , \, n \in \mathbb{N}$$

Let us now repeat the construction of remark5.1.7 using free products instead of tensor products:

so, given the one dimensional lattice $\mathbb{Z}$, let us attach to the n^{th} lattice site the one-qubit $W^{\star}$-algebra:

$$A_n \; := \; M_2(\mathbb{C}) \, n \in \mathbb{Z} \tag{7.2.7.90}$$

Given an arbitary set of sites $\Lambda \subseteq \mathbb{Z}$, let us define:

$$(A_{\Lambda}^{free} \, , \, \tau_{\Lambda}^{free}) \; := \; *_{n \in \Lambda}(A_n \, , \, \tau_2) \tag{7.2.7.91}$$

Let us then introduce the following $W^{\star}$-algebra:

$$R_{free} \; := \; \pi_{\tau_{\mathbb{Z}}}(A_{\mathbb{Z}}^{free})'' \tag{7.2.7.92}$$

We can now try to implement mathematically the following:

CONSTRAINT 7.2.3

FREENESS-CONSTRAINT ON THE NOTION OF A RANDOM SEQUENCE ON THE NONCOMMUTATIVE ALPHABET Σ_{NC} :

Making infinite ***free*** *trials of the experiment consisting on tossing a* ***quantum coin*** *we must obtain an algorithmically-random sequence of qubits with certainty*

The quantum coin tossing at time $n \in \mathbb{N}$ will be then represented by a noncommutative random variable $\tilde{c}_n \in A_n^{free}$ such that $\{\tilde{c}_n\}$ is a free sequence or, more precisely, by the associated free sequence obtained in the passage to R_{free}.

The mathematical implementation of constraint7.2.3 is, anyway, affected by the following two issues:

1. it would be natural, at this, point, to think that constraint7.2.3 is translated mathematically by the statement:

$$P_{unbaised}[RANDOM(R_{free})] \; = \; 1 \qquad (7.2.7.93)$$

   Anyway it must be observed that:

   (a) since:

$$Type[R_{free}] \; = \; III \qquad (7.2.7.94)$$

   the unbiased noncommutative probability distribution doesn't exist

   (b) also supposed to bypass such a problem, translating mathematically the constraint7.2.3 by a suitable statement:

$$F[RANDOM(R_{free})] \; = \; 0 \qquad (7.2.7.95)$$

   it is not clear how to express it in terms of Σ_{NC}^{∞}

   A possible way to overcome the first problem may consist in passing from the family of noncommutative random variables $\{\bar{c}_n\}$ to the family of noncommutative random variables $\{av_n\}$ defined as:

$$av_n \; := \; \frac{1}{\sqrt{n}} \sum_{i=1}^{n} \tilde{c}_i \qquad (7.2.7.96)$$

   and investigating the typical properties of the sequence $\{av_n\}$ w.r.t. the central limit distribution.

   This immediately leads to analyze the relationship between the probabilistic-quantum-information and alghorithmic-quantum-information, as we will discuss in the next section.

Remark 7.2.5

ABOUT ALGORITHMICALLY-RANDOM MATRICES:

Most of the success of Voiculescu's Free Probability Theory and the interest about it shown by theoretical physicists is owed to the fact that random matrices of the most commom ensembles (cfr.[Pas00] or the section 10.3 of [Dro89b] for a review), are asymptotically free.

Given a classical probability space $CPS := (X , P)$:

DEFINITION 7.2.39

ENSEMBLE W.R.T. CPS OF ORDER n:

the noncommutative probability space:

$$ENSEMBLE[CPS , n] := (RANDOM - MATRICES[CPS , n] , e\tau_n) \tag{7.2.7.97}$$

where:

$$RANDOM - MATRICES[CPS , N] := \{a \in M_n(\mathbb{C}) : M_k(a_{i,j}) \in \bigcap_{1 \leq p \leq \infty} L^p(X,P)\} \tag{7.2.7.98}$$

$$e\tau_n(a) := E(\tau_n(a)) = \frac{1}{n} \sum_{i=1}^{n} E(a_{i,i}) \tag{7.2.7.99}$$

DEFINITION 7.2.40

EMPIRICAL EIGENVALUE DISTRIBUTION OF THE RANDOM MATRIX $a \in ENSEMBLE[CPS , n]$:

the random atomic measure:

$$\mu_{emp}(a) := \frac{1}{n} \sum_{i=1}^{n} \delta(\lambda_i(a)) \tag{7.2.7.100}$$

where $\lambda_1(a) , \cdots , \lambda_n(a)$ are the eigenvalues of a.

DEFINITION 7.2.41

MEAN EIGENVALUE DISTRIBUTION OF THE RANDOM MATRIX $a \in ENSEMBLE[CPS , n]$:

$$\mu_{mean}(a) := E(\mu_{emp}(a)) \tag{7.2.7.101}$$

Example 7.2.5

THE GAUSSIAN ORTHOGONAL ENSEMBLE (GOE) AND THE GAUSSIAN UNITARY ENSEMBLE (GUE)

Let us consider the random matrices' ensemble describing a random $n\times$ real-entries symmetric matrix a such that $\{a_{i,j} : 1 \leq i \leq j \leq n\}$ is a family of independent real Gaussian random variables such that:

$$E(a_{ij}) = 0 \tag{7.2.7.102}$$

$$E(a_{ij}^2) = \frac{1+\delta_{ij}}{n+1} \tag{7.2.7.103}$$

The variance has been chosen so that:

$$e\tau_n(a^2) = 1 \tag{7.2.7.104}$$

Such an ensemble is usually called the **n-order gaussian orthogonal ensemble (n-GOE)** , the name being owed to the orthogonal invariance of the underlying classical probability measure.

Another very important random matrices' ensemble is that describing a random $n\times$ complex self-adjoint matrix a such that:

1. $\{Re(a_{i,j}) : 1 \leq i \leq j \leq n\} \bigcup \{Im(a_{i,j}) : 1 \leq i \leq j \leq n\}$ is an independent family of Gaussian random variables

2.
$$E(a_{ij}) = 0 \;\; 1 \leq i \leq j \leq n \tag{7.2.7.105}$$
$$E(a_{ii}^2) = \frac{1}{n} \;\; 1 \leq i \leq n \tag{7.2.7.106}$$
$$E((\Re(a_{ij})^2)) = E((\Im(a_{ij})^2)) = \frac{1}{2n} \;\; 1 \leq i \leq j \leq n \tag{7.2.7.107}$$

   where the normalization has been chosen again in order that:

$$e\tau_n(a^2) = 1 \tag{7.2.7.108}$$

Such an ensemble is usually called the **n-order gaussian unitary ensemble (n-GUE)**, the name being owed to the unitary invariance of the underlying classical probability measure.

Let us now consider a sequence $\{(A_n , \omega_n)\}_{n\in\mathbb{N}}$ of noncommutative probability spaces and a sequence $\{a_1^{(n)} , \cdots , a_k^{(n)}\}_{n\in\mathbb{N}}$ of k^{ples} of noncommutative random variables over the $\{(A_n , \omega_n)\}_{n\in\mathbb{N}}$'s.

DEFINITION 7.2.42

THE NONCOMMUTATIVE RANDOM VARIABLES $\{a_1^{(n)} , \cdots , a_k^{(n)}\}_{n\in\mathbb{N}}$ ARE ASYMPTOTICALLY FREE:

$$E(\prod_{i=1}^{k} a_i^{(n)}) = \sum_{i=1}^{k} \sum_{1\leq k_1 \leq \cdots \leq k_r \leq k} (-1)^{r+1} E(a_{k_1}^{(n)}) \cdots E(a_{k_r}^{(n)}) E(a_1^{(n)} \cdots \hat{a}_{k_1}^{(n)} \cdots \hat{a}_{k_r}^{(n)} \cdots a_k^{(n)}) + O(\frac{1}{n}) \tag{7.2.7.109}$$

where ˆ indicates again terms that are omitted.

It may be proved that [Pet00]:

Theorem 7.2.11

ASYMPTOTIC FREENESS OF INDEPENDENT GOE'S RANDOM MATRICES

HP:

$$a_1^{(n)}, \cdots, a_n^{(n)} \text{ independent n-GOE's random matrices}$$

TH:

$$a_1^{(n)}, \cdots, a_n^{(n)} \text{ are asymptotically free}$$

Theorem7.2.11 gives a noncommutative-probabilistic foundation to the following celebrated:

Corollary 7.2.3

WIGNER'S THEOREM:

HP:

$$a^{(n)} \in n - GOE$$

TH:

$$d - \lim_{n \to \infty} \mu_{mean}(a^{(n)}) = sc_{STANDARD}$$

PROOF:

Given $b_1^{(n)}, \cdots, b_n^{(n)}$ independent n-GOE's random matrices one has that the distribution of the random matrix:

$$\frac{\sum_{k=1}^{n} b_k^{(n)}}{\sqrt{n}}$$

is the same as that of $a^{(n)}$.

The thesis immediately follows from theorem7.2.11 and theorem7.3.2 ■

7.3 From the communicational-compression of the Quantum Coding Theorems to the algorithmic-compression in Quantum Computation

Among the many successes of Quantum Information Theory must be certainly acknoledged the Quantum Coding Theorems, i.e. the Schumacher's Theorem ruling the upper bound for the compression of quantum information in a noiseless quantum-channel, and the Holevo-Schumacher-Westmoreland Theorem ruling the upper bound for the capacity of noisy quantum-channels used to transmit classical information [Win99], [Chu00], [Wer01].

As we will show, from a structural point of view Coding Theorems, both classical and quantum, are an application of **Algebraic Large Deviations' Theory**, a noncommutative generalization of **Classical Large Devations's Theory** [Var84], [Zei98].

Let us begin to introduce the necessary stuff starting from the Central Limit Theorems we informally introduced in the remark7.2.3.

Theorem 7.3.1

INDEPENDENCE'S CENTRAL LIMIT THEOREM:
HP:

$$(A\,,\,\omega) \text{ algebraic probability space}$$

$$\{a_n\}_{n \in \mathbb{N}_+} \text{ sequence of } \textbf{independent} \text{ algebraic random variables on } (A\,,\omega)$$

$$E(a_i) \;=\; 0\;,\; Var(a_i) \;=\; 1 \;\; i \in \mathbb{N}_+$$

$$M_k(a_i) \;<\; +\infty \;\; \forall i, k \in \mathbb{N}_+$$

TH:

$$d - \lim_{n \to \infty} \frac{1}{\sqrt{n}} \sum_{i=1}^{n} a_i \;=\; gauss_{STANDARD}$$

where $d - \lim$ denotes convergence in distribution.

Theorem 7.3.2

FRENESS' CENTRAL LIMIT THEOREM:
HP:

$$(A\,,\,\omega) \text{ algebraic probability space}$$

$$\{a_n\}_{n\in\mathbb{N}_+} \text{ sequence of } \textbf{free} \text{ algebraic random variables on } (A\,,\omega)$$

$$E(a_i) \;=\; 0\;,\; Var(a_i) \;=\; 1 \;\; i \in \mathbb{N}_+$$

$$M_k(a_i) \;<\; +\infty \;\; \forall i, k \in \mathbb{N}_+$$

TH:

$$d - \lim_{n\to\infty} \frac{1}{\sqrt{n}} \sum_{i=1}^{n} a_i \;=\; sc_{STANDARD}$$

Remark 7.3.1

THE EXPONENTIAL DECAY OF THE DEVIATION FROM THE CENTRAL LIMIT

We have seen in chapter3 that the Law of Randomness $p_{\text{Borel normality of order 1}}$ stating the Law of Large Numbers is not the whole story.

Also the way in which such an asymptotic behaviour is reached, as ruled by suitable Laws of Randomness, such as $p_{\text{iterated logarithm}}$ or $p_{\text{infinite recurrence}}$, is essential to the Foundation of Probability Theory in the sense of remark3.3.1.

This situation has an immediate translation in terms of the convergence in distribution of the averages $\frac{1}{\sqrt{n}}\sum_{i=1}^{n} a_i$: not only the asymptotic behaviour, as stated by the Central Limit Theorems, is important, but also the way such asymptotic distribution is reached.

It is here where the Large Deviation Principle appears:

informally speaking, if it does exist a two-argument functional $R(d_A, d_B)$ over the probability distributions, said a **rate functional**, such that the probability that the distribution d_n of the average $\frac{1}{\sqrt{n}}\sum_{i=1}^{n} a_i$ deviates from its central limit $d_{\text{central limit}}$ decays exponentially as:

$$Probability[d_n \text{deviates from } d_{\text{central limit}}] \;\sim\; \exp[-n\, R(d_n, d_{\text{central limit}})] \tag{7.3.7.1}$$

then we will say that the convergence to the central limit obeys the Large Deviation Principle w.r.t. the rate functional R.

In such situation a Probabilistic-information Coding Theorem naturally occurs, since realizing a transmission coding neglecting the exponentially improbable messages one obtains a trasmissional compression of information with asymptotically vanishing probability of error.

The maximum possible compression is ruled by the rate functional R

Let us now formalize these considerations starting from the classical case [Zei98].

Given a topological space X:

DEFINITION 7.3.1

RATE FUNCTION OVER X:

a map $I \in MAP[X \, , \, [0, \infty)]$:

$$\{x \in X \, : \, I(x) \leq \alpha\} \text{ is closed } \; \forall \alpha \in [0, \infty) \tag{7.3.7.2}$$

Let us now consider a family of probability measures $\{\mu_{\epsilon}\}$ over X having all the same halting set:

$$HALTING(\mu_{\epsilon}) \; = \; \mathcal{B} \tag{7.3.7.3}$$

where $\mathcal{B}$ is a certain σ-algebra over X, not necessary equal to the Borel-σ-algebra of X.

We will say that:

DEFINITION 7.3.2

$\{\mu_{\epsilon}\}$ SATISFIES THE LARGE DEVIATION PRINCIPLE WITH RATE FUNCTION I:

$$- \inf_{x \in \Gamma^0} I(x) \; \leq \; \liminf_{\epsilon \rightarrow 0} \epsilon \log \mu_{\epsilon}(\Gamma) \; \leq \; \limsup_{\epsilon \rightarrow 0} \epsilon \log \mu_{\epsilon}(\Gamma) \; \leq \; - \inf_{x \in \bar{\Gamma}} I(x) \;\; \forall \Gamma \in \mathcal{B} \tag{7.3.7.4}$$

where Γ^0 denotes the interior of Γ while $\bar{\Gamma}$ denotes the closure of Γ.

Denoted by P_{μ} the probability law μ^{∞} on Σ^{∞} associated to a sequence of independent, identically distributed random variables distributed following $\mu \in \mathcal{D}(\Sigma)$, let us now introduce the following notions:

DEFINITION 7.3.3

TYPE OF $\vec{x} \in \Sigma^{n}$:

the probability measure $L_{n}^{\vec{x}} \in \mathcal{D}(\Sigma)$:

$$L_{n}^{\vec{x}}(i) \; = \; \frac{N_{i}(\vec{x})}{n} \tag{7.3.7.5}$$

We will denote the set of all possible types of strings of length n by $\mathcal{L}_{n}$, i.e.:

$$\mathcal{L}_{n} \; := \; \{L_{n}^{\vec{x}} \, , \, \vec{x} \in \Sigma^{n}\} \tag{7.3.7.6}$$

Let us then denote by $L_{n}^{\vec{X}}$ the random element of $\mathcal{L}_{n}$ associated with the random string $\vec{X}$.

Then:

Theorem 7.3.3

SANOV'S THEOREM:

The family of laws $P_{\mu}(L_n^{\vec{Y}} \in \cdot)$ satisfies the Large Deviation Principle with rate function $S_{Kullback-Leibler}(\cdot|\mu)$

where:

DEFINITION 7.3.4

KULLBACK-LEIBLER RELATIVE ENTROPY OF μ WITH RESPECT TO ν:

$$S_{Kullback-Leibler}(\mu, \nu) := \begin{cases} \int_X d\mu(x) & \log \frac{d\mu(x)}{d\nu(x)} \text{if } \mu \prec \nu, \\ +\infty & \text{otherwise.} \end{cases} \tag{7.3.7.7}$$

$\prec$ being the **absolute continuity** partial-ordering relation among classical measures.

Theorem7.3.3 lies at the heart of the proof of theorem1.3.6.

To show it let us observe that:

1. Shannon's entropy of definition1.3.7 may be considered as a derived quantity arising from the Kullback-Leibler relative entropy of definition7.3.4, as is stated by the commutative case of a general procedure of Algebraic Probability Theory by which probabilistic-information may be derived from the notion of relative probabilistic-information,i.e. relative entropy (cfr. the paper "*From relative entropy to entropy*" at pagg.149-158 of [Thi98] and the homonymous sixth chapter of [Pet93]):

   given a $W^{\star}$-algebra A acting on an Hilbert space $\mathcal{H}$:

   DEFINITION 7.3.5

   ARAKI'S RELATIVE ENTROPY OF $\omega_1 \in S(A)$ W.R.T. $\omega_2 \in S(A)$:

   $$S_{Araki}(\omega_1 \, , \, \omega_2) := \begin{cases} -(\log \Delta(\phi, & \omega'_{|\psi>})|\psi>, |\psi>) \text{if } |\psi> \in supp(\phi), \\ +\infty & \text{otherwise.} \end{cases} \tag{7.3.7.8}$$

   where $|\psi> \in \mathcal{H}$ is an (arbitrary) auxiliary vector and $\omega'_{|\psi>} \in S(A')$ is the state on the commutant A' of A induced by the state $\omega_{|\psi>} \in S(A)$ associated to $|\psi>$.

   One has that:

   Theorem 7.3.4

   ARAKI'S RELATIVE ENTROPY IS A NONCOMMUTATIVE GENERALIZATION OF KULLBACK-LEIBLER RELATIVE ENTROPY:

   HP:

μ, ν probability measures on X: $HALTING(\mu) \,=\, HALTING(\nu)$

TH:

$$S_{Araki}(\omega_{\mu} \, , \, \omega_{\nu}) \;=\; S_{Kullback-Leibler}(\mu, \nu)$$

Definition7.3.5 may sound rather exotic; if ω_1 and ω_2 are normal states, anyway, it reduced to the more used Umegaki's expression:

Theorem 7.3.5

ON UMEGAKI'S RELATIVE ENTROPY:

$$\omega, \varphi \in S_n(A) \;\Rightarrow$$
$$S_{Araki}(\omega_1, \omega_2) \;=\; S_{Umegaki}(\rho_{\omega}, \varphi_{\phi}) \;=\; Tr[\rho_{\omega}(\log_2 \rho_{\omega} \,-\, \log_2 \rho_{\phi})]$$

$$S_{Umegaki}(\rho_{\omega}, \rho_{\varphi}) \;:=\; \begin{cases} Tr[\rho_{\omega}(\log_2 \rho_{\omega} \,-\, \log_2 \rho_{\varphi})] & \text{if } supp(\rho_{\omega}) \leq supp(\rho_{\varphi}) \;, \\ +\infty & \text{otherwise.} \end{cases}$$

One of the most important tools in Quantum Information Theory is the following:

Theorem 7.3.6

SECOND UHLMANN'S THEOREM (MONOTONICITY'S THEOREM FOR RELATIVE ENTROPY)

HP:

$$A \, , \, B \;\; W^{\star} - algebras$$

$$\alpha \in CPU(A, B)$$

TH:

$$S_{Araki}(\omega_1 \circ \alpha, \omega_2 \circ \alpha) \;\leq\; S_{Araki}(\omega_1, \omega_2) \;\; \forall \omega_1, \omega_2 \in S(A)$$

Another important property of Araki's relative entropy is the following:

Theorem 7.3.7

POSITIVITY OF ARAKI'S RELATIVE ENTROPY:

(a)

$$S_{Araki}(\omega_1, \omega_2) \;\geq\; 0 \;\; \forall \omega_1, \omega_2 \in S_n(A) \tag{7.3.7.9}$$

(b)

$$(\, S_{Araki}(\omega_1, \omega_2) \;=\; 0 \;\Leftrightarrow\; \omega_1 \;=\; \omega_2 \,) \;\; \forall \omega_1, \omega_2 \in S_n(A) \tag{7.3.7.10}$$

Remark 7.3.2

THE LINK BETWEEN QUANTUM PROBABILISTIC INFORMATION AND QUANTUM ALGORITHMIC INFORMATION

The **probabilistic approach** and the **algorithmic approach** to Information Theory, trying to focalize the same object from different point of views, are strictly linked.

As to the cell $C_M - C_\Phi$ of the diagram1.1.1 such a link is explicitly formalized by theorem1.3.7.

It is very natural to suppose that an analogous situation occurs as to the cell $NC_M - NC_\Phi$, in particular when the underlying physical theory is Quantum Physics, so that NC_Φ may be read not only as **physically not-classical**, but, equivalently, as **physically not-commutative**.

It must be then possible to use such a link to sharp the concept and properties of quantum algorithmic information.

DEFINITION 7.3.6

DECOMPOSITIONS OF $\omega \in S(A)$:

$$DEC(\omega) \;:=\; \{\{(\lambda_i, \omega_i)\}_{i=1}^{n} \;:\; \lambda_i \in [0,1]\,,\, ,\omega_i \in S(A)\,,\, i = 1, \cdots, n \;: \sum_{i=1}^{n} \lambda_i = 1\,,\, n \in \mathbb{N}\} \tag{7.3.7.11}$$

DEFINITION 7.3.7

EXTREMAL DECOMPOSITIONS $\omega \in S(A)$:

$$DEC_{EXT}(\omega) \; := \; \{\{(\lambda_i,\omega_i)\} \in DEC(\omega) \, : \, \omega_i \in \Xi(A) \, \forall i\} \tag{7.3.7.12}$$

DEFINITION 7.3.8

ORTHOGONAL DECOMPOSITIONS OF $\omega \in S(A)$:

$$DEC_{\perp}(\omega) \; := \; \{\{(\lambda_i,\omega_i)\} \in DEC(\omega) \, : \, supp(\omega_i) \; \perp \; supp(\omega_j) \;\; \forall i \neq j\} \tag{7.3.7.13}$$

Example 7.3.1

SCHATTEN DECOMPOSITIONS:

Given the density operator $\rho_{\omega} \in \mathcal{D}(\mathcal{H})$ of a normal state $\omega \in S_n(A)$ on a Von Neumann algebra $A \subseteq \mathcal{B}(\mathcal{H})$ acting on a separable Hilbert space $\mathcal{H}$, let us consider the sequence $1 \, \leq \, \rho_1 \, \leq \, \rho_2 \, \leq \, \cdots \, \leq \, 0$ of its eigenvalues, repeated according to their multiplicity , let us introduce the following:

DEFINITION 7.3.9

SCHATTEN DECOMPOSITIONS OF ω:

$$DEC_{Schatten}(\omega) \; := \; \{\mathcal{E} = \{\rho_i \, , \, |e_i><e_i|\} \; \in \; DEC_{\perp}(\omega) \bigcap DEC_{EXT}(\omega) \; : \\ \{|e_i>\} \text{ is an orthogonal basis of eigenvectors of } \rho_{\omega}\} \tag{7.3.7.14}$$

DEFINITION 7.3.10

ENTROPY OF $\omega \in S(A)$:

$$S(\omega) \; := \; \sup\{\sum_i \lambda_i S(\omega_i,\omega) \, : \, \{(\lambda_i,\omega_i)\} \; \in \; DEC(A)\} \tag{7.3.7.15}$$

One has that:

Theorem 7.3.8

INVARIANCE OF A STATE'S ENTROPY UNDER INNER AUTOMORPHISMS:

$$S(\alpha_{\star}(\omega)) \; = \; S(\omega) \;\; \forall \alpha \in INN(A) \, , \forall \omega \in S(A) \tag{7.3.7.16}$$

Theorem 7.3.9

NOT-MONOTONICITY OF A STATE'S ENTROPY UNDER CHANNELS:

(a)

$$\alpha \in CPU(A) \, , \, \omega \in S(A) \; \not\Rightarrow \; S(\alpha_{\star}(\omega)) \; = \; S(\omega) \tag{7.3.7.17}$$

(b)

$$\alpha \in CPU(A) \, , \, \omega \in S(A) \; \not\Rightarrow \; S(\alpha_{\star}(\omega)) \; > \; S(\omega) \tag{7.3.7.18}$$

(c)

$$\alpha \in CPU(A) \, , \, \omega \in S(A) \; \not\Rightarrow \; S(\alpha_{\star}(\omega)) \; < \; S(\omega) \tag{7.3.7.19}$$

Theorem7.3.7 immediately implies the following:

Theorem 7.3.10

POSITIVITY OF A STATE'S ENTROPY:

(a)

$$S(\omega) \; \geq \; 0 \;\; \forall \omega \in S(A) \tag{7.3.7.20}$$

(b)

$$S(\omega) \; = \; 0 \Leftrightarrow \omega \in \Xi(A) \tag{7.3.7.21}$$

Another important property of the entropy functional is the following:

Theorem 7.3.11

CONCAVITY OF THE ENTROPY FUNCTIONAL:

$$S(\sum_{i=1}^{n} \lambda_i \omega_i) \; \geq \; \sum_{i=1}^{n} \lambda_i S(\omega_i) \;\; \forall \{ (\lambda_i \, , \, \omega_i) \}_{i=1}^{n} \in DEC(\omega) \tag{7.3.7.22}$$

One has furthermore that:

Theorem 7.3.12

THE ENTROPY OF A STATE IS A NONCOMMUTATIVE GENERALIZATION OF SHANNON'S ENTROPY:

HP:

μ probability measure on X

TH:

$$S(\omega_{\mu}) \ = \ H_{Shannon}(\mu)$$

Theorem 7.3.13

ON VON NEUMANN'S ENTROPY:

$\omega \in S_n(A) \ \Rightarrow$

$$S(\omega) \ = \ S_{Von\ Neumann}(\rho_{\omega}) \ := \ -Tr(\rho_{\omega} \log_2 \rho_{\omega})$$

In 1956 E.T. Jaynes proved what in our algebraic setting may be stated as the following: [Pet01]:

Theorem 7.3.14

JAYNES' THEOREM:

HP:

$$\omega \in S_n(A)$$

TH:

$$\mathcal{E} \text{ is optimal } \quad \forall \mathcal{E} \in DEC_{Schatten}(\omega)$$

that immediately implies that:

Corollary 7.3.1

VON NEUMANN'S ENTROPY AS THE SHANNON'S ENTROPY OF THE EIGENVALUES

HP:

$$\omega \in S_n(A)$$

TH:

$$S(\omega) \ = \ H(\{\rho_i\})$$

Remark 7.3.3

FROM THE VARIATIONAL PRINCIPLE OF MINIMUM FREE ENERGY TO THE VARIATIONAL PRINCIPLE OF MAXIMUM ENTROPY

Having at last introduced Von Neumann's entropy we can discuss some conseguences of theorem7.3.7. Given a closed quantum dynamical system with observables' algebra the space $\mathcal{B}(\mathcal{H})$ of all bounded operators over an Hilbert space $\mathcal{H}$ such that:

$$cardinality_{NC}(\mathcal{B}(\mathcal{H})) \ < \ \aleph_0 \tag{7.3.7.23}$$

and dynamics described by the strongly-continuous one-parameter family of $\mathcal{B}(\mathcal{H})$'s inner automorphisms generated by the hamiltonian $h \in (\mathcal{B}(\mathcal{H}))_{sa}$, let us introduce the following notions:

DEFINITION 7.3.11

CANONICAL STATE W.R.T. h AND $\beta \in [0\,,\,\infty]$:

$$\omega_{h,\beta}^{(CAN)} \ \in \ S(\mathcal{B}(\mathcal{H}))$$

$$\omega_{h,\beta}^{(CAN)}(a) \ := \ \frac{e^{-\beta\, h}\, a}{Tre^{-\beta\, h}}$$

DEFINITION 7.3.12

FREE ENERGY OF $\omega \in S(\mathcal{B}(\mathcal{H}))$ W.R.T. h AND $\beta \in [0\,,\,\infty]$:

$$F_{h,\beta}(\omega) \ := \ Tr(\rho_{\omega} h) \ - \ \frac{1}{\beta} S(\omega) \tag{7.3.7.24}$$

Then one has the following:

Theorem 7.3.15

VARIATIONAL PRINCIPLE OF MINIMUM FREE ENERGY:

$$F_{h,\beta}(\omega_{h,\beta}^{(CAN)}) \ \leq \ F_{h,\beta}(\omega) \ \ \forall \omega \in S(\mathcal{B}(\mathcal{H})) \tag{7.3.7.25}$$

PROOF:

Let us observe that:

$$S_{Araki}(\omega_{h,\beta}^{(CAN)}, \omega) \,=\, F_{h,\beta}(\omega) \,-\, F_{h,\beta}(\omega)(\omega_{h,\beta}^{(CAN)}) \;\; \forall \omega \in S(\mathcal{B}(\mathcal{H})) \tag{7.3.7.26}$$

Applying theorem7.3.7 the thesis follows. ■

Corollary 7.3.2

VARIATIONAL PRINCIPLE OF MAXIMUM ENTROPY:

$$(Tr(\rho_{\omega} h) \,=\, Tr(\rho_{\omega_{h,\beta}^{(CAN)}} h)) \,\Rightarrow\, (S(\omega) \,\leq\, S(\omega_{h,\beta}^{(CAN)}) \tag{7.3.7.27}$$

PROOF:

Theorem7.3.15 says that the free entropy of $\omega_{h,\beta}^{(CAN)}$ is less of equal to the free antropy of any other state; so, in particular, it is less or equal to the free entropy of any other state having the same energy.

By the definition7.3.12 the thesis immediately follows ■

2. the key point in the proof of theorem1.3.6 is the Asymptotic Equipartition Property.

   Given a probability distribution $P \in \mathcal{D}(\Sigma)$ let us introduce the following:

   DEFINITION 7.3.13

   TIPICAL SET OF P W.R.T. $(n\,, \epsilon)$:

   $$A_{\epsilon}^{(n)} \;:=\; \{\vec{x} \in \Sigma^{n} \,:\, P^{n}(\vec{x}) \,\in\, (2^{-n(H(P)+\epsilon)}\,, 2^{-n(H(P)-\epsilon)})\} \tag{7.3.7.28}$$

   where we have denoted by P^n the product measure $\times_{i=1}^{n} P$.
   One has that:

   Theorem 7.3.16

   ASYMPTOTIC EQUIPARTITION PROPERTY:

   (a)

   $$H(P) - \epsilon \,\leq\, -\frac{1}{n} \log_2 P^{n}(\vec{x}) \,\leq\, H(P) + \epsilon \;\; \forall \vec{x} \in \Sigma^{n}\,, \forall \epsilon \in \mathbb{R}_{+}$$

(b)

$$\forall \epsilon \in \mathbb{R}_+ \, \exists N \in \mathbb{N}_+ \; : \quad P^n(A_\epsilon^{(n)}) \, > \, 1 - \epsilon \;\; \forall n > N$$

(c)

$$cardinality(A_\epsilon^{(n)}) \; \leq \; 2^{n(H(P)+\epsilon)} \;\; \forall \epsilon \in \mathbb{R}_+ , \forall n \in \mathbb{N}_+$$

$$\forall \epsilon \in \mathbb{R}_+ \, \exists N \in \mathbb{N}_+ \; : \quad cardinality(A_\epsilon^{(n)}) \; \geq \; (1-\epsilon) 2^{n(H(P)-\epsilon)} \;\; \forall n > N$$

Remark 7.3.4

THE RELEVANCE OF THE ASYMPTOTIC EQUIPARTITION PROPERTY FOR DATA COMPRESSION

The fact that theorem7.3.16 immediately implies theorem1.3.6 may be intuitivelly understood observing that is states substantially that asymptotically:

- the set Σ^n, made of 2^n strings, is the union of roughly $2^{nH(P)}$ **typical strings** and $2^n - 2^{nH(P)}$ **nontypical strings**
- the **typical strings** are equiprobable, each having a probability roughly equal to $2^{-nH(P)}$
- the **nontypical strings** have a roughly vanishing probability of occurring

The lexicographic ordering on Σ^n induces, clearly, a total ordering on $A_\epsilon^{(n)}$. Let us thus define a code D such that:

- $$D(\vec{x}) \; := \uparrow \;\; \forall \vec{x} \in \Sigma^n - A_\epsilon^{(n)} \tag{7.3.7.29}$$
- D assign to each typical sequence its ordering-number

For $n \; \rightarrow \infty$ the average code-word length $L_{D,P}$ tends to $H(P)$ that is conseguentially the required minimal number of cbit per letter

3. theorem7.3.16 may be easily shown to derive from Sanov's Theorem.

   Following the eight section of [Var84] let us introduce the following notion:

   DEFINITION 7.3.14

EMPIRICAL PROBABILITY MEASURE INDUCED BY $\vec{x} \in \Sigma^{\star}$:

the probability measure $R_{\vec{x}}$ on Σ^{∞}:

$$R_{\vec{x}} := \frac{1}{|\vec{x}|} \sum_{i=1}^{n} \delta_{\sigma^{i} \vec{x}^{\infty}} \tag{7.3.7.30}$$

Denoted by Q_n the distribution of $R_{\vec{x}}$ in the space of all the classical shifts over Σ, theorem7.3.3 implies that the sequence of distributions $\{Q_n\}_{n \in \mathbb{N}}$ satisfies the Large Deviation Principle with rate function $I(P) := -H(P)$, implying theorem1.3.6

Let us at last observe that it must be possible to translate the link among $C_M - C_{\Phi}$-probabilistic information and $C_M - C_{\Phi}$-algorithmic information stated by theorem1.3.7 looking at the satisfaction of a **Large Deviation Principle** as a **Law of Randomness**.

Let us consider again the case of a sequence of independent tosses of a classical coin, the throw at time n being described by the Bernoulli(1/2) random variable x_n.

Since the averages of the first tosses $av_n := \frac{1}{n} \sum_{i=1}^{n} x_i$ take values in the whole interval $[0,1]$ the sequence $\vec{av} := \{av_n\}_{n \in \mathbb{N}}$ belong to $[0,1]^{\infty}$.

On each copy of $[0,1]$ it is defined the central limit distribution $P_{central\ limit} := gauss_{standard}$.

Taking the direct product of all them we obtain the probability measure $P_{central\ limit}^{\infty}$ by which we can define the classical probability space $([0,1]^{\infty}, P_{central\ limit}^{\infty})$.

Sanov's Theorem may then be seen as a Law of Randomness $p_{Sanov} \in \mathcal{L}_{RANDOMNESS}[([0,1]^{\infty}, P_{central\ limit}^{\infty})]$.

Remark 7.3.5

THE COMPUTABILITY ISSUE INVOLVED IN THE CHARACTERIZATION OF THE LAWS OF RANDOMNESS OF $[([0,1]^{\infty}, P_{central\ limit}^{\infty})]$:

While the definition of the typical properties of $[([0,1]^{\infty}, P_{central\ limit}^{\infty})]$ is standard, the definition of the Laws of Randomness of such a classical probability space is a subtle issue since it involves the specification of $NC_M - C_{\Phi} - \Delta_0^0$ or $NC_M - NC_{\Phi} - \Delta_0^0$ objects with the inherent problematics we discussed in section1.1 and will further analyze in chapter7.4.

The next step consists in generalizing noncommutatively the definition7.3.2.

Let us consider again the sequence of independent tosses of a classical coin of constraint7.2.1.

Sanov's Theorem states, informally speaking, that in a statistical inferential process in which we estimate the probability distribution of the coin from the experimental result of n tosses, the probability that we don't distinguish the true unbiased probability distribution $P_{unbiased} = Bernoulli(\frac{1}{2})$ from a biased one P decades exponentially for large n as:

$$P[not - distinguish(P, P_{unbiased})] \sim \exp[-n S_{Kullback-Leibler}(P, P_{unbiased})] \tag{7.3.7.31}$$

It appears then natural to consider the same issue as to constraint7.2.2 analyzing what V. Vedral, M. B. Plenio and P.L. Knight call the Quantum Sanov's Theorem (cfr. the section 6.4.6 "Statistical Basis of Entanglement Measure" of [Kni00]).

This requires, anyway, to afford the subtle issue of **distinguishability of quantum states**.

A proper way of making this is to introduce some generalization of definition7.3.10 [Pet93], [Ohy97], [Ohy98].

Given a sub-$W^{\star}$-algebra $A_{accessible} \subset A$ of a $W^{\star}$-algebra A:

DEFINITION 7.3.15

ENTROPY OF THE SUBALGEBRA $A_{accessible}$ W.R.T. THE STATE $\omega \in S(A)$:

$$H_{\omega}(A_{accessible}) := \sup\{\sum_{i} \lambda_i S(\omega_i|_{A_{accessible}}, \omega|_{A_{accessible}}) : \{(\lambda_i, \omega_i)\} \in DEC(A)\} \tag{7.3.7.32}$$

We have clearly that:

Theorem 7.3.17

$$H_{\omega}(A) = S(\omega) \tag{7.3.7.33}$$

Furthermore Uhlmann's Monotonicity's Theorem for relative entropy, namely theorem7.3.6, immediately implies the following:

Theorem 7.3.18

MONOTONOCITY'S THEOREM FOR THE ENTROPY OF A SUBALGEBRA W.R.T. TO A STATE:

$$A_1 \subset A_2 \subset A \Rightarrow H_{\omega}(A_1) \leq H_{\omega}(A_2) \tag{7.3.7.34}$$

Considered another $W^{\star}$-algebra B and a channel $\alpha \in CPU(B, A)$:

DEFINITION 7.3.16

ENTROPY OF THE CHANNEL α W.R.T. $\omega \in S(A)$:

$$H_{\omega}(\alpha) := \sup\{\sum_{i} \lambda_i S(\omega_i \circ \alpha, \omega \circ \alpha) : \{(\lambda_i, \omega_i)\} \in DEC(A)\} \tag{7.3.7.35}$$

Uhlmann's Monotonicity's Theorem for relative entropy, namely theorem7.3.6, can be used again to derive another monotonicity's property:

Theorem 7.3.19

MONOTONOCITY'S THEOREM FOR THE ENTROPY OF A CHANNEL W.R.T. TO A STATE:

$$H_{\omega}(\beta \circ \alpha) \ \leq \ H_{\omega}(\alpha) \ \ \forall \omega \in S(A) \, , \forall \alpha, \beta \in CPU(A) \tag{7.3.7.36}$$

Let us now introduce the following quantitity:

DEFINITION 7.3.17

MUTUAL ENTROPY OF THE STATE $\omega \in S(A)$ AND THE CHANNEL $\alpha \in CPU(B, A)$:

$$I(\omega\, ; \, \alpha) \ := \ \sup\{ \sum_{i} \lambda_{i} S(\omega_{i} \circ \alpha , \omega \circ \alpha) \ : \ \{ (\lambda_{i} , \omega_{i}) \} \ \in \ DEC_{\perp}(\omega) \} \tag{7.3.7.37}$$

Remark 7.3.6

THE ENTROPY OF A CHANNEL W.R.T. A STATE VERSUS THE MUTUAL ENTROPY OF A STATE AND A CHANNEL

Definition7.3.16 and definition7.3.17 differ only in the **orthogonality constraint** for the involved decompositions.

Not surprisingly the two notions are then intimately related, as it is stated by the following:

Theorem 7.3.20

1.

$$(A \ commutative \ and \ card_{NC}(A) < \aleph_{0}) \ \Rightarrow \ (H_{\omega}(\alpha) \ = \ I(\omega, \alpha) \quad \forall \omega \in S(A) \, , \forall \alpha \in CPU(B, A) \ \forall B \text{ algebraic space})$$

2.

$$H_{\omega}(\alpha) \ = \ \sup\{ I(\mu , \beta \circ \alpha) \ : \ \omega \ = \ \mu \circ \beta \}$$

where β runs over all channels $A \mapsto C$ where C is finite-dimensional and commutative while μ runs over all the states on C such that $\omega \ = \ \mu \circ \beta$

Given a state $\omega \in S(A)$ and a decomposition of its $\mathcal{E} \ := \ \{ (\lambda_{i} , \omega_{i}) \}_{i=1}^{n} \ \in DEC(\omega)$:

DEFINITION 7.3.18

HOLEVO INFORMATION OF THE DECOMPOSITION $\mathcal{E}$:

$$I_{Holevo}(\mathcal{E}) \ := \ S(\sum_{i=1}^{n} \lambda_{i} , \omega_{i}) \ - \ \sum_{i=1}^{n} \lambda_{i} S(\omega_{i}) \tag{7.3.7.38}$$

Once more Uhlmann's Monotonicity's Theorem for relative entropy, namely theorem7.3.6, can be used to derive another monotonicity's property:

Theorem 7.3.21

MONOTONOCITY'S THEOREM FOR THE HOLEVO'S INFORMATION OF A DECOMPOSITION:

$$I_{Holevo}(\alpha_{\star}\mathcal{E}) \ \leq \ I_{Holevo}(\mathcal{E}) \ \ \forall \alpha \in CPU(A) \tag{7.3.7.39}$$

where the action of the dual channel $\alpha_{\star}$ of α on the decomposition $\mathcal{E}$ is simply defined as:

$$\alpha_{\star}(\{(\lambda_i, \omega_i)\}_{i=1}^{n}) \ := \ \{(\lambda_i, \alpha_{\star}\omega_i)\}_{i=1}^{n} \tag{7.3.7.40}$$

By theorem7.3.10 one has that:

Theorem 7.3.22

HOLEVO'S INFORMATION AND ENTROPY:

$$I_{Holevo}(\mathcal{E}) \ = \ S(\omega) \ \ \forall \mathcal{E} \in DEC_{EXT}(\omega)$$

Furthermore theorem7.3.11 immediately implies the following:

Theorem 7.3.23

POSITIVITY OF HOLEVO'S INFORMATION:

1.

$$I_{Holevo}(\mathcal{E}) \ \geq \ 0 \ \ \forall \mathcal{E} \in DEC(\omega) \, , \forall \omega \in S(A) \tag{7.3.7.41}$$

2.

$$(I_{Holevo}(\mathcal{E}) \ = \ 0 \ \Leftrightarrow \ (\lambda_i, \lambda_j > 0 \ \Rightarrow \omega_i = \omega_j)) \\ \forall \mathcal{E} = \{(\lambda_i, \omega_i)\} \in DEC(\omega) \, , \forall \omega \in S(A) \tag{7.3.7.42}$$

Let us now introduce the following notion:

DEFINITION 7.3.19

SHANNON'S ENTROPY OF THE DECOMPOSITION $\mathcal{E} \ := \ \{(\lambda_i, \omega_i)\}_{i=1}^{n}$:

$$H_{Shannon}(\mathcal{E}) \ := \ H(\{\lambda_i\}_{i=1}^{n}) \tag{7.3.7.43}$$

We have at last all the ingredients required to afford the **Distiguishability Issue** in a sistematic way, clarifying at last the reason of the locution **channel** adopted to denote a completely-positive unital map (cfr. definition5.1.73)

Let us start , at this purpose, from the the following simple situation:

Alice adopts a communicational-channel to send to Bob a letter A of the n-letters' alphabet Σ_n, choosing the letter A to send according to to a certain probability distribution $\vec{p}^{(A)} \in \mathcal{D}(\Sigma_n)$.

Let us suppose that the communicational-channel is noisy so that the letter B received by Bob is a classical random variable with probability distribution $\vec{p}^{(B)} \in \mathcal{D}(\Sigma_n)$ different from A.

DEFINITION 7.3.20

JOINT ENTROPY OF THE CLASSICAL RANDOM VARIABLES A AND B:

$$H(A\,,\,B) \;:=\; -\sum_{a,b\in\Sigma_n} p(a,b)\log_2 p(a,b) \tag{7.3.7.44}$$

Let us introduce a useful property we will use in the sequel:

Lemma 7.3.1

$$\sum_k p_k \log_2 q_k \;\leq\; \sum_k p_k \log_2 p_k \;\;\forall \vec{p},\vec{q}\in\mathcal{D}(\Sigma_n) \tag{7.3.7.45}$$

PROOF:

It follows by the inequality:

$$\log_2 x \;\leq\; x\,-\,1 \;\;\forall x\in\mathbb{R}_+ \tag{7.3.7.46}$$

poning $x \;:=\; \frac{q_k}{p_k}$ ■

As we already preannounced in section1.3 the joint entropy has the following important property:

Theorem 7.3.24

SUBADDITIVITY PROPERTY OF THE JOINT ENTROPY:

$$H(A\,,\,B) \;\leq\; H(A)\,+\,H(B) \tag{7.3.7.47}$$

PROOF:

The thesis immediately follows by lemma7.3.1 and the the definition of the involved objects ■

Introduced the following more convenient notation for the Kullback-Leibler's relative entropy:

DEFINITION 7.3.21

CONDITIONAL ENTROPY OF THE CLASSICAL RANDOM VARIABLES A W.R.T. THE CLASSICAL RANDOM VARIABLE B:

$$H(A\,|\,B) \;:=\; S_{Kullback-Leibler}(\vec{p}^{(A)},\vec{p}^{(B)}) \tag{7.3.7.48}$$

one has the following:

Theorem 7.3.25

CHAIN RULE FOR THE JOINT ENTROPY:

$$H(A\,,\,B) \;=\; H(A)\,+\,H(B\,|\,A) \tag{7.3.7.49}$$

PROOF:

Introduced the marginal distributions of A and B:

$$p(a) := \sum_{a \in \Sigma_n} p(a, b) \quad (7.3.7.50)$$

$$p(b) := \sum_{b \in \Sigma_n} p(a, b) \quad (7.3.7.51)$$

one has that:

$$\begin{aligned} H(A\,,\,B) &= -\sum_{a \in \Sigma_n} \sum_{b \in \Sigma_n} p(a,b) \log_2 p(a,b) = -\sum_{a \in \Sigma_n} \sum_{b \in \Sigma_n} p(a,b) \log_2 p(a) p(b|a) \\ &= -\sum_{a \in \Sigma_n} \sum_{b \in \Sigma_n} p(a,b) \log_2 p(a) - \sum_{a \in \Sigma_n} \sum_{b \in \Sigma_n} p(a,b) \log_2 p(b|a) \\ &= -\sum_{a \in \Sigma_n} p(a) \log_2 p(a) - \sum_{a \in \Sigma_n} \sum_{b \in \Sigma_n} p(a,b) \log_2 p(b|a) = H(A) + H(B \mid A) \end{aligned} \quad (7.3.7.52)$$

■

DEFINITION 7.3.22

MUTUAL INFORMATION OF THE CLASSICAL RANDOM VARIABLES A AND B:

$$I(A\,;\,B) := H(A) + H(B) - H(A,B) \quad (7.3.7.53)$$

Theorem 7.3.26

POSITIVITY OF THE MUTUAL INFORMATION:

1.

$$I(A\,;\,B) \geq 0 \quad (7.3.7.54)$$

2.

$$I(A\,;\,B) = 0 \Leftrightarrow \text{ A and B are independent} \quad (7.3.7.55)$$

PROOF:

Applying theorem7.3.24 and definition7.3.22 the thesis follows ■

The joint entropy $H(A\,,\,B)$ quantifies the total uncertainty we have about the pair $(A\,,\,B)$.

The mutual information $I(A\,;\,B)$, instead, quantifies how much information X and Y have in common; in fact, $H(X) + H(Y)$ is equal twice the information common to X and Y plus the non-common information of both the variables:

hence the information common to X and Y may be obtained subtracting from $H(X) + H(Y)$ their joint entropy.

Let us now observe that the information about A that can be obtained testing B is precisely the information that is common to A and B, namely $H(A\,;\,B)$ as it is stated formally by the following:

Theorem 7.3.27

ON GETTING INFORMATION ON A RANDOM VARIABLE TESTING ANOTHER RANDOM VARIABLE

$$I(A\,;\,B) \;=\; H(B) - H(A|B) \tag{7.3.7.56}$$

PROOF:

It is sufficient to apply theorem7.3.25 at the r.h.s. of definition7.3.22 ■

Let us now suppose that Alice tries to maximize the classical information she can trasmit to Bob sending a letter: she can do it choosing the distribution $\vec{p}^{(A)}$ in a clever way, i.e. so that it maximizes the mutual information $I(A\,;\,B)$.

Also with that choice, anyway, she can't transmit more than:

$$C_{classical} \;:=\; \max_{\vec{p}^{(A)} \in \Sigma_n} I(A\,;\,B) \tag{7.3.7.57}$$

cbit per letter.

Let us now observe that the number C depends only on the joint-distribution $p(a,b)$ defining the trasmission-channel adopted by Alice and Bob and is called the **classical-capacity** of the channel.

Clearly $C_{classical}$ is maximal when the transmission-channel is noiseless, i.e.:

$$p(b\,|\,a) \;=\; \delta_{a,b} \tag{7.3.7.58}$$

In this case one has that the general expression for the mutual entropy in terms of the marginal distribution of eq. 7.3.7.50

$$I(A\,;\,B) \;=\; \sum_{a \in \Sigma_n} \sum_{b \in \Sigma_n} p(a,b) \log_2 \frac{p(a,b)}{p(a)p(b)} \tag{7.3.7.59}$$

(one immediately derives from the definition7.3.22) reduces to the entropy of A:

$$I(A\,;\,B) \;=\; \sum_{a \in \Sigma_n} \sum_{b \in \Sigma_n} p(a,b) \log_2 \frac{p(a)\,p(b\,|\,a)}{p(a)p(b)}$$
$$= \sum_{a \in \Sigma_n} \sum_{b \in \Sigma_n} p(a)\,\delta_{a,b} \log_2 \frac{\delta_{a,b}}{p(b)} \;=\; -\sum_{a \in \Sigma_n} p(a) \log_2 p(a) \;=\; H(A) \tag{7.3.7.60}$$

since no misunderstanding-error by Bob can occur, a fact that we can express saying that Bob can **distinguish** the letters of Alice's adopted alphabet Σ_n.

Let us now observe that to say that the transmission channel is specified by the joint probability distribution $p(a,b)$ is equivalent to say that it is specified by the linear map $\alpha_{\star} : \mathcal{D}(\Sigma_n) \mapsto \mathcal{D}(\Sigma_n)$ such that:

$$\alpha_{\star}(\vec{p}^{(A)}) \; = \; \vec{p}^{(B)} \tag{7.3.7.61}$$

By theorem5.2.6 we can in an equivalent way look at $\alpha_{\star}$ as a map:

$$\alpha_{\star} \; : \; S(L^{\infty}(\Sigma_n \, , \, \vec{p}_{unbiased})) \; \mapsto \; S(L^{\infty}(\Sigma_n \, , \, \vec{p}_{unbiased}))$$

and, by theorem5.1.11, to infer that it is indeed the dual of a channel $\alpha \in CPU(L^{\infty}(\Sigma_n \, , \, \vec{p}_{unbiased}))$.

We have thus shown that a C_{Φ}-classical transmission-channel may be seen as a channel in the meaning of definition5.1.76.

Let us observe, furthermore, that instead of speaking about the mutual entropy $I(A \; ; \; B)$ of the two classical random variables A and B one could speak, in an equivalent way, of the mutual information $I(A \, , \, \alpha)$ of the random variable A and the channel α, i.e. of the mutual entropy $I(\omega_{\vec{p}_A} \; ; \; \alpha)$ of the state $\omega_{\vec{p}_A} \in L^{\infty}(\Sigma_n \, , \, \vec{p}_{unbiased})$ and the channel $\alpha \in CPU(L^{\infty}(\Sigma_n \, , \, \vec{p}_{unbiased}))$ in the meaning specified by the definition7.3.17 of which it is indeed a particular case.

Let us now suppose that to send her classical information, i.e. a letter of the commutative alphabet Σ_n Alice uses a quantum-communicational channel in the following way:

she codifies the letter $i \in \Sigma_n$ through a certain state $\omega_i \in S(\mathcal{A})$, where $\mathcal{A}$ is a certain noncommutative space.

Clearly Alice's state of affairs is described by the following decomposition:

$$\mathcal{E}^{(A)} \; := \; \{p_i^{(A)} \, , \, \omega_i\}_{i=1}^{n} \; \in \; DEC(\sum_{i=1}^{n} p_i^{(A)} \omega_i) \tag{7.3.7.62}$$

Let us now suppose that Alice transmit the state corresponding to the chosen letter through a noiseless quantum-transmission channel, mathematically described by the dual identity-channel $\mathbb{I}_{\star}$.

So the state arrives unchanged to Bob who would like, through a suitable experimental process to distinguish it in order of recovering the classical information Alice sent him.

To do this he makes a measurement, described by a suitable observational channel $\alpha \in CPU(C, \mathcal{A})$ on the noncommutative space $\mathcal{A}$,

Supposing that $cardinality_{NC}(C) = m$ so that the observational channel is determined by an m-ary partition of unity, Bob gets as output a classical random variable $j \in \Sigma_m$ with classical probability distribution $\vec{p}^{(B)} \in \mathcal{D}(\Sigma_m)$.

The classical information that Bob obtains in this way is clearly given by $I(A \, ; \, B)$.

Clearly Bob we will make his measurement in order of maximizing such a quantity; the maximal classical information he can gain, i.e. the classical capacity of the adopted quantum-transmission-channel, is then given by:

$$C_{classical} \; = \; \max_{\alpha} I(A \, ; \, B) \tag{7.3.7.63}$$

Let us now formalize this analysis; given an algebraic probability space $(A\,,\,\omega)$ and a decomposition $\mathcal{E} \;=\; \{\lambda_i\,,\,\omega_i\}_{i=1}^{n} \in DEC(\omega)$:

DEFINITION 7.3.23

ACCESSIBLE CLASSICAL INFORMATION OF $\mathcal{E}$:

$$I_{acc}(\mathcal{E}) \;:=\; \max_{\mathcal{V}\,\in\,OPU(A)} I(\{\lambda_i\}_{i=1}^{n}\,;\,\{\omega(\alpha_j)(\mathcal{V})\}_{j=1}^{card(\mathcal{V})})\} \qquad (7.3.7.64)$$

The **distinguishibility issue** may be completely analyzed in terms of the Groenwold-Lindblad's inequality, nowadays reknown as the:

Theorem 7.3.28

HOLEVO'S BOUND:

$$I_{acc}(\mathcal{E}) \;\leq\; I_{Holevo}(\mathcal{E}) \qquad (7.3.7.65)$$

PROOF:

The thesis follows applying theorem7.3.21 w.r.t. the reduction channel of the involved operational partitions of unity ■

Remark 7.3.7

INDISTINGUISHIBILITY OF NONORTHOGONAL STATES:

Considering again previous communicational situation among Alice and Bob, let us suppose that Alice codifies the i^{th} letter of the n-letters alphabet through a normal, pure state ω_i:

$$\rho_{\omega_i} \;=\; |\phi_i><\phi_i| \;\; i \in \Sigma_n \qquad (7.3.7.66)$$

where $\{|\phi_i>\}_{i=1}^{n}$ is a collection of **mutually-orthogonal** states over a suitable Hilbert space $\mathcal{H}$:

$$(i \neq j \;\Rightarrow <\phi_i|\phi_j> = 0) \;\; \forall i,j \in \Sigma_n \qquad (7.3.7.67)$$

Clearly:

$$\{p_i\,,\,\omega_i\}_{i=1}^{n} \;\in\; DEC_{EXT}(\sum_{i=1}^{n} p_i\,\omega_i) \;\; \forall \vec{p} \in \mathcal{D}(\Sigma_n) \qquad (7.3.7.68)$$

so that theorem7.3.22 implies that:

$$I_{Holevo}(\{p_i\,,\,\omega_i\}_{i=1}^{n}) \;=\; S(\sum_{i=1}^{n} p_i\,\omega_i) \;\; \forall \vec{p} \in \mathcal{D}(\Sigma_n) \qquad (7.3.7.69)$$

By the orthogonality condition we have, furthermore, that:

$$\{p_i\,,\,\omega_i\}_{i=1}^{n} \;\in\; DEC_{Schatten}(\sum_{i=1}^{n} p_i\,\omega_i) \qquad (7.3.7.70)$$

so that, by corollary7.3.1, we have that:

$$I_{Holevo}(\{p_i \, , \, \omega_i\}_{i=1}^{n}) \; = \; H_{Shannon}(\{p_i \, , \, \omega_i\}_{i=1}^{n}) \qquad (7.3.7.71)$$

Let us now consider the operational partition of unity $\mathcal{V} \; := \; \{|\phi_i><\phi_i|\}_{i=1}^{n}$; by the orthogonality-condition we have that:

$$I(\{p_i\}_{i=1}^{n} \, ; \, \{\omega(\alpha_j)(\mathcal{V})\}_{j=1}^{n}) \; = \; H_{Shannon}(\{p_i \, , \, \omega_i\}_{i=1}^{n}) \qquad (7.3.7.72)$$

We have thus shown that all the classical information contained in the Schatten-decomposition $\{p_i \, , \, \omega_i\}_{i=1}^{n}$ is accessible:

$$I_{acc}(\{p_i \, , \, \omega_i\}_{i=1}^{n}) \; = \; I_{Holevo}(\{p_i \, , \, \omega_i\}_{i=1}^{n}) \; = \; H_{Shannon}(\{p_i \, , \, \omega_i\}_{i=1}^{n}) \qquad (7.3.7.73)$$

so that Bob can distinguish the state Alice sent him, i.e. the letter of the alphabet Σ_n she transmitted.

Let us now remove the hypothesis of orthogonality of the states $\{|\phi_i>\}_{i=1}^{n}$ used by Alice.

Theorem7.3.14 implies than that:

$$S(\sum_{i=1}^{n} p_i \, \omega_i) \; \leq \; H_{Shannon}(\{p_i \, , \, \omega_i\}_{i=1}^{n}) \qquad (7.3.7.74)$$

so that:

$$I_{acc}(\{p_i \, , \, \omega_i\}_{i=1}^{n}) \; < \; I_{Holevo}(\{p_i \, , \, \omega_i\}_{i=1}^{n}) \; < \; H_{Shannon}(\{p_i \, , \, \omega_i\}_{i=1}^{n}) \qquad (7.3.7.75)$$

In this situation Bob cannot distinguish the state Alice sent him and, conseguentially, the letter of the alphabet Σ_n she trasmitted.

The situation of remark7.3.7 is absolutely general:

Theorem 7.3.29

ON THE REACHABILITY OF HOLEVO'S BOUND

$$I_{acc}(\mathcal{E}) \; = \; I_{acc}(\mathcal{E}) \; \Leftrightarrow \; \mathcal{E} \; \in \; DEC_{\perp}(\mathcal{E}) \qquad (7.3.7.76)$$

obviously implying, by theorem7.3.28, that the elements of an arbitrary ensemble of states over a noncommutative space are distinguishable iff they are mutually orthogonal:

Corollary 7.3.3

INDISTINGUISHIBILITY OF NONORTHOGONAL STATES:

$$I_{acc}(\mathcal{E}) \; < \; I_{acc}(\mathcal{E}) \;\; \forall \mathcal{E} \in (DEC(\mathcal{E}) - DEC_{\perp}(\mathcal{E})) \qquad (7.3.7.77)$$

Remark 7.3.8

HOLEVO'S INFORMATION OF A DECOMPOSITION VERSUS THE ENTROPY OF A SUB-$W^{\star}$-ALGEBRA:

Let us consider the following two notions:

- the Holevo's information $I_{Holevo}(\mathcal{E})$ of a decomposition $\mathcal{E} \in DEC(\omega)$
- the entropy $H_{\omega}(B)$ of a sub-$W^{\star}$-algebra B w.r.t. ω

where $\omega \in S(A)$ is a certain state on the algebraic space A.

Both have the feature of not-depending alone by ω but also by an other ingredient.

It would appear, then, rather natural to investigate their interrelation asking ourselves if they are not, trivially, speaking about the same thing in different languages, i.e. if,given an algebraic probability space $(A\,,\,\omega)$, it is not trivially the case that there exist a translator-bijection $Translation\,:\,\{$ sub-$W^{\star}$-algebras of A $\} \rightarrow DEC(\omega)$ such that:

$$H_{\omega}(B) \;=\; I_{Holevo}(Translation(B)) \;\; \forall B \in \{ \text{ sub-}W^{\star}\text{-algebras of A } \} \tag{7.3.7.78}$$

Related issues has been extensively analyzed by Fabio Benatti [Ben93], [Ben96], [Uhl99].

Given a k-dimensional abelian sub-$W^{\star}$-algebra B of A let us denote by $\{\hat{n}_{i}\}_{i=1}^{k}$ its **minimal projections**.

It would then natural to pose:

$$Translation(B) \;:=\; \{\omega(\hat{n}_{i})\,,\, \frac{\omega(\hat{n}_{i}\cdot)}{\omega(\hat{n}_{i})}\}_{i=1}^{k} \tag{7.3.7.79}$$

Benatti has proved that in this case one has that:

$$H_{\omega}(B) \;=\; I_{acc}(Translation(B)) \tag{7.3.7.80}$$

Since:

$$Translation(B) \;\in\; DEC_{\perp}(\omega) \tag{7.3.7.81}$$

it follows by theorem7.3.28 and corollary7.3.3 that:

$$H_{\omega}(B) \;=\; I_{Holevo}(Translation(B)) \tag{7.3.7.82}$$

Unfortunately the argument doesn't generalize to noncommutative sub$W^{\star}$algebras.

Remark 7.3.9

DISTINGUISHIBILITY VERSUS CLONING OF STATES

In 1982 two papers, one by D. Dieks and the other by W.K. Wooters and W.H. Zurek, introduced the following:

Theorem 7.3.30

NO UNITARY-CLONING THEOREM FOR NONORTHOGONAL PURE STATES ON HILBERT SPACES:

HP:

$$\mathcal{H} \text{ Hilbert space}$$

$$|\psi_1> \ |\psi_2>, |s> \in , \mathcal{H}$$

$$|\psi_1> \not\perp \ |\psi_2> \ and \, |\psi_1> \neq \ |\psi_2>$$

$$< s|s> = \ 1$$

TH:

$$\nexists \hat{U} \ \in \mathcal{U}[\mathcal{B}(\mathcal{H})] \ : \quad \hat{U}|\psi_i> \bigotimes |s> = \ |\psi_i> \bigotimes |\psi_i> \quad i \ = \ 1,2$$

PROOF:

If, ad absurdum, the thesis holded, it would imply that the complex number:

$$< \psi_1| \bigotimes < s|\hat{U}^{\dagger}\hat{U}|\psi_2> \bigotimes |s> \quad < \psi_1| \bigotimes < s|\psi_2> \bigotimes |s> = < \psi_1|\psi_2>$$

should be equal to:

$$< \psi_1| \bigotimes < \psi_1|\hat{U}^{\dagger}\hat{U}|\psi_2> \bigotimes |\psi_2> \quad < \psi_1| \bigotimes < \psi_1|\psi_2> \bigotimes |\psi_2> = \ | < \psi_1|\psi_2> |^2$$

i.e.:

$$| < \psi_1|\psi_2> |^2 \ = < \psi_1|\psi_2>$$

that implies that $|\psi_1> \perp \ |\psi_2>$ contradicting the hypothesis. ■

Furthermore one has that (cfr. cap.12 of [Chu00]):

Theorem 7.3.31

EQUIVALENCE BETWEEN THE NOT-UNITARY-CLONABILITY OF NONORTHOGONAL PURE STATES AND THEIR NOT-DISTINGUISHABILITY:

Theorem7.3.30 is equivalent to the restriction of corollary7.3.3 to extremal-decompositions over discrete noncommutative-probability-spaces

Theorem 7.3.32

NO CLONING THEOREM FOR NONORTHOGONAL NORMAL STATES ON DISCRETE NONCOMMUTATIVE PROBABILITY SPACES:

HP:

$$\mathcal{H} \text{ Hilbert space}$$

$$\omega_1 \, , \, \omega_2 \, , \, \omega_s \in S_n[\mathcal{B}(\mathcal{H})]$$

$$\omega_1 \not\perp \omega_2 \; and \; \omega_1 \neq \omega_2$$

TH:

$$\nexists \alpha \in CPU(A \bigotimes A) \; : \; \alpha_\star(\omega_i \cdot \omega_s) \; = \; \omega_i \cdot \omega_i \;\; i \; = \; 1,2$$

Up to date the only attempt to catch the $W^\star$-algebraic structure lying behind the No-cloning theorems is a theorem by Göran Lindblad [Lin99] that is, indeed, a generalization of theorem7.3.32 but is not yet a theorem poning a censorphip of cloning of suitable states on an arbitary noncommutative space.

Theorem7.3.31 can lead to suspect that such a (still lacking) theorem would be equivalent to corollary7.3.3.

Remark 7.3.10

DISTINGUISHIBILITY OF STATES VERSUS MAXWELL'S DEMONOLOGY

In the 9^{th} chapter of [Per95] Asher Peres claims that a violation of corollary7.3.3 would imply a violation of the Second Law of Thermodynamics.

His argument, anyway, lies on the assumption that the **thermodynamical-entropy** of a quantum system is described by **Von Neumann's entropy**, assumption that he deeply analyzes explicitly reporting the celebrated original calculus by which Von Neumann, in the section5.2 of [Neu83], computed the thermodynamical entropy of a mixture $\{p_i \, , \, |\phi_i >< \phi_i|\}_{i=1}^{n} \in DEC_{EXT}(\sum_i p_i |\phi_i >< \phi_i|)$ as if each $|\phi_i >< \phi_i|$ was a specie of ideal gas enclosed in a large impenetrable box and inferring that the thermodynamical mixing entropy of the different species is $S_{VonNeumann}(\sum_i p_i |\phi_i >< \phi_i|)$.

The assumption $S_{therm}(\omega) \; = \; S(\omega)$ would indeed seem to respect the Second Principle of Thermodynamics:

- by theorem7.3.8 and axiom5.2.3, the thermodynamical-entropy of a closed quantum dynamical system remains unchanged and thus, in particular, cannot decrease with time

- by theorem7.3.9 the thermodynamical-entropy of an open quantum dynamical system can decrease with time

But here the problem of Maxwell's demon, inherited from the classical problem for the mixing of different species of different ideal gases, appears.

Let us introduce it with Maxwell's own words; in the section "Limitation of The Second Law of Thermodynamics" of the 12^{th} chapter of [Max71] he writes:

"One of the best extablished facts in thermodynamics is that it is impossible in a system enclosed in an envelope which permits neither change of volume nor passage of heat, and in which both the temperature and the pressure are everywhere the same, to produce any inequality of temperature or of pressure without the expenditure of work. This is the second law of thermodynamics, and it is undoubtedly true as long as we can deal with bodies only in mass, and have no power of perceiving or handling the separate molecules of which they are made up. But if we conceive a being whose faculties are so sharpened that he can follow every molecule in its course, such a being, whose attributes are still as essentially finite as our own, would be able to do what is at present impossible to us. For we have seen that the molecules in a vessel full of air at uniform temperature are moving with velocities by no means uniform, though the mean velocity of any great number of them, arbitrary selected, is almost exactly uniform. Now let us suppose that such a vessel is divided in two portions, A and B, by a division in which there is a small hall, and that a being, who can see the individual molecules, opens and closes this hole so as to allow only the lower ones to pass from B to A. He will see, thus, without expenditure of work, raise the temperature of B and lower that of A, in contradiction with the second law of thermodynamics" (cited in the first chapter of [Rex90])

In our case, instead of leaving to pass or stopping molecules according to their velocity, it leaves to pass or stops Von Neuman's impenetrable boxes according to the specie of the $|\phi_i><\phi_i|$ it pertains in the following way:

- it leaves to pass from A to B only boxes pertaining to species with label $i \geq \lfloor \frac{n}{2} \rfloor$

- it leaves to pass from B to a only boxes pertaining to species with label $i < \lfloor \frac{n}{2} \rfloor$

Let us then leave aside for the moment our quantum situation and let us analyze the classical problem, as Maxwell presents it. In the 220 years after the publication of Maxwell's book an enormous literature tried to exorcize it in different ways; an historical review may be found in the first chapter "Overview" as well as in the "Chronological Bibliography with Annotations and Selected

Quotations" of the wonderful book edited by Harvey S. Leff and Andrew F. Rex [Rex90].

All these exorcisms were based on the idea that, to accomplish his task, the Maxwell'demon necessarily causes a thermodynamical-entropy's raising causing the Second Law to be preserved:

they anyway strongly differed in identifying the element of the demon's dynamical evolution which is **necessarily thermodinamically-irreversible**:

coming to recent times, most of the Scientific Community strongly believed in Leon Brillouin's exorcism [Bri90], identifying such an element in the **demon's information-acquisition's process**

When anyone though that the "The-end" script had at last appeared to conclude "The Exorcist" movie, Charles H. Bennett showed in 1982 [Ben90a], [Ben90b], basing on the previous work by Rolf Landauer on the **Thermodynamics of Computation** [Lan90], that:

1. Maxwell's Demon was still alive owing to the nullity of Brillouin's exorcism: the demon's acquisition process may be done in a completelly thermodynamically-reversible way:
2. the **necessarily thermodinamically-irreversible** element is instead **demon's information-erasure's process**

Given two arbitrary sets A and B a partial function f from A to B $f \in \overset{\circ}{MAP}$ (A, B):

DEFINITION 7.3.24

f IS LOGICALLY REVERSIBLE:

it is injective, i.e.:

$$cardinality(f^{-1}(b)) \in \{0, 1\} \ \ \forall b \in B \tag{7.3.7.83}$$

DEFINITION 7.3.25

f IS THERMODINAMICALLY-REVERSIBLY-COMPUTABLE:

1. there exist a physical device of any kind computing f $\cdots$:

$$f \ \in \ \Delta_0^0 - \overset{\circ}{MAP} \ (A, B)$$

2. $\cdots$ in a thermodinamically reversible way (i.e. in such a way that the computational-process doesn't increase the thermodynamical entropy of the Universe)

Both the theoretical analysis of specific computational models and the experiments strongly support the following:

AXIOM 7.3.1

LANDAUER'S PRINCIPLE:
HP:

$$f \in \Delta_0^0 - \overset{\circ}{MAP}(A, B)$$

TH:

$$\text{f is thermodynamically-reversibly-computable} \Leftrightarrow \text{f is logically-reversible} \quad (7.3.7.84)$$

Let us now suppose that we want to compute a thermodinamically-irreversibly-computable function $f : A \overset{\circ}{\to} B$.

We can exploit our computation in a thermodinamically-reversible way at the prize of keeping memory of the input , e.g. computing the thermodinamically-reversibly-computable function $\tilde{f} : A \overset{\circ}{\to} B$:

$$\tilde{f}(a) := (a , f(a)) \quad (7.3.7.85)$$

In Thermodynamics of Computation, the suppletive information on the input we have conserved is called **garbage**.

Let us now consider the process of information-erasing: it can be mathematically described by the following:

DEFINITION 7.3.26

ERASURE-FUNCTION OF A:

$$er(A) : A \to \emptyset \quad (7.3.7.86)$$

One has then that:

Corollary 7.3.4

INFORMATION-ERASURE IS THERMODINAMICALLY-IRREVERSIBLY-COMPUTABLE:
er(A) is thermodynmamically-irreversibly-computable

PROOF:

Given a thermodinamically-irreversibly-computable function $f : A \overset{\circ}{\to} B$ let us suppose ad absurdum that er(A) is thermodynmamically-irreversibly-computable; then $\tilde{f} \circ er(A)$ would be thermodinamically-reversibly-computable. Since:

$$\tilde{f} \circ er(A) = f \quad (7.3.7.87)$$

this would contradict the hypothesis ■

Let us now return to the Maxwell's demon: conceptually it may be formalized as a computer that:

1. gets the input (s, v) from a device measuring both the side s from which the molecule arrives and its velocity
2. computes a certain semaphore-function p such that $(s, v) \stackrel{p}{\to} p[(s, v)]$ giving as output a 0 if the molecule must be left to pass while gives as output a one if the molecule must be stopped
3. gives the output p[(s,v)] to a suitable device that operates on the molecule in the specified way

Both the first and the third phases of this process, taking into account also the involved devices, may be made in a thermodinamically-reversible way.

As to the second step, anyway, let us observe that the semaphore-function p is logically-irreversible and hence, by axiom7.3.1, also thermodinamically-irreversibly-computable.

As above specified, such a thermodinamically-irreversibility may be avoided conserving **garbage**; let us, precisely, suppose, that the demon-computer computes the thermodynamically-reversibly-computable function $\tilde{p}$.

Let us suppose to make operate the demon-computer n times on n different molecules.

When n grows then demon, with no expenditure of work, would raise the temperature of B and lower that of A.

But let us now analyze more carefully Clausius's formulation of the Second Principle:

AXIOM 7.3.2

SECOND PRINCIPLE OF THERMODYNAMICS IN CLAUSIUS' FORM:

No thermodynamical transformation is possible **that has as its only result** the passage of heat from a body at lower temperature to a body at higher temperature

In the above process the passage of heat from A to B is not the only result: another result is the storage in the demon-computer's memory of the n-ple of inputs $((s_1, v_1), \cdots, (s_n, v_n))$.

To make the passage of heat from A to B to become the only result of the process we could think that the demon, at the end, erases his memory; but, by corollary7.3.4 this (and only this) cannot be done in a thermodynamically-reversible way: such an erasure causes an increase of entropy that may be proved to be greater than or equal to the entropy-decrease produced by the passage of heat from A to B (an explicit computation for the conceptually analogous situation of Szilard's engine [Szi90] may be found in the section8.5 of [Vit97]).

Bennett's exorcism of Maxwell's demon, has, anyway, a far reaching conseguence; supposed that the gas is described by thermodynamical ensemble (X, P), let us introduce the following:

DEFINITION 7.3.27

BENNETT'S ENTROPY OF P:

$$S_{Bennett}(P) \ := \ I_{probabilistic}(P) \ + \ I_{algorithmic}(P) \ = \ H(P) + I(P) \tag{7.3.7.88}$$

where H(P) is Shannon's entropy of the distribution P (i.e. it Gibbs' entropy in thermodynamical language), while I(P) is its prefix-algorithmic-entropy, i.e. the length of the shortest program computing it on the fixed Chaitin universal computer U.

One has that:

Theorem 7.3.33

BENNETT'S THEOREM:

$$S_{therm}(P) \ = \ S_{Bennett}(P) \ \neq H(P)$$

PROOF:

The thesis follows by Bennett's exorcism of Maxwell's demon: it implies that when a physical system increases its prefix-algorithmic-entropy by n cbits, it has the capacity to convert about $nT \ln 2$ of wasten heat into useful work in its surrounding.

Conversely, the conversion of about $nT \ln 2$ of work into heat in the surrounding is necessary to decrease a system's prefix-algorithmic-entropy by n cbits $\blacksquare$

It may be worth to observe that the additive constant by which prefix-algorithmic entropy is defined, depending on the choice of the fixed universal computer doesn't matter as far as the first two principles of thermodynamics are concerned.

Such a constant is anyway fixed by the imposition of the Third Principle of Thermodynamics:

so, the imposition that the thermodynamical-entropy vanishes at zero temperature, curiously results in a fixing of a particular Chaitin's universal computer U and, conseguentially, of the associated Halting Probability Ω_U.

The generalization both of Bennett's exorcism of Maxwell's demon and of the Bennett's Theorem to the quantum domain has been extensively analyzed by Wojciech H. Zurek [Zur89], [Zur90b], [Zur90a], [Zur99].

Given a density operator $\rho \in \mathcal{D}(\mathcal{H})$ on an Hilbert space $\mathcal{H}$:

DEFINITION 7.3.28

ZUREK'S ENTROPY OF ρ:

$$S_{Zurek}(\rho) \ := \ S_{VonNeumann}(\rho) \ + \ I(\rho) \tag{7.3.7.89}$$

with:

$$I(\rho) \ := \min_{\vec{x} \in \Sigma^\star \, : \, U(\vec{x}) = \rho} |\vec{x}| \tag{7.3.7.90}$$

Zurek's claim that the assumption of the Church-Turing's Thesis eliminate any dependence from the particular universal computer U adopted, or better constituting the demon.

He, in particular, seems to claim that, by the Church-Turing's Thesis, it doesn't matter if U is a **classical computer** or a **quantum computer**, i.e. that the assumption of Church-Turing's Thesis implies that Quantum Algorithmic Information Theory collapses to Classical Algorithmic information Theory, an assumption absolutely arbitary as we will analyze more completely in section8.3.

We will, therefore assume, from here and beyond that the computer U in definition7.3.28 is Universal Quantum Computer.

But let, then observe, that in this way, one implicitely assumes that the quantum algorithmic information of a quantum state must be defined in terms of classical-descriptions of such a state , as claimed by Svozil [Svo96] and Vitanyi [Vit99], [Vit01] and not in terms of quantum descriptions as it is claimed by Berthiaume, Van Dam and Laplante [vDSL00] as we discussed in chapter6.

The **garbage** accumulated by the demon is, therefore, made of cbits, i.e. of classical information.

Let us suppose, instead, that the inputs of the quantum computer U are qubits and not cbits, i.e. let us suppose to modify definition7.3.28 replacing the defintion of $I(\rho)$ given by eq.7.3.7.90 so that U's inputs are qubits and not cbit: the **garbage** accumulated by the demon would then consist of **quantum information** instead of **classical information**.

As far as the exorcism is concerned, anyway, such a replacement doesn't change anything, since the generality of corollary7.3.4 assures the thermodynamical-irreversible-computability of the erasure of both classical and quantum information.

What is important here to stress is the Zurek's extension of Bennett's exorcism to the quantum domain implies the quantum analogue of theorem7.3.33:

Theorem 7.3.34

ZUREK'S THEOREM:

$$S_{therm}(\rho) \;=\; S_{Zurek}(\rho) \;\neq\; S_{VonNeumann}(\rho) \tag{7.3.7.91}$$

Let us now observe that, in the general framework of Quantum Probability Theory, Bennett's and Zurek's results may be unified in the following way:

given an algebraic probability space $(A\,,\,\omega)\,,\,\omega \in NC_M - NC_\Phi - \Delta_0^0 - S(A)$ (according to the the notion of computability we will extensively discuss in chapter8):

DEFINITION 7.3.29

DOUBLE-APPROACH ENTROPY OF ω:

$$S_{\text{double approach}}(\omega) \;:=\; S(\omega) \,+\, I(\omega) \tag{7.3.7.92}$$

where $I(\omega)$ is the **algebraic algorithmic information** of ω we will introduce in chapter8)

The name in definition7.3.29 has been chosen to stress that involves , in the Kolmogorovian terms introduced in section0.4, **both the probabilistic and the algorithmic approach to Information Theory**.

What it is important to stress is that Bennett's and Zurek's analyses generalize in a straightforward way giving rise to the following:

Theorem 7.3.35

BENNETT-ZUREK'S THEOREM:

$$S_{therm}(\omega) \; = \; S_{\text{double approach}}(\omega) \; \neq \; S(\omega) \qquad (7.3.7.93)$$

The fact, stated by theorem7.3.35 that to the **thermodynamical entropy** of a system doesn't contibute only its **probabilistic entropy** but also its **algorithmic entropy** is according to us nothing but the opening of a new chapter in the history of Thermodynamics, whose still lacking precise mathematical formalization, has prevented it to be even taken in consideration by the Mathematical-Physicists' Community.

Those of them has spent a life studying Rigorous Statistical Mechanics, e.g. in [Sim93] [Rue99], [Rob97], may be reassured that in any situation involving no information-gathering-and-using-system (IGUS) $I(\omega)$ vanishes so that so all the theorems therein contained apply.

Instead of reacting to theorem7.3.35 with that typical reactionary attitude of the worst among mathematicians and mathematical-physicists (but fortunately not by the greatest minds of both Mathematics and Mathematical-Physics), consisting in discarding any novelty since is not presented specifying if functions are of class $C^{(1)}$ or $C^{(2)}$ and have not all the bows around the ϵ's and δ's well posed, the lovers of mathematical rigour should contribute to mathematically formalize the proof of theorem7.3.35, as well as to mathematically formalize the notion of an IGUS.

We have now all the ingredients required to analyze Asher Peres' claim that a violation of corollary7.3.3 would imply a violation of the Second Law of Thermodynamics, returning to his analysis of Von Neumann's computation of the thermodynamical-entropy of the mixture $\{p_i \, , |\phi_i \; >< \; \phi_i|\}_{i=1}^{n} \in DEC_{EXT}(\sum_i p_i |\phi_i \; >< \; \phi_i|)$. Peres reviews Von Neumann's procedure in the following way:

"It also assumes the existence of semipermeable membranes which can be used to perform quantum tests. ***These membranes separate orthogonal states with perfect efficency****. The fundamental problem here is whether it is legitimate to treat* ***quantum states*** *in the same way as varieties of classical ideal gases. This issue was clarified by Einstein in the early days of the "old" quantum theory as follows: consider an ensemble of quantum systems, each one enclosed in a large impenetrable box, so as to prevent any interaction between them. These boxes are enclosed in an even larger container, where*

they behave ***as an ideal gas****, because each each box is so massive that classical mechanics is valid for its motion* $(\cdots)$*. The container itself has ideal walls and pistons which may be, according to our needs, perfectly conducting, or perfectly insulating, or with properties equivalent to those of semipermeable membranes.* ***The latter are endowed with automatic devices able to peak inside the boxes and to test the state*** *of the quantum system enclosed therein." (from the section9.3 of [Per95])*

There is a point, anyway, of this review in which, deliberately, Peres moves away from Von Neumann's original treatment:

he doesn't assume that **the membranes separate nonorthogonal states with perfect efficiency** as, instead, Von Neumann does:

"Each system $s_1, \cdots, s_n$ *is confined in a box* $K_1, \cdots, K_n$ ***whose walls are impenetrable to all transmission effects*** *– which is possible for this system because of the lack of interaction" (from the section5.2 of [Neu83])*

The reason why Peres, contrary to Von Neumann, doesn't make such an assumption is that, according to him, this would imply a violation of the Second Law of Thermodynamics; his argument is the following: if semi-permeable membranes which unambiguously distinguish non-orthogonal states where possible, one could use then to realize the following cyclic thermodynamical transformation for a mixture of two species of 1-qubit's states, the $|0><0|$-specie and the $\frac{1}{2}(|0>+|1>)(<0|+<1|)\}$- specie, both with the same concentration $\frac{1}{2}$

- in the initial state the two species occupy two chambers with equal volumes, with the $|0><0|$- specie occupying the right-half of the left-half of the vessel and the $\frac{1}{2}(|0>+|1>)(<0|+<1|)\}$- specie occupying the left-half of the right-half of the vessel

- the first step of the process is an isothermal expansion by which the $|0><0|$- specie occupies all the left-half of the vessel while the $\frac{1}{2}(|0>+|1>)(<0|+<1|)$-specie occupies all the right-half of the vessel; this expansion supplies an amount of work:

$$\Delta L_1 \;=\; +nT\ln 2 \qquad (7.3.7.94)$$

  T being the temperature of the reservoir.

- at this stage the impenetrable partitions separating the two species are replaced by the "magic"-semi-permeable membranes having the ability of distinguish non-orthogonal states; precisely one of them is transparent to the $|0><0|$-specie and reflect the $\frac{1}{2}(|0>+|1>)(<0|+<1|)\}$-specie while the other membrane has the opposite properties; then, by a double frictionless piston, it is possible to bring the engine, without expenditure of work or heat transfer, to a state in which all the two species occupy with the same concentration only the left-hand of the vessel, the right-hand of the vessel remaining empty; we can represent mathematically the state of affairs of the system by the decomposition:

$$\mathcal{E}_1 \; := \; \{(\frac{1}{2}, |0><0|) \, , \, (\frac{1}{2}, \frac{1}{2}(|0>+|1>)(<0|+<1|))\} \; \in \; DEC_{EXT}(\rho) \tag{7.3.7.95}$$

$$\rho \; := \; \begin{pmatrix} \frac{3}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} \end{pmatrix} \tag{7.3.7.96}$$

- since the state of the mixture-of-species is completelly determined by ρ, and not by a particular its decomposition, to represent the actual state of affairs by $\mathcal{E}$ or by the Schatten's decomposition of ρ:

$$\mathcal{E}_1 \; := \; \{(\rho_-, |e_- >< e_-|) \, , \, (\rho_+, |e_+ >< e_+|)\} \in DEC_{Schatten}(\rho) \tag{7.3.7.97}$$

$$\rho_\pm \; := \; \frac{1}{4}(2 \pm \sqrt{2}) \tag{7.3.7.98}$$

$$|e_\pm > \; := \; (1 \pm \sqrt{2})(|0> + |1>) \tag{7.3.7.99}$$

- let us now replace the two "magic" membranes with ordinary membranes able to distinguish only orthogonal species; since the $|e_- >< e_-|$-specie and the $|e_+ >< e_-|$-specie are orthogonal, the reversible diffusion of the two species separate them, with the $|e_+ >< e_+|$-specie occupying the left-half of the vessel and the $|e_- >< e_-|$-specie occupying the left-half of the vessel.

- finally an isothermal compression takes the system in a situation in which the volume and the pressure are the same of the initial state ; such a compression requires an expenditure of work of:

$$\Delta L_2 \; = \; -nT[\rho_1 \log \rho_1 \; + \; \rho_2 \log \rho_2] \tag{7.3.7.100}$$

- finally a suitable unitary evolution takes the system again in the initial state.

The net work made by the engine during the cycle is:

$$\Delta L \; = \; \Delta L_1 + \Delta L_2 \; > \; 0 \tag{7.3.7.101}$$

so that,the whole thermodynamical cycle converts the heat extracted by the reservoir in a positive amount of work of ΔL.

This, according to Peres violates the Second Principle, proving that **the the "magic" membranes able to separate nonorthogonal states with perfect efficiency** cannot exist.

But let us again look more carefully at the precise formulation of the Second Principle, making use of the following well known theorem of Thermodynamics:

Theorem 7.3.36

EQUIVALENCE OF CLAUSIUS' AND KELVIN'S FORMULATIONS OF THE SECOND PRINCIPLE OF THERMODYNMAMICS:

Axiom7.3.2 is equivalent to the following Kelvin's-formulation:

No thermodynamical transformation is possible **that has as its only result** the transformation of heat into work

Let us now analyze a cycle of Peres'-engine: is the conversion of heat into work **the only result** of the process ?

The answer is negative and lead immediately to the the conceptual deepness of theorem7.3.35, whose complete comprehension requires to explicitly analyze the bug in Von Neumann's proof that $S_{therm}(\rho) = S_{VonNeumann}(\rho)$.

The key point lies in the own definition of the semi-permeables membranes of Einstein's method: as correctly observed by Peres **the semipermeable-membranes are endowed with automatic devices able to peak inside the boxes and to test the state**.

What Peres seems unfortunately not to catch is that a semi-permeable membrane is then an IGUS operating in the following way:

1. gets the input (s,i) from a device measuring both the side s from which the $|\phi_i><\phi_i|$-species arrives and its kind, i.e. the classical information codified by its label i.

2. computes a certain semaphore-function p such that $(s,i) \stackrel{p}{\rightarrow} p[(s,i)]$ giving as output a 0 if the $|\phi_i><\phi_i|$-specie must be left to pass while gives as output a one if the $|\phi_i><\phi_i|$-specie must be stopped

3. gives the output p[(s,i)] to a suitable device that operates on the $|\phi_i><\phi_i|$-specie in the specified way

The argument of Bennett's exorcism concerning the necessity of taking into account the prefix-algorithmic-information of the sequences of successive recorded (s,i)'s in the membrane's memory thus apply.

But this must be done, in particular, in the cases of Peres'-engine:

taking into account also the algorithmic-entropy of the semi-permeable's membranes, one sees that it is greater than or equal to the universe's entropy decrease corresponding to the work made by the engine, so that, by theorem7.3.35:

$$\Delta S_{therm} \geq 0 \tag{7.3.7.102}$$

and Peres' arguments falls down.

Having analyzed in details the many subtilities of the **Distinguishibility Issue**, we can return to Vedral, Plenio and Knight's Quantum Sanov's Theorem with the objective of rephrasing it as a Quantum Law of Randomness in the same way we sketched for the classical case

Informally speaking, the argument by Vedral, Plenio and Knight is that the probability of not distinguishing two quantum states $\rho , \sigma \in \mathcal{D}(\mathcal{H})$ after n measurements decades exponentially as:

$$P[not-distinguish(\rho\,,\,\sigma)] \;\sim\; \exp[-n\, S_{Umegaki}(\sigma\,,\rho)] \qquad (7.3.7.103)$$

As we preannounced, its mathematical formalization requires to generalize noncommutatively the definition7.3.2.

Given an algebraic space A:

DEFINITION 7.3.30

ALGEBRAIC RATE FUNCTION OVER A:

a map $I \in MAP[A\,,\,[0,\infty)]$:

$$\{a \in A \,:\, I(a) \leq \alpha\} \text{ is closed } \;\forall \alpha \in [0,\infty) \qquad (7.3.7.104)$$

Given a family $\{\omega_{\epsilon}\}$ of states over A:

DEFINITION 7.3.31

$\{\omega_{\epsilon}\}$ SATISFIES THE ALGEBRAIC LARGE DEVIATION PRINCIPLE WITH RATE FUNCTION I:

$$-\inf_{a \in \Gamma^0} I(a) \;\leq\; \liminf_{\epsilon \rightarrow 0} \epsilon \log \omega_{\epsilon}(\Gamma) \;\leq\; \limsup_{\epsilon \rightarrow 0} \epsilon \log \omega_{\epsilon}(\Gamma) \;\leq\; -\inf_{a \in \bar{\Gamma}} I(a) \;\; \forall \Gamma \subset A \qquad (7.3.7.105)$$

where Γ^0 denotes the interior of Γ while $\bar{\Gamma}$ denotes the closure of Γ w.r.t. a suitable topology on A (let's say the weak topology).

Denoted by $P_{\omega}^{(NC)} \in S(\Sigma_{NC}^{\infty})$ the state over Σ_{NC}^{∞} associated to a sequence of independent, identically distributed noncommutative random variables distributed following $\omega \in S(\Sigma_{NC})$, the key not trivial point is how to generalize noncommutatively the definition7.3.3 of the **type** $L_n^{\vec{a}} \in S(\Sigma_{NC})$ of a qubit string $\vec{a} \in S(\Sigma_{NC})$ so that:

Conjecture 7.3.1

QUANTUM SANOV'S THEOREM:

The family of laws $P_{\omega}(L_n^{\vec{a}} \,\in\, \cdot)$ satisfies the Algebraic Large Deviation Principle with algebraic rate function $S_{Araki}(\cdot\,,\,\omega)$.

The reformulation of 7.3.1 as a Law of Randomness of $(\Sigma_{NC}^{\infty}\,,\, P_{\text{noncommutative central limit}}^{\infty})$ would be then straightforward.

7.4 On absolute conformism in Quantum Probability Theory

Given an algebraic probability space (A, ω) we have seen in section7.1 how, trying to generalize noncommutatively Kolmogorov's approach of characterizing absolute conformism, one ends up in definition7.1.6 and definition7.1.7 according to one takes into account, respectively, **commutative predicates** or **noncommutative predicates** over A.

We know, anyway, by theorem3.2.1 that absolute-conformism in Classical Probability Theory is impossible so that:

Corollary 7.4.1

$$A \, commutative \; \Rightarrow \; KOLMOGOROV_{C}(APS) \, = \, KOLMOGOROV_{NC}(APS) \, = \, \emptyset$$

At a classical level this fact has the conceptually-deep effect of not-allowing to define an individual random element of a classical probability space with only measure-theoretic tools, requiring the introduction of ingredients from Computations' Theory in order of selecting a suitable subclass of the the typical properties, the Laws of Randomness, to the constraint on conformism is restricted.

Let us remind that the diagonalization-proof of theorem3.2.1 lies on the fact that:

$$p_{\text{difference from } \bar{y}} \, \in \, \mathcal{P}(\Sigma^{\infty}, P_{unbaised}) \;\; \forall \bar{y} \in \Sigma^{\infty} \qquad (7.4.7.1)$$

Let us than analyze the state of affairs of the algebraic generalization of such difference predicates:

DEFINITION 7.4.1

COMMUTATIVE PREDICATE OF DIFFERENCE FROM $b \in A$:

$$p_{\text{difference from b}} \in \mathcal{P}_{C}(APS)$$

$$p_{\text{difference from b}}(a) \; := \; << a \neq b >> \qquad (7.4.7.2)$$

Let us observe that, owing to the nonexistence of points (not even hidden) on a noncommutative space we discussed in section5.3, one has that:

$$p_{\text{difference from b}} \; \notin \; \mathcal{P}_{C}^{typical}(APS) \;\; \forall b \in A \qquad (7.4.7.3)$$

so that the diagonalization proof of theorem3.2.1 doesn't generalize noncommutatively as to commutative predicates; obviously this is true also as as to noncommutative predicate where no natural noncommutative predicate of difference from a single element exists.

One could, conseguentially, think of that the notion of a random sequence of qubits might be characterized through $KOLMOGOROV_{C}(\Sigma_{NC}^{\infty})$ or by $KOLMOGOROV_{NC}(\Sigma_{NC}^{\infty})$.

According to us, anyway, one has to impose again the effectiveness's constraint on the considered typical properties, as we will do in the next chapter

Chapter 8

Quantum algorithmic randomness as satisfaction of all the quantum algorithmic typical properties

8.1 The problem of characterizing mathematically the notion of a quantum algorithm

The greatest goal of Quantum Computation is the discovery of many **quantum algorithms** allowing to make **tractable** problems **intractable** by classical computers, in the sense specified in section5.4, in almost all cases reconducting it to particular istances of the **Abelian hidden subgroup problem** (cfr. the 5^{th} and 6^{th} chapters of [Chu00])

Beside all that business the answer to the innocent question:

what is a quantum algorithm ?

is absolutely not known.

Let us, then, return to the discussion of the Computability Issue of section1.1 As far as the $cell_{21}$ of the diagram1.1.1 is concerned, let us return to the discussion whether Quantum Mechanics can lead to a violation Church-Turing's Thesis, i.e. it cannot be the case that:

$$Q_{\Phi} - C_{M} - \Delta_{0}^{0} - \overset{\circ}{MAP}\,(\Sigma^{\star}, \Sigma^{\star}) \supset REC - \overset{\circ}{MAP}\,(\Sigma^{\star}, \Sigma^{\star})$$

where by $Q_{\Phi} \subset NC_{\Phi}$ we denote that the involved physically-nonclassical computational device obeys the Laws of **Nonrelativistic Quantum Mechanics** or those of **Special-relativistic Quantum Mechanics**.

The problem has been recently analyzed by Michael Nielsen in the following way:

given a not-recursive function $f \in MAP(\Sigma^{\star}, \Sigma^{\star})$ let us consider the following operators on $\mathcal{H}_2^{\star}$:

$$\hat{f} := \sum_{\vec{x} \in \Sigma^{\star}} f(\vec{x}) \, |\vec{x} >< \vec{x}| \tag{8.1.8.1}$$

$$\hat{U}_f := \sum_{\vec{x} \in \Sigma^{\star}} |f(\vec{x}) >< \vec{x}| \tag{8.1.8.2}$$

Let us then introduce the following:

DEFINITION 8.1.1

FIRST NIELSEN'S ALGORITHM W.R.T. f ($NIELSEN_1(f)$):

1. take a closed quantum mechanical system with observables' algebra $\mathcal{B}(\mathcal{H}_2^{\star})$
2. prepare it in the state $|\vec{x}>$
3. make a measurement of $\hat{f}$
4. read the measurement's outcome

DEFINITION 8.1.2

SECOND NIELSEN'S ALGORITHM W.R.T. f ($NIELSEN_2(f)$):

1. take a closed quantum mechanical system with observables' algebra $\mathcal{B}(\mathcal{H}_2^{\star})$
2. prepare it in the state $|\vec{x}>$
3. act on it the quantum gate $\hat{U}_f$
4. make a measurement of $|\vec{x} >< \vec{x}|$
5. read the measurement's outcome

One has then the following:

Theorem 8.1.1

ON THE EFFECTIVE-REALIZABILITY OF NIELSEN'S QUANTUM ALGORITHMS:

HP:

$NIELSEN_1(f)$ or $NIELSEN_2(f)$ is effectively-realizable

TH:

$$Q_{\Phi} - C_M - \Delta_0^0 - \overset{\circ}{MAP} (\Sigma^{\star}, \Sigma^{\star}) \supset REC - \overset{\circ}{MAP} (\Sigma^{\star}, \Sigma^{\star})$$

PROOF:

$NIELSEN_1(f)$ and $NIELSEN_2(f)$ compute the the not-recursive function f ■

Theorem8.1.1 implies that assuming the preservation of the Church's Thesis one can infer the existence of a new superselection-rule:

Corollary 8.1.1

ON NIELSEN'S SUPERSELECTION RULE:
HP:

$$Q_{\Phi} - C_M - \Delta_0^0 - \overset{\circ}{MAP} (\Sigma^{\star}, \Sigma^{\star}) = REC - \overset{\circ}{MAP} (\Sigma^{\star}, \Sigma^{\star})$$

TH:

$$\hat{f} \text{ is not an observable } \quad \forall f \in REC - \overset{\circ}{MAP} (\Sigma^{\star}, \Sigma^{\star})$$

Remark 8.1.1

THE MATHEMATICAL PECULIARITY OF NIELSEN'S SUPERSELECTION RULE

Though, according to the general definition we gave in the remark5.2.5, Nielsen's one is a superselection-rule, its mathematical structure is rather peculiar

Let us analyze this issue starting from the Hilbert space axiomatizations of Quantum Mechanics and making w.r.t. it the same observations that in remark5.2.5 we made concerning the Noncommutative Axiomatizations:

axiom5.1.1 tells us that a pure state of a quantum-mechanical system is represented by a ray on an Hilbert space $\mathcal{H}$ but doesn't say that any ray on $\mathcal{H}$ represents a pure physical state of the system.

In the same way axiom5.1.2 tells us that an observable of a quantum-mechanical system is represented by a self-adjoint operator on $\mathcal{H}$ but it doesn't say that any self-adjoint operator on $\mathcal{H}$ represents a physical observable.

Now the usual superselection structure of a quantum system QS consists in the existence of a set $\{Q_i\}_{i \in I}$ of mutually commutating observables of the system, called its **superselection charges**, such that:

1. a self-adjoint operator O is an observable of the system iff:

$$[O\,,\,Q_i] \;=\; 0 \;\; \forall i \in I \tag{8.1.8.3}$$

2. a ray $|\psi><\psi|$ on $\mathcal{H}$ is a physical pure state of the system iff:

$$[|\psi><\psi|\,,\,Q_i] \;=\; 0 \;\; \forall i \in I \tag{8.1.8.4}$$

Introduced the following:

DEFINITION 8.1.3

SKEW INFORMATION OF $\rho \in \mathcal{D}(\mathcal{H})$ W.R.T. $a \in \mathcal{B}(\mathcal{H})$:

$$I_{skew}(\rho\,,\,a) \;:=\; \frac{1}{2}Tr([a\,,\,\rho^{\frac{1}{2}}]\,[\rho^{\frac{1}{2}}\,,\,a]) \tag{8.1.8.5}$$

one has then that [Wig95]:

Theorem 8.1.2

ON THE RULE OF SKEW INFORMATION W.R.T. SUPERSELECTION RULES:

HP:

$$\rho \,\in\, \mathcal{D}(\mathcal{H})$$

TH:

$$\rho \text{ is a physical state of QS } \Rightarrow \; I_{skew}(\rho\,,\,Q_i) \;=\; 0 \;\; \forall i \in I$$

The situation as to Nielsen's Superselection Rule is, instead, strongly different as it may be easily inferred observing that:

$$[\hat{I}\,,\,\hat{f}] \;=\; 0 \;\; \forall f \in MAP(\Sigma^{\star}\,,\,\Sigma^{\star}) \tag{8.1.8.6}$$

so that, whichever putatitive candidate superselection charge:

$$\hat{Q}_{Nielsen} \;=\; \sum_{\vec{x}\in\Sigma^{\star}}\sum_{\vec{y}\in\Sigma^{\star}} q_{Nielsen}(\vec{x},\vec{y})|\vec{x}><\vec{y}| \tag{8.1.8.7}$$

cannot satisfy the condition:

$$([\hat{Q}_{Nielsen}\,,\,\hat{f}] \;=\; 0) \;\Leftrightarrow\; f \in REC-\overset{\circ}{MAP}\,(\Sigma^{\star},\Sigma^{\star}) \tag{8.1.8.8}$$

Remark8.1.1 can lead to think that a suitable formalization of Nielsen's Superselection Rule requires some kind of effectivization of the compatibility-condition.

This requires the introduction of **relative recursivity**, i.e. of **recursivity w.r.t. oracles** [Odi89].

Given a partial function $f\,in\,\overset{\circ}{MAP}\,(\Sigma^{\star},\Sigma^{\star})$:

DEFINITION 8.1.4

CLASS OF PARTIAL FUNCTIONS RECURSIVE IN f (ON STRINGS) ($REC_f - \overset{\circ}{MAP}$ $(\Sigma^\star, \Sigma^\star)$):

the smallest class of partial functions:

1. containing the initial functions:

$$\mathcal{O}(x) := 0 \quad (8.1.8.9)$$
$$\mathcal{S}(x) := x+1 \quad (8.1.8.10)$$
$$\mathcal{I}_i^n(x_1, \cdots, x_n) := x_i \;\; i = 1, \cdots, n \,, \, n \in \mathbb{N} \quad (8.1.8.11)$$
$$f \quad (8.1.8.12)$$

2. closed under **composition**, i.e. the schema that given $\gamma_1, \cdots, \gamma_m, \psi$ produces:

$$\varphi(\vec{x}) := \psi(\gamma_1(\vec{x}), \cdots, \gamma_m(\vec{x})) \quad (8.1.8.13)$$

3. closed under **primitive recursion**, i.e. the schema that given ψ , γ produces:

$$\varphi(\vec{x}, 0) := \psi(\vec{x}) \quad (8.1.8.14)$$
$$\varphi(\vec{x}, y+1) := \gamma(\vec{x}, y, \phi(\vec{x}, y)) \quad (8.1.8.15)$$

4. closed under **unrestricted μ-recursion**, i.e. the schema that given ψ produces:

$$\varphi(\vec{x}) := \min\{y \,:\, (\psi(\vec{x}, z) \downarrow \; \forall z \leq y) \; and \; (\psi(\vec{x}, y) = 0)\} \quad (8.1.8.16)$$

   where $\varphi(\vec{x}) := \uparrow$ if there is no such function

Given a set $S \subseteq \Sigma^\star$:

DEFINITION 8.1.5

CLASS OF PARTIAL FUNCTIONS RECURSIVE IN S (ON STRINGS)

$$(REC_S - \overset{\circ}{MAP} \; (\Sigma^\star, \Sigma^\star)) := (REC_{\chi_S} - \overset{\circ}{MAP} \; (\Sigma^\star, \Sigma^\star)) \quad (8.1.8.17)$$

Given an n-ary predicate $R(x_1, \cdots, x_n)$ on $\Sigma^\star$:

DEFINITION 8.1.6

R IS RECURSIVE IN f:

$$\chi_R \in REC_f - MAP(\Sigma^\star, \Sigma^\star))$$

DEFINITION 8.1.7

R IS RECURSIVE IN S:

$$\chi_R \in REC_S - MAP(\Sigma^\star, \Sigma^\star))$$

A standard pictorial way of expressing the nature of the class of functions $REC_f - \overset{\circ}{MAP} (\Sigma^\star, \Sigma^\star)$ introduced by Alan Turing is to say that they are $C_\phi - computable$ w.r.t. the **oracle** f.

Definition1.1.5 and definition8.1.4 immediately imply the following:

Theorem 8.1.3

RECURSIVE ORACLES ARE USELESS:

$$REC_f - \overset{\circ}{MAP} (\Sigma^\star, \Sigma^\star) = REC - \overset{\circ}{MAP} (\Sigma^\star, \Sigma^\star) \ \forall f \in REC - \overset{\circ}{MAP} (\Sigma^\star, \Sigma^\star) \tag{8.1.8.18}$$

Relative-recursivity naturally induces a partial ordering over $\overset{\circ}{MAP} (\Sigma^\star, \Sigma^\star)$; given f , $g \in \overset{\circ}{MAP} (\Sigma^\star, \Sigma^\star)$:

DEFINITION 8.1.8

f IS TURING REDUCIBLE TO g ($f \leq_T g$):

$$f \in REC_g - \overset{\circ}{MAP} (\Sigma^\star, \Sigma^\star) \tag{8.1.8.19}$$

DEFINITION 8.1.9

f IS TURING EQUIVALENT TO g ($f \sim_T g$):

$$f \leq_T g \ and \ g \leq_T f \tag{8.1.8.20}$$

Since $\leq_T$ is a partial-ordering, $\sim_T$ is an equivalence relation so that we can introduce the following:

DEFINITION 8.1.10

TURING DEGREES ($\mathcal{D}_T$, $\leq_T$):

$$\mathcal{D}_T := \frac{\overset{\circ}{MAP} (\Sigma^\star, \Sigma^\star)}{\sim_T}$$

$$[f]_T \leq_T [g]_T := h \leq_T l \ \forall h \in [f]_T, \forall l \in [g]_T$$

Given then two functions $f, g \in \overset{\circ}{MAP} (\Sigma^\star, \Sigma^\star)$ we can introduce the following:

DEFINITION 8.1.11

EFFECTIVE COMMUTATOR OF $\hat{f}$ AND $\hat{g}$:

$$[\hat{f}\,,\,\hat{g}]_{EFF} \;:=\; \begin{cases} [\hat{f}\,,\,\hat{g}] & \text{if } f \sim_{T} g, \\ \uparrow & \text{otherwise.} \end{cases} \tag{8.1.8.21}$$

Let us introduce, furthermore, the following notion:

DEFINITION 8.1.12

EFFECTIVE SKEW INFORMATION OF $\rho \in \mathcal{D}(\mathcal{H})$ W.R.T. $a \in \mathcal{B}(\mathcal{H})$:

$$I_{skew}^{(EFF)}(\rho\,,\,a) \;:=\; \frac{1}{2} Tr([a\,,\,\rho^{\frac{1}{2}}]_{EFF}\,[\rho^{\frac{1}{2}}\,,\,a]_{EFF}) \tag{8.1.8.22}$$

Conjecture 8.1.1

It is possible that the situation as to Nielsen's Superselection Rule may then be recasted so that it resembles ordinary superselection rules in the following sense:

1. a necessary condition for the self-adjoint operator O on $\mathcal{B}(\mathcal{H}_{2}^{\star})$ to be an observable of the system is that:

$$[O\,,\,Q_{Nielsen}]_{EFF} \;=\; 0 \tag{8.1.8.23}$$

2. a a necessary condition for the ray $|\psi><\psi|$ on $\mathcal{H}_{2}^{\star}$ to be a physical pure state of the system is that:

$$[|\psi><\psi|\,,\,Q_{Nielsen}]_{EFF} \;=\; 0 \tag{8.1.8.24}$$

3. a necessary condition for a density matrix to be an observable is that:

$$I_{skew}^{(EFF)}(\rho\,,\,Q_{Nielsen}) \;=\; 0 \tag{8.1.8.25}$$

Let us now, anyway, move away the Hilbert space axiomatization originally assumed by Nielsen and let us analyze his argument in the general framework of the Noncommutative Axiomatization introduced in section5.1.

Given a quantum-mechanical system with observables' algebra A the algebra generated by the superselection rule is nothing but A'.

The hypothesis that all the superselection-charges commute among themselves may then be formalized as the following:

CONSTRAINT 8.1.1

CONSTRAINT OF COMMUTATIVE SUPERSELECTION RULES:

$$\mathcal{Z}(A) \;=\; A' \tag{8.1.8.26}$$

The previuosly discussed peculiarity of Nielsen's Superselection Rule is such that it doesn't fit in this picture as we will now show, starting from the following:

DEFINITION 8.1.13

NIELSEN-COMPUTABLE PART OF A:

$$REC_{Nielsen}(A) \;:=\; \{a \in A \,:\, Sp(a) \subseteq REC(\mathbb{C})\} \tag{8.1.8.27}$$

Given $a, b \,\in\, A_{p.s.d.}$:

DEFINITION 8.1.14

EFFECTIVE COMMUTATOR OF a AND b:

$$[a\,,\,b]_{EFF} \;:=\; \begin{cases} [a\,,\,b] & \text{if } Sp(a) \,\sim_T\, Sp(b), \\ \uparrow & \text{otherwise.} \end{cases} \tag{8.1.8.28}$$

Let us observe, anyway, that the generalization of definition8.1.14 for arbitrary spectrum requires the introduction of concepts lying outside the boundaries of $C_\Phi - C_M$-Recursion Theory, i.e. the definition of the Turing degrees in Σ^∞.

Demanding to the literature (e.g. the 5^{th}-chapter of [Odi89] or [Odi99b], [Sla99]) for details it will be sufficient here to say that exactly as definition8.1.7 allows to introduce the partial ordering of relative computability $\leq_T$ over $2^{\Sigma^\star}$ and the associated equivalence relation $\sim_T$ quotienting w.r.t. which Turing degrees on $2^{\Sigma^\star}$ are defined, the definition of a partial ordering relation of relative computability $\leq_T$ over 2^{Σ^∞} and the associated equivalence relation $\sim_T$ allows, by quotienting, to define Turing degrees over 2^{Σ^∞}, allowing to generalize the definition8.1.14 of the effective comutator from $A_{p.s.d.} \,\times\, A_{p.s.d.}$ to the whole $A \,\times\, A$.

Assuming that the Von Neumann algebra $A \subseteq \mathcal{B}(\mathcal{H})$ acts on the Hilbert space $\mathcal{H}$ one would be tempted to suspect that a suitable algebraic formalization of Nielsen's Superselection Rule requires the intoduction of the following notion

DEFINITION 8.1.15

EFFECTIVE COMMUTANT OF A:

$$(A')^{(EFF)} \;:=\; \{a \in A \,:\, [a,b]_{EFF} \,=\, 0 \;\; \forall b \in B(\mathcal{H})\} \tag{8.1.8.29}$$

Leaving aside, for the moment, Nielsen's Superselection Rule to which we will return in the next section, we would now to analyze an objection moved to Nielsen's analysis by Masanao Ozawa [Oza98a] showing its nullity.

Let us start from the following well-known results of Mathematical Logic [Odi89].

Theorem 8.1.4

ON THE REPRESENTABILITY IN ZFC:

assuming the consistence of the formal system of Zermelo-Fraenkel with the Axiom of Choice (ZFC) it follows that any function representable in ZFC is recursive

Theorem 8.1.5

ON THE UNDECIDABILITY OF THE CONSISTENCE OF ZFC FROM INSIDE

the statement << *ZFC is consistent* >> is undecidable in ZFC

Ozawa observes that any book, article, review on the recursive/not-recursive nature of Quantum Mechanics is written in mathematical language and, then, its statements are formulas of the formal system giving foundation to Mathematics, namely ZFC.

This would be true, obviously, also for any statement of the form:

$$s(QP, f) \ := \ << \textit{the quantum process } QP \textit{ computates the function } f >> \tag{8.1.8.30}$$

Ozawa's argument, then, runs as follow:

1. if s(QP,f) may be shown to be a physical truth, this implies that, properly effectively-codified as a numerical function, s(QP,f) must be representable in ZFC
2. inside ZFC, we cannot prove its consistence; however for our mathematical and physical work to be meaningful we must assume the consistence of ZFC
3. but then, for the theorem8.1.4, it follows that f is a recursive function

In other words, for Ozawa, the very fact that mathematically one expresses the computability of a function by some physical device implies its recursivity.

Both the argument and the general conclusion, however, do not appear to be correct: point 3 does not hold, in that it cannot be inferred from point2, after which we may only infer that s(QP,f) must be a recursive function.

Of course recursivity of s(QP,f) does not imply the recursivity of f and the whole argument fails.

Indeed Masanao Ozawa himself seems to realize in [Oza98c] that his reasoning that would lead to the automatic recursiveness of a C_M-map computed by a quantum computer must be wrong somewhere;

In section1 we already mentioned how Ozawa himself acts in [Oza98c] in order of leave preserved Church's Thesis; let us analyze the issue more precisely:

DEFINITION 8.1.16

CLASSICAL DETERMINISTIC TURING MACHINE ($M \ := \ (Q \, , \Sigma \, , \delta)$):

a classical device:

- whose hardware is composed by the following three elements:
    1. a **processor** consisting in a finite set Q of possible **internal states** containing two particular states: the **starting state** q_{START} AND THE **halting state** q_{HALT}

2. an infinite **tape** registering a binary-sequence $\bar{t} \in (\Sigma \bigcup \{-\})^{\infty}$ where $-$ is called the **empty symbol**
3. a **head** whose position on the tape is parametrized by a variable h, having the chance of moving on it left and right

- whose configuration space is:

$$S := Q \times (\Sigma \bigcup \{-\})^{\infty} \times \mathbb{Z} \tag{8.1.8.31}$$

where the state:

$$s(n) := (q_n , T_n , h_n) \tag{8.1.8.32}$$

is the configuration in which the **internal state** is q, the tape contains the message:

$$T_n = \{T_n(i) , i \in \mathbb{Z}\} \tag{8.1.8.33}$$

and the head is located on the h^{th} cell of the tape

- whose discrete-time dynamics is specified by a **local transition-function** $\delta : Q \times \Sigma \times \{-1, 0, 1\}$ through the following rule:

$$\delta(q_n , T_n(h_n)) = (q , a , d) \Rightarrow$$
$$q_{n+1} = q_n , h_{n+1} = h_n + d , T_{n+1}(i) = \begin{cases} T_n(i) & \text{if } i \neq h_n , \\ a & \text{otherwise.} \end{cases} \tag{8.1.8.34}$$

and by an **initial condition** of the form:

$$s(0) = (q_{START} , 0 , T_{INPUT}) \tag{8.1.8.35}$$

where T_{INPUT} obeys the following conditions:

$$T_{INPUT}(i) = - \ \forall i < 0 \tag{8.1.8.36}$$
$$\exists ! l(INPUT) \in \mathbb{N}_{+} : (T_{INPUT}(i) = - \ \forall i > l(INPUT) \tag{8.1.8.37}$$

where $l(INPUT)$ is called the **length** of the **input**, this last notion been defined as:

$$INPUT := \{T_{INPUT}(i) , i \in \{0, \cdots , l(INPUT)\}\} \tag{8.1.8.38}$$

At the first time the internal state gets the value q_{HALT} the output, constitued by a word of $\Sigma^{\star}$ surrounded by infinite $-$'s from left and right, is read on the tape.

Let us now pass to Quantum Computation, introducing the following:

DEFINITION 8.1.17

QUANTUM TURING MACHINE ($\hat{M} := (Q , \Sigma , \delta)$)
a quantum device:

- whose hardware is the same of that of a classical deterministic Turing machine with alphabet Σ and set of internal states Q
- whose Hilbert space $\mathcal{H}$ of quantum states is generated by the so called **computational basis** of $\hat{M}$:

$$\mathbb{E} := \{|q, h, T >, q \in Q , h \in Z , T \in \Sigma^{\star}\} \tag{8.1.8.39}$$

- whose discrete-time dynamics is, at the $(n+1)^{th}$ step, made of two sub-steps:
  1. application to the current state $|s(n) >$ of the unitary operator $\hat{U}$ on $\mathcal{H}$ identified by a suitable **local transition function** $\delta : Q^2 \times \Sigma^2 \times \{-1 , 0 , 1\} \mapsto \mathbb{C}$ through the relation:

$$\hat{U}|q , h , T > := \sum_{a \in \Sigma , q_2 \in Q , d \in \{-1,0,1\}} \delta(q_1 , T(h) , a , q_2 , d)|q_2 , h+d , T_h^a > \tag{8.1.8.40}$$

     where:

$$T_h^a(i) := \begin{cases} a & \text{if } i = h, \\ T(i) & \text{otherwise.} \end{cases} \quad a \in \Sigma , h \in \mathbb{Z} \tag{8.1.8.41}$$

  2. a measurement of the halting qubit:

$$\hat{q}_{HALT} := |q_{HALT} >< q_{HALT}| \tag{8.1.8.42}$$

Remark 8.1.2

ON LOCAL COMPUTATION:
Given a generic classical or quantum discrete-time dynamical system M:

DEFINITION 8.1.18

M IS LOCAL:
in each temporal step it may be altered only a **finite number** of **localized** cbits or qubits

Both classical and quantum Turing machines are local.

As to quantum Turing machines, their locality is essential to guarantee that one never goes out from $\mathcal{H}_2^{\star}$ with all the involved issues discussed in section5.1.

It may be finally worth to observe that , instead both the Rasetti, Castagnoli, Vincenti's [Vin92] and Nielsen's analysis about eventual violations of Church's Thesis by Quantum Mechanics involve **nonlocal quantum computations**

But here comes the following:

Theorem 8.1.6

OZAWA'S THEOREM:
HP:

$$Q_{\Phi} - C_M - \Delta_0^0 - \overset{\circ}{MAP}\,(\Sigma^{\star}, \Sigma^{\star}) \;=\; REC - \overset{\circ}{MAP}\,(\Sigma^{\star}, \Sigma^{\star})$$

$$\hat{M} \;:=\; (Q\,,\,\Sigma\,,\,\delta\,) \text{ quantum Turing machine}$$

TH:

$$\hat{M} \text{ physically possible } \;\Rightarrow\; Im(\delta) \;\subseteq\; REC(\mathbb{C})$$

PROOF:

Let us suppose, ad absurdum, that:

$$\exists\,(q_1\,,\,q_2\,,\,a_1\,,\,a_2\,,\,d) \;\in\; Q^2 \times \Sigma^2 \times \{-1, 0, 1\} \;: \qquad \delta(q_1\,,\,q_2\,,\,a_1\,,\,a_2\,,\,d) \;\in\; \mathbb{C} - REC(\mathbb{C})$$

One could then compute $|\delta(q_1\,,\,q_2\,,\,a_1\,,\,a_2\,,\,d)|$ as a relative frequency.
Since $REC(\mathbb{C})$ is a field, one has that:

$$\delta(q_1\,,\,q_2\,,\,a_1\,,\,a_2\,,\,d) \notin REC(\mathbb{C}) \;\Rightarrow\; |\delta(q_1\,,\,q_2\,,\,a_1\,,\,a_2\,,\,d)|^2 \notin REC(\mathbb{R}) \;\; \forall z \in \mathbb{C} \tag{8.1.8.43}$$

Since the digits' sequence of $|\delta(q_1\,,\,q_2\,,\,a_1\,,\,a_2\,,\,d)|^2$ may be seen as map on $\mathbb{N}$ the thesis immediately follows ■

8.2 From Church's Thesis to Pour El's Thesis

Marian B. Pour-El and Jonathan Ian Richards have [Ric89], [PE99] have developed a very interesting extension of Computable Analysis consisting in a Recursion Theory of Operators on Banach spaces.

Given a double sequence $\{x_{n,k} \in \mathbb{R}\}$ and an other sequence $\{x_n\}$ of real numbers such that:

$$\lim_{k \to \infty} x_{n,k} = x_n \forall n \in \mathbb{N} \tag{8.2.8.1}$$

DEFINITION 8.2.1

$\{x_{n,k}\}$ CONVERGES RECURSIVELY TO $\{x_n\}$ ($r - \lim_{k \to \infty} x_{n,k} = x_n$):

$$\exists e \in REC - MAP(\mathbb{N} \times \mathbb{N}, \mathbb{N}) :$$

$$(k > e(n, N) \Rightarrow \mid r_k - x \mid \leq \frac{1}{2^N}) \forall n \in \mathbb{N}, \forall N \in \mathbb{N} \tag{8.2.8.2}$$

Given a sequence of real numbers: $\{x_n \in \mathbb{R}\}_{n \in \mathbb{N}}$:

DEFINITION 8.2.2

$\{x_n \in \mathbb{R}\}_{n \in \mathbb{N}}$ IS RECURSIVE:

$$\exists \{r_{n,k} \in \mathbb{Q}\}_{n,k \in \mathbb{N}} : \mid r_{n,k} - x_n \mid \leq \frac{1}{2^k} \tag{8.2.8.3}$$

Given a sequence of complex numbers $\{z_n \in \mathbb{C}\}_{n \in \mathbb{N}}$:

DEFINITION 8.2.3

$\{z_n \in \mathbb{R}\}_{n \in \mathbb{N}}$ IS RECURSIVE:

$$\{\Re(z_n) \in \mathbb{R}\}_{n \in \mathbb{N}} \; and \{\Im(z_n) \in \mathbb{R}\}_{n \in \mathbb{N}} \text{ are recursive} \tag{8.2.8.4}$$

Remark 8.2.1

THE RECURSIVITY OF A SEQUENCE OF COMPLEX NUMBER IS STRONGER THAN THE RECURSIVITY OF ALL ITS ELEMENTS

Given a sequence $\{x_n\}$ of complex numbers, the fact that each element of the sequence is recursive, and can, conseguentially, be effectively approximated to any desired degree of precision by a computer program P_n given in advance, doesn't imply the recursivity of the whole sequence since there might not exist a way of combining the sequence of programs $\{P_n\}$ in an unique program P computing the whole sequence $\{x_n\}$.

The starting point of the Pour El-Richard's Theory is the notion of a **computability structure** on a Banach space B.

Owing to remark8.2.1 the definition of a computability structure on B is made through a proper specification of the computable sequences in B and not, simply, by the specification of a suitable set of recursive vectors.

DEFINITION 8.2.4

COMPUTABILITY STRUCTURE ON B:
a specification of a subset $\mathcal{S}$ of the set B^{∞} of all the sequences in B identified as the **set of the computable sequences on B** satisfying the following axioms:

AXIOM 8.2.1

ON LINEAR FORMS:
HP:

$$\{|x_n>\} \, , \{|y_n>\} \ \in \ \mathcal{S}$$

$$\{\alpha_{n,k}\} \, , \{\beta_{n,k}\} \text{ recursive double sequences in } \mathbb{C}$$

$$d \ \in \ REC - MAP(\mathbb{N}, \, \mathbb{N})$$

$$|s_n> := \sum_{k=0}^{d(n)} \alpha_{n,k}|x_k> + \beta_{n,k}|y_k>$$

TH:

$$\{|s_n>\} \in \mathcal{S}$$

AXIOM 8.2.2

ON LIMITS:
HP:

$$\{|x_{n,k}>\} \text{ recursive double sequence in B } \ : \ r - \lim_{k \to \infty} |x_{n,k}> = |x_n>$$

TH:

$$\{|x_n>\} \in \mathcal{S}$$

AXIOM 8.2.3

ON NORMS:
HP:

$$\{|x_n>\} \in \mathcal{S}$$

TH:

$$\{\| |x_n> \|\} \text{ is a recursive sequence in } \mathbb{R}$$

We will denote the set of all computability structures on a Banach space B by COMP-ST(B).

Remark 8.2.2

COMPUTABILITY STRUCTURE AS AN EFFECTIVIZATION OF BANACH'S STRUCTURE:
The idea behind definition8.2.4 lies in effectivizing the three ingredients a Banach space is made of: a vector space V, a norm on V and the condition of convergence of Cauchy's sequences.
Given a Banach space B endowed with a computability structure $\mathcal{S} \in COMP - ST(B)$:

DEFINITION 8.2.5

POUR EL - COMPUTABLE VECTORS OF B:

$$REC_{Pour\ El}(B\,,\mathcal{S}) \ := \ \{|\psi>\in B \ : \ (|\psi>,|\psi>,\cdots) \ \in \ \mathcal{S}\} \quad (8.2.8.5)$$

We will speak, more concisely, of $REC_{Pour\ El}(B$ when the assumed computability structure may be understood.

Unfortunately axiom8.2.1 definition8.2.4 doesn't provide the axiomatic definition of a unique structure for a Banach space B since in general, $card[COM - ST(B) \ > \ 1$.
This requires the existence of an additional condition by which the univocity condition can be obtained.
Given $\mathcal{S} \ \in \ COM - ST(B)$ on a Banach space B:

DEFINITION 8.2.6

EFFECTIVE GENERATING SET FOR B W.R.T. $\mathcal{S}$:
a computable sequence $\{|e_n>\} \in \mathcal{S}$ whose linear span is dense in B

DEFINITION 8.2.7

B IS EFFECTIVELY-SEPARABLE:

$$\exists \{|e_n>\} \in \mathcal{S} \text{ effective generating set of B w.r.t. } \mathcal{S} \tag{8.2.8.6}$$

Pour-El and Richards proved the following:

Theorem 8.2.1

THEOREM OF STABILITY:
HP:

$$\mathcal{S}_1 \, , \, \mathcal{S}_2 \; \in \; COMP - ST(B)$$

$$\{|e_n>\} \in \mathcal{S}_1 \cap \mathcal{S}_2 \text{ effective generating set}$$

TH:

$$\mathcal{S}_1 \; = \; \mathcal{S}_2$$

Example 8.2.1

COMPUTABILITY FOR CONTINUOUS FUNCTIONS:
Given $a \, , \, b \; \in \; REC - (\mathbb{R}) \; : \; a \; < \; b$ let us denote by C[a , b] the set of all continuous functions on the interval $(a \, , \, b)$.
C[a , b] is well known to be a Banach space w.r.t. the uniform norm:

$$\|f\| \; := \; \sup_{x \in [a \, , \, b]} |f(x)| \tag{8.2.8.7}$$

It is natural to assume that the sequence $\{x^n\}_{n \in \mathbb{N}}$ is computable.
Since it is then an effective generating set of C[a , b] for theorem8.2.1 it identifies a natural computability structure on it

Example 8.2.2

L^p-COMPUTABILITY

Given $a\,,\,b\ \in\ REC-(\mathbb{R})\ :\ a\ <\ b$ let us denote by $L^p[a,b]$, with $p\in[1\,,\,+\infty)$, the space of p-integrable functions, i.e.:

$$L^p[a,b]\ :=\ \{f\ :\ \int_a^b dx|f(x)|^p\ <\ +\infty\}\tag{8.2.8.8}$$

We will assume that $p\in REC(\mathbb{R})\bigcap[1\,,\,+\infty)$.

$L^p[a,b]$ is well-known to be a Banach space w.r.t. the norm:

$$\|f\|_p\ :=\ \int_a^b dx|f(x)|^p\tag{8.2.8.9}$$

It is natural to assume that the sequence $\{x^n\}_{n\in\mathbb{N}}$ is computable.

Since it is then an effective generating set of $L^p[a,b]$ for theorem8.2.1 it identifies a natural computability structure on it

Remark 8.2.3

THE COMPUTABILITY STRUCTURES OF QUANTUM INFORMATION: HILBERT SPACE FRAMEWORK

Given a quantum-mechanical system with Hilbert space of states $\mathcal{H}$ it is natural to assume that any complete basis of eigenvectors of an effectively measurable physical observable is an effective generating set of $\mathcal{H}$.

Since this is the case as to the qubits' string operators:

$$\hat{q}^n\ :=\ \bigotimes_{i=1}^{n}\hat{q}\ \ n\in\mathbb{N}\tag{8.2.8.10}$$

(where $\hat{q}$ is the qubit operator defined in eq.5.1.5.31) it is then natural to assume that the computational basis $\mathbb{E}_\star$ is an effective generating set of $\mathcal{H}_2^{\bigotimes\star}$ that, by theorem8.2.1, determines a computability structure on $\mathcal{H}_2^{\bigotimes\star}$ with which we will assume it to be endowed form here and beyond.

The situation is, instead strongly subtler as to $\mathcal{H}_2^{\bigotimes\infty}$ that, being **not separable**, is clearly also **non effectively separable**.

In our noncommutative framework, anyway, the basic objects of Quantum Information Theory are the noncommutative spaces $\Sigma_{NC}^{\star}$ and Σ_{NC}^{∞} of, respectively, qubits' strings and qubits' sequences, so that what would be relevant to us would be the identification of natural computability structure on these spaces.

The analysis on how this may be performed requires the introduction of some further notion of the Pour El Richards' Theory

Given an Hilbert space $\mathcal{H}$ endowed with a computability structure $\mathcal{S}\ \in COMP-ST(\mathcal{H})$ and a closed linear operator T on $\mathcal{H}$ [1] :

[1] We recall that an operator T on a Banach space B is called **closed** if its graph $\Gamma(T)\ :=\{(|\psi>,T|\psi>)\ :\ |\psi>\in HALTING(T)\}$ is a closed subset of $\mathcal{H}\times\mathcal{H}$.

DEFINITION 8.2.8

T IS EFFECTIVELY-DETERMINED:
it there exists $\{|e_n>\in \mathcal{S}$ such that:

1. $$\{(|e_n>, T|e_n>)\} \in \mathcal{S} \times \mathcal{S} \tag{8.2.8.11}$$

2. $$span\{(|e_n>, T|e_n>)\} \; is \; dense \; in \; \Gamma(T) \tag{8.2.8.12}$$

We will denote the set of all effectively-determined linear operators on $\mathcal{H}$ w.r.t. the computability structure $\mathcal{S}$ as $REC_{Pour\ El} - \mathcal{O}(\mathcal{H}\,, \mathcal{S})$ or simply as $REC_{Pour\ El} - \mathcal{O}(\mathcal{H})$ when the assumed computability structure may be understood.

Remark 8.2.4

EFFECTIVE DETERMINABILITY OF UNBOUNDED OPERATORS
for a bounded T operator on an Hilbert space $\mathcal{H}$ one has that:

$$HALTING(T) = \mathcal{H} \tag{8.2.8.13}$$

and the notion of effective determinability simply requires that the action of T on any Pour El-computable vector must be effectively determinable; for an unbounded operator, anyway, one has that:

$$HALTING(T) \subset \mathcal{H} \tag{8.2.8.14}$$

so that we must be able to effectively determine if T halts on the given Pour El-computable vector or not.

Remark 8.2.5

THE DOUBLE WAY INSIDE THE POUR EL-RICHARDS' THEORY OF SPECIFYING COMPUTABILITY ON A NONCOMMUTATIVE SPACE
Given a Von Neumann algebra $A \subseteq \mathcal{B}(\mathcal{H})$ acting on an Hilbert space $\mathcal{H}$ let us observe that in the Pour-El Richards' theory there exist two ways of specifying which elements of A are computable:

1. to assign a computability structure $\mathcal{S}_1 \in COMP - ST(\mathcal{H})$ on $\mathcal{H}$ and then to consider the effectively determined elements of it, resulting in $A \bigcap REC_{Pour\ El} - \mathcal{O}(\mathcal{H}, \mathcal{S}_1)$
2. to assign directly a computability structure $\mathcal{S}_2 \in COMP - ST(A)$

Remark 8.2.6

THE COMPUTABILITY STRUCTURES OF QUANTUM INFORMATION: NONCOMMUTATIVE FRAMEWORK

According to remark8.2.5 there exist two ways of specifying which elements of $\Sigma_{NC}^{\star}$ and Σ_{NC}^{∞}.

Let us start with $\Sigma_{NC}^{\star}$; we can:

1. consider the set $REC_{Pour\ El} - \mathcal{O}(\mathcal{H}\ ,\ \mathcal{S}_{natural})$, where $S_{natural} \in COMP-ST(\mathcal{H}_2^{\bigotimes \star})$ is the natural computability structure over $\mathcal{H}_2^{\bigotimes \star}$ induced by the computational basis $\mathbb{E}_{\star}$
2. to identify directly a natural computability structure over $\Sigma_{NC}^{\star}$

In this case, anyway, these two strategies **partially** collapse since a natural computability structure on $\Sigma_{NC}^{\star} = \mathcal{B}(\mathcal{H}_2^{\bigotimes \star})$ may be immediately derived from $\mathbb{E}_{\star}$ considering the associated system of projectors $\{\, |\vec{x} >< \vec{x}| \, : \, \vec{x} \in \Sigma^{\star} \,\}$.

The situation is, anyway, more difficult as to Σ_{NC}^{∞} since:

1. the nonseparability of $\mathcal{H}_2^{\bigotimes \infty}$ causes that, as we discussed in the remark8.2.3, the computational basis $\mathbb{E}_{\infty}$ doesn't induce a natural computability structure on it
2. since $\Sigma_{NC}^{\infty} \subset \mathcal{B}(\mathcal{H}_2^{\bigotimes \star})$ the specification of an effective generating basis of $\mathcal{H}_2^{\bigotimes \star}$ doesn't induce, passing to projectors, the specification of an effective generating set of Σ_{NC}^{∞}

The main results of the Pour El-Richard's Theory are the following theorems:

Theorem 8.2.2

ON COMPUTABILITY'S PRESERVATION:

HP:

$$X_1 \ , \ X_2 \text{ Banach spaces}$$

$$\mathcal{S}_i \ \in \ COMP - ST(X_i) \ \ i \ = \ 1, 2$$

$$\{|e_n>\} \text{ effective generating set of } X_1$$

$$T : X_1 \mapsto X_2 \text{ closed linear operator } \ : \quad \{|e_n >\} \ \subseteq \ D(T) \ and \ \{T|e_n >\} \in \mathcal{S}_2$$

TH:

$$T(REC_{Pour\ El}(X_1)) \subseteq REC_{Pour\ El}(X_2) \Leftrightarrow T\ is\ bounded \tag{8.2.8.15}$$

Example 8.2.3

UNCOMPUTABLE PROPAGATION OF WAVES:

Let us consider the Cauchy's problem for the wave-equation:

$$(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2} - \frac{\partial^2}{\partial t^2}) u = 0 \tag{8.2.8.16}$$

$$u(x, y, z, 0) = f(x, y, z) \tag{8.2.8.17}$$

$$\frac{\partial u}{\partial t}(x, y, z, 0) = 0 \tag{8.2.8.18}$$

Introduced the cubes:

$$D_l := \{|x| \leq l\,,\, |y| \leq l\,,\, |z| \leq l\} \;\; l \in \mathbb{R}_+ \tag{8.2.8.19}$$

the immediate multidimensional generalization of eq.8.2.1 allows to infer that there exist a natural computability structure on any Banach space $C(D_l)\, l \in \mathbb{R}_+$ (endowed with the uniform norm): that determined by the effective generating set $\{x^a y^b z^c \,:\, a, b, c \in \mathbb{N}\}$.

Since eq.8.2.8.16 describes waves travelling with unitary velocity, one has that for $t \in (0\,,\,2)$ the solution of the wave equation on D_1 doesn't depend on the initial values $u(x, y, z, 0)$ outside D_2.

Hence, we can look at the time-evolution operator $T_t\,,\, t \in (0\,,\,2)$:

$$u(\vec{x}, t) := T_t\, u(\vec{x}, 0) \;\; t \in (0\,,\,2) \tag{8.2.8.20}$$

as a linear operator from $C(D_2)$ to $C(D_1)$.

Explicitly:

$$(T_t f)(\vec{x}) = \int_{\partial S^{(2)}} [f(\vec{x} + t\vec{n}) + t(\vec{\nabla} f)(\vec{x} + t\vec{n}) \cdot \vec{n}]\, d\Omega(\vec{n}) \tag{8.2.8.21}$$

Owing to the gradient-term, $T_t\,,\, t \in (0\,,\,2)$ is unbounded; by theorem8.2.2 it follows that there exist a Pour-El-computable function $f\ in\ REC_{Pour\ El}(C(D_2))$ such that $T_1 f \notin REC_{Pour\ El}(C(D_2))$.

So $u(\vec{x}, 1)$ is not computable despite the computability of the initial condition $u(\vec{x}, 0)$.

Example 8.2.4

COMPUTABLE EUCLIDEAN EVOLUTION OF A QUANTUM FREE PARTICLE:

Let us consider the Cauchy's problem for the heat-equation:

$$\frac{\partial u}{\partial t} = (\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2})u \quad (8.2.8.22)$$

$$u(x,y,z,0) = f(x,y,z) \quad (8.2.8.23)$$

Let us introduce the hyper-cubes:

$$D_{\vec{a}} := \{\vec{x} \in \mathbb{R}^n \, : \, |x_i| \leq a_i \; i = 1, \cdots, n\} \;\; \vec{a} \in \mathbb{R}^n_+ \quad (8.2.8.24)$$

It should be now clear that a natural computability structure on any $C(D_{\vec{a}})$ is that identified by the effective generating set $\{\prod_{i=1}^n x_i^{n_i} \;\; n_i \in \mathbb{N}, \, i = 1, \cdots, n\}$.

Let us now consider the Banach spaces $C_0(\mathbb{R}^n)$ of all the continuous compactly-supported functions over $\mathbb{R}^n$ (endowed with the uniform norm): a computability structure on it is specified by the condition that a computable function $f \in C_0(\mathbb{R}^n)$ must be computable in any $C(D_{\vec{a}})$ and:

$$r - \lim_{|\vec{x}| \rightarrow \infty} f(\vec{x}) = 0 \quad (8.2.8.25)$$

The solution to eq.8.2.8.22 is given by the time-evolution operator $T_t : C_0(\mathbb{R}^3) \rightarrow C_0(\mathbb{R}^4) \; t \geq 0$:

$$(T_t f)(x,y,z) := \int_{\mathbb{R}^3} dx' dy' dz' \, K_t(x - x' \, , \, y - y' \, , \, z - z') \, f(x', y', z') \quad (8.2.8.26)$$

$$K_t(x,y,z) = (\frac{1}{4 \pi t})^{\frac{3}{2}} \exp(- \frac{x^2 + y^2 + z^2}{4 \, t}) \quad (8.2.8.27)$$

Since T_t is bounded it follows that, if the initial condition is computable, $u(x,y,z,t)$ remains computable for every time.

Let us observe, by the way, that eq.8.2.8.22 may be seen as the euclidean Schrödinger equation for a free-particle of mass $m = 2$.

The Hilbert space $\mathcal{H} = L^2(\mathbb{R}^3 \, , \, d\vec{x})$ may be endowed with a natural computability structure in the same way such a business was managed for $C_0(\mathbb{R}^3)$;

introduced the natural computability structure on $L^2(\mathbb{R}^3)$ again defining previously the computability on any $L^2(D_{\vec{a}})$ requiring that $\{\prod_{i=1}^n x_i^{n_i} \;\; n_i \in \mathbb{N}, \, i = 1, \cdots, n\}$ is an effective generating set and the defining a function $f \; in \; REC_{Pour \; El}(L^2(\mathbb{R}^3))$ if it belongs to any $COMP - ST(L^2(D_{\vec{a}}))$ and furthermore:

$$r - \lim_{|\vec{x}| \rightarrow \infty} f(\vec{x}) = 0 \quad (8.2.8.28)$$

$\{T_t\}_{t \in \mathbb{R}_+}$ may then be seen as the markovian strongly-continuous contraction semigroup [Tak94] describing the euclidean evolution of the $m = 2$ free particle preserving itself the computability of the initial wave-function.

The next key step of the Pour El - Richards' theory is the following:

Theorem 8.2.3

FIRST THEOREM ON THE COMPUTABILITY OF THE EIGENVALUES' SEQUENCE

HP:

$T : \mathcal{H} \rightarrow \mathcal{H}$ effectively-determined self-adjoint operator

TH:

$\exists \{\lambda_n\}_{n \in \mathbb{N}} \in COMP - ST(\mathcal{H})$, $A \subset \mathbb{N}$ *r.e.* such that:

1.

$$\lambda_n \in Sp(T) \, \forall n \in \mathbb{N} \tag{8.2.8.29}$$

2.

$$Sp(T) = \overline{\{\lambda_n\}_{n \in \mathbb{N}}} \tag{8.2.8.30}$$

3.

$$Eigenvalues(T) = \{\lambda_n \, , \, n \in \mathbb{N} - A\} \tag{8.2.8.31}$$

Theorem 8.2.4

SECOND THEOREM ON THE COMPUTABILITY OF THE EIGENVALUES' SEQUENCE

HP:

$(\mathcal{H} , \mathcal{S})$ Hilbert space endowed with the computability structure $\mathcal{S}$

$$\{\lambda_n\}_{n \in \mathbb{N}} \in COMP - ST(\mathbb{R}) \, , \, A \subset \mathbb{N} \, r.e.$$

TH:

$\exists T$ effectively-determined operator on $\mathcal{H}$:

1.

$$Sp(T) = Closure(\{\lambda_n\}_{n \in \mathbb{N}})$$

2.

$$Eigenvalues(T) \; = \; \{\lambda_n \; : \; n \in \mathbb{N} - A\}$$

3.

$$\{\lambda_n\}_{n \in \mathbb{N}} \, bounded \; \Rightarrow \; T \text{ can be chosen bounded}$$

Remark 8.2.7

WHEN EACH EIGENVALUE IS COMPUTABLE BUT THE EIGENVALUES' SEQUENCE IS NOT COMPUTABLE:

the meaning of theorem8.2.3 and theorem8.2.4 is, roughly speaking, that each single eigenvalue λ_n of an effectively-determined operator is computable by a suitable program P_n, but these program cannot be fit together to obtain a single program P computing the whole sequence $\{\lambda_n\}$.

Corollary 8.2.1

ON INCOMPUTABLE EIGENVALUES OF SHARP OBSERVABLES IN DISCRETE NONCOMMUTATIVE SPACES:

HP:

$$\mathcal{S} \in COMP - ST(\mathcal{H}) \; : \; \mathcal{H} \text{ Hilbert space}$$

TH:

$$\exists T \in (\mathcal{B}(\mathcal{H}))_{sa} \; : \; Eigenvalues(T) \notin \mathcal{S}$$

Corollary 8.2.2

COMPUTABILITY OF THE EIGENVALUES OF NONCOMMUTATIVE INFINITESIMALS IN DISCRETE NONCOMMUTATIVE SPACES:

HP:

$$\mathcal{S} \in COMP - ST(\mathcal{H}) \; : \; \mathcal{H} \text{ Hilbert space}$$

$$T \in \mathcal{C}(\mathcal{H})$$

TH:

$Eigenvalues(T)$ (suitably ordered) is a recursive sequence of $\mathbb{R}$

Finally, Pour El and Richard has proved the following:

Theorem 8.2.5

ON THE UNCOMPUTABLE EIGENVECTOR:

$\exists T$ compact, self-adjoint, effectively determined operator on $L^2([0,1])$ (endowed with the natural computability structure) such that:

$$Ker(T) \bigcap REC_{Pour\ El}(L^2([0,1])) \ = \ \emptyset$$

Example 8.2.5

FREE PARTICLE ON A INFINITE WELL AND ON THE CIRCLE:

Let us observe that, if not censored by a superselection-rule, one would look at the operator T of theorem8.2.5 as a physical observable for a free particle of mass $m = 2$ on the infinite well defined by the potential:

$$V(x) \ := \ \begin{cases} 0 & \text{if } x \in (0,1), \\ +\infty & \text{otherwise.} \end{cases} \tag{8.2.8.32}$$

whose hamiltonian is given by the self-adjoint operator on $L^2([0,1])$:

$$(H\,\psi)(x) \ := \ -(\frac{d^2}{dx^2}\psi)(x) \tag{8.2.8.33}$$

$$\psi(0) \ = \ \psi(1) \ = \ 0 \tag{8.2.8.34}$$

as well as for a particle moving on the circle $S^{(1)}$ whose Aharonov-Bohm coupling with the encircled magnetic flux tube $\theta \in [0\,,\,2\pi)$ selects the self-adjoint extension of the operator $-\frac{d^2}{dx^2}$ on $C_0^\infty([0,1])$ specified by the boundary condition (cfr. the 10^{th} chapter of [Sim75], the 23^{th} chapter of [Sch81] and the 11^{th} chapter of [Lan97]):

$$\psi(0) \ = \ e^{i\theta}\psi(1) \tag{8.2.8.35}$$

Up to this point we have discussed the Pour El-Richards' theory from the pure mathematical side.

As to the **physical relevance** of the **mathematical theory** of partial recursive functions, namely C_M-Classical Recursion Theory, it lies on:

1. the **mathematical observation** that all the different attempts of formalizing the notion of C_M-computability collapse to a unique notion
2. the **physical observation** of the **experimental verification** of a **physical principle**: Church's Principle

the eventual physical relevance of the **mathematical** Pour El-Richards' theory should lie on:

1. the **mathematical observation** of a collapse to a unique mathematical structure of all the attempts to formalize the notion of Computability of **objects** belonging to Linear Algebra on Banach Spaces

2. the **physical observation** of the **experimental verification** of a **physical principle** stating the nature of the objects **objects** of Linear Algebra on Banach Spaces that appear physically to be effectively computable w.r.t. the informal notion of effective computability

The satisfaction of the first of these two requirements has been explicitly invoked by Marian Pour El:

"Thus, we are able to achieve the intrinsic quality we associate with the notion of computability. The situation is reminiscent of the one in ordinary recursion theory, when the various definitions, proposed by Turing, Herbrand-Gödel, Church, Post and others, all intuitively convincing, were proposed to be equivalent. The notion of a computability structure acts as a unifying concept, since seemingly different definitions of computability, are, in fact, equivalent because of this unicity. Thus we have a "Church's Thesis" for the given Banach space"; from [PE99] at pag.450

The second point, strongly more relevant, leads us to analyze a weakened form of such a putative physical principle, concerning a unquestionably experimentally testable setting:

DEFINITION 8.2.9

POUR EL'S THESIS:

1. the set of the effectively-computable elements of $\mathcal{H}_2^{\bigotimes \star}$, w.r.t. to the informal notion of effective computability, is $REC_{Pour\ El}(\mathcal{H}_2^{\bigotimes \star}, \mathcal{S}_{natural})$, where $\mathcal{S}_{natural}$ is the natural computability structure introduced in the remark8.2.3

2. the set of the effectively-computable elements of $\Sigma_{NC}^{\star}$, w.r.t. to the informal notion of effective computability, is $REC_{Pour\ El}(\mathcal{H}_2^{\bigotimes \star}, \mathcal{S}_{natural})$, where $\mathcal{S}_{natural}$ is the natural computability structure over $\Sigma_{NC}^{\star}$ discussed in the remark8.2.6

3. the set of the effectively-computable elements of $CPU(\Sigma_{NC}^{\star})$, w.r.t. to the informal notion of effective computability, is $CPU(\Sigma_{NC}^{\star}) \bigcap REC_{Pour\ El} - \mathcal{O}(\mathcal{H}_2^{\bigotimes \star})$, namely the set of the effectively-determined channels over $\Sigma_{NC}^{\star}$.

A first thing to do, in order of evaluating whether the two mentioned conditions suggesting the assumption of Pour El's Thesis are really satisfied, is to compare it with Nielsen's Superselection Rule.

One has that:

Theorem 8.2.6

NIELSEN'S SUPERSELECTION RULE VERSUS POUR-EL'S THESIS:

$$REC_{Pour\ El}(\Sigma_{NC}^{\star}) = REC_{Nielsen}(\Sigma_{NC}^{\star}) \tag{8.2.8.36}$$

PROOF:

Let us consider a basis $\mathbb{E} := \{|e_n>\}_{n \in \mathbb{N}}$ of $\mathcal{H}_2^{\bigotimes \star}$ such that:

$$\mathbb{E} \notin COMP - ST(\mathcal{H}_2^{\bigotimes \star}) \tag{8.2.8.37}$$

Given a recursive function $f \in REC - MAP(\mathbb{N}, \mathbb{N})$ one has that:

$$\hat{f} := \sum_{n=0}^{\infty} f(n)|e_n >< e_n| \in REC_{Nielsen}(\Sigma_{NC}^{\star}) \tag{8.2.8.38}$$

though $\hat{f}$ cannot be obtained as an effective linear combination of the vectors of the computational basis ■

Theorem8.2.6 suggest a negative feature of Nielsen's approach to characterize the effectively computable elements of a noncommutative space: to take into account only the spectrum is not sufficient, since an operator can have recursive eigenvalues w.r.t. an effectively-nondeterminable basis.

While the Nielsen's approach is more compelling from a physical ground, arising from the anlaysis of the constraints required in order Quantum Computation doesn't violate Church's Thesis, the Pour El-Richards' Theory is, conseguentially, more refined from a mathematical side.

As it happened in the thirties for $C_{\Phi} - C_M$-computability, we have to expect that the right answers will arise comparing all the different pioneering attempts.

Among these it must be cited Robin Havea's work on Constructive Operators' Theory [Hav00]:

though, as it has been strongly stressed by Douglas S. Bridges, the link between **Constructive Mathematics** and **Computability Theory** is rather subtle since if it is true that Constructive Mathematics is based on the assumption:

$$EXISTENCE = COMPUTABILITY \tag{8.2.8.39}$$

it is also true that the meaning of **computability** at the r.h.s. of eq.8.2.8.39 is something more radical than **recursive**, as it is dramatically shown by Bridge's example concerning the recursive function $f : \mathbb{N} \rightarrow \mathbb{N}$:

$$f(n) := \begin{cases} 0 & \text{if } 2^{\aleph_0} = \aleph_1, \\ 1 & \text{otherwise.} \end{cases} \tag{8.2.8.40}$$

that nobody would consider constructive owing to Cohen's celebrated independence result [Bri98], yet such a link does exist.

It is funny, with this respect, that the Constructive Theory of Von Neumann's algebras is linked with a radicalization of the meaning of the term **constructive** in the Constructive Field Theory's program [Jaf87], [Jaf00].

The analysis on the concept of quantum algorithm of the previous sections should allow to charaterize the notion of quantum algorithmic randomness as ownership of all the quantum algorithmic typical properties in the following way:

given an algebraic probability space $APS := (A , \omega)$:

DEFINITION 8.2.10

COMMUTATIVE LAWS OF RANDOMNESS OF APS:

$$\mathcal{L}^{C}_{RANDOMNESS}(APS) \ := \ \{p \in \mathcal{P}^{TYPICAL}_{C} \ Q_{\Phi} - \Delta^{0}_{0}\} \tag{8.2.8.41}$$

DEFINITION 8.2.11

NONCOMMUTATIVE LAWS OF RANDOMNESS OF APS:

$$\mathcal{L}^{NC}_{RANDOMNESS}(APS) \ := \ \{p \in \mathcal{P}^{TYPICAL}_{NC} \ Q_{\Phi} - \Delta^{0}_{0}\} \tag{8.2.8.42}$$

It should then be finally possible to define $RANDOM(\Sigma_{NC}^{\infty})$ as the subset of all the elements of Σ_{NC}^{∞} possessing all the laws of randomness of $(\Sigma_{NC}^{\infty} , \tau_{unbaised})$.

8.3 Quantum Algorithmic Information Theory as a particular case of the abstract Uspensky's approach

We saw in section6.2 how Karl Svozil arrived to introduce the idea of the quantum algorithmic information of the qubits' strings' Hilbert space w.r.t. a quantum computer Q.

The consistence of such an approach lies on the existence of a quantum analogue of theorem1.2.9 allowing to get rid of dependence from the particular quantum computer Q.

This consideration suggests that the delineation of Quantum Algorithmic Information Theory should be made realizing it as a particular instance of the Uspensky's abstract approach introduced in lksection1.2.

The problem consists, clearly, in identifying:

- a suitable aggregate $A_1 := (X_1 , R_1)$
- a suitable metric aggregate $A_2 := (X_2 , R_2 , \mu)$
- a suitable universe of description of A_2 through $A_1 : \mathcal{R} \in \mathcal{D}(A_1 , A_2)$

The key point of such an approach is that it structurally founds Quantum Algorithmic Information Theory, from the beginning, on:

1. the mathematical characterization of the concept of **quantum algorithm**
2. the condition that there exist an **optimal quantum algorithm**

Since, as we saw in section1.6, even in the classical case the applicability of the Uspensky's abstract approach to sequences is strongly doubtful, also in the quantum case we will apply it only for strings.

We will assume, conseguentially, that:

$$X_1 := \Sigma_{NC}^{\star} \quad (8.3.8.1)$$

$$X_2 := \Sigma_{NC}^{\star} \quad (8.3.8.2)$$

The next key step consists in assuming that the **concordance relations** $\mathcal{R}_1$ and $\mathcal{R}_2$ are such that that the **modes of descriptions** on $\Sigma_{NC}^{\star}$ are the **channels** on it, i.e.:

$$\mathcal{D}(A_1 , A_2) = CPU(\Sigma_{NC}^{\star}) \quad (8.3.8.3)$$

Remark 8.3.1

QUANTUM ALGORITHMIC INFORMATION VERSUS QUANTUM REVERSIBLE COMPUTATION

Let us observe that, whichever choice we adopt for the point measure μ (e.g. the norm on $\Sigma_{NC}^{\star}$ or some other candidate induced on it by duality from a distance on S($\Sigma_{NC}^{\star}$) such as a the noncommutative geodesic distance w.r.t. some noncommutative riemannian metric) one has that the resulting notion of quantum algorithmic information given by our particular instance of definition1.2.5) is not-trivial iff also logically-non reversible modes of descriptions, in the sense of definition7.3.24, are taken into account.

This immediately leads to the following:

CONSTRAINT 8.3.1

NONTRIVIALITY'S CONSTRAINT ON QUANTUM ALGORITHMIC INFORMATION THEORY:

$$\mathcal{R} \nsubseteq AUT(\Sigma_{NC}^{\star}) \tag{8.3.8.4}$$

The assumption of constraint8.3.1 implies in particular that:

Corollary 8.3.1

QUANTUM ALGORITHMIC INFORMATION THEORY IS MEANINGFUL ONLY FOR OPEN SYSTEMS:

$$\mathcal{R} \nsubseteq INN(\Sigma_{NC}^{\star}) \tag{8.3.8.5}$$

Corollary8.3.1 tells us that Quantum Algorithmic Information Theory is nontrivial only if we allow description methods corresponding, by axiom5.2.3, to **open dynamics**.

As to the classical case, theorem1.2.2, was the first of a set of theorems showing that certain quantities of Classical Algorithmic Information Theory are meaningful only by effectivizing some notion.

As we saw in section7.4 with regard to theorem3.2.1, the translation of these results to the quantum domain is far from obvious.

In this case, anyway, it seems to us that the reasoning lying behind theorem3.2.1 may be suitably translated concluding that Algorithmic Information Theory w.r.t. $CPU(\Sigma_{NC}^{\star})$ is not meaningful.

Requiring the effectiveness of the description modes, one is then led to assume as universe of description the set of the quantistically-computable channels over the noncommutative space of qubits' strings:

$$\mathcal{R} := Q_{\Phi} - NC_{M} - \Delta_{0}^{0} - CPU(\Sigma_{NC}^{\star}) \tag{8.3.8.6}$$

In particular, assuming Pour-El's thesis, such an assumption means that:

$$\mathcal{R} = CPU(\Sigma_{NC}^{\star}) \bigcap REC_{Pour\ El} - \mathcal{O}(\mathcal{H}_{2}^{\bigotimes \star}) \tag{8.3.8.7}$$

The next step open problem consists in proving that Algorithmic Information Theory is meaningful w.r.t. $Q_{\Phi} - NC_{M} - \Delta_{0}^{0} - CPU(\Sigma_{NC}^{\star})$.

Remark 8.3.2

C_Φ-QUANTUM ALGORITHMIC INFORMATION THEORY VERSUS $Q_M - C_\Phi$-CLASSICAL ALGORITHMIC INFORMATION THEORY

In section1.1 we observed, on analyzing the $cell_{22}$ of the diagram1.1.1, that Church's Thesis doesn't imply that the answers to the question:

what is computable?

concerning the $cell_{12}$ and the $cell_{22}$ of the diagram1.1.1 must be equal.

Denoting with Q_M-computability the kind of NC_M-computability concerning noncommutative spaces and channels over them, such an observation implies, in particular, that Church's Thesis does not imply that $C_\Phi - Q_M$-computability is equal to $Q_\Phi - Q_M$-computability.

This is particularly important to our purposes since if Algorithmic Information Theory is defined in terms of Uspensky's abstract approach, the condition:

$$C_\Phi - Q_M - \Delta_0^0 \neq Q_\Phi - Q_M - \Delta_0^0 \qquad (8.3.8.8)$$

is necessary and sufficient so that Quantum Algorithmic Information Theory doesn't collapse to the Classical Algorithmic Information Theory of Q_M-quantities.

Such a collapse occurs, instead, assuming Pour-El's thesis, from which the violation of eq.8.3.8.7 may be immediately inferred.

Chapter 9

Quantum algorithmic randomness and The Law of Excluded Quantum Gambling Systems

9.1 On the frequentistic interpretation of Quantum Probability

On introducing the concept of a **quantum ensemble**, i.e. of a statistical ensemble consisting of many individual quantum systems $S_1 , \ldots , S_n$, in the section 4.1 *"The fundamental basis of the statistical theory"* of his basic 1932's book, Von Neumann explicitely says that:

> *"Such ensembles, called collectives, are in general necessary for establishing probability theory as the theory of ferquencies. They were introduced by R. v. Mises, who discovered their meaning for probability theory, and who built up a complete theory on this foundation" note 156 of [Neu83]*

Indeed, in 1932, Von Mises' axiomatization of (classical) probability was the only one available on the market, the now standard Kolmogorovian , measure-theoretic axiomatization [Kol56] not been appeared yet.

As we saw in section5.3, on discussing the meaning of Bell's Theorem, the irreducibility of Noncommutative Probability Theory to the Commutative one may be seen, in an equivalent way, as the impossibility, in general, of describing noncommutative random variables on a **single classical probability space**, owing to the lack of operational meaning of the joint moments.

With this respect Von Neumann thought to be able to mantain the frequentistic interpretation of quantum probability inherited from the frequentistic interpretation of classical probability getting around such a problem, in the following way:

"Even if two or more quantities R, S in a single system are not simultaneously measurable, their probability distribution in a given ensemble $[S_1 , \cdots S_N]$ *can be obtained with arbitary accuracy if N is sufficiently large. Indeed, with an ensemble of N elements it suffices to carry out the statistical ispections, relative to the distribution of values of the quantity R, not on all N elements* $[S_1 , \cdots S_N]$*, but on any subset of M (* $\leq N$ *) elements, say* $[S_1 , \cdots S_M]$*, provided that M, N are both large, and that M is very small compared to N. Then only the M/N-th part of the ensemble is affected by the changes with result from the measurement. The effect is an arbitrary small one if M/N is chosen small enough - which is possible for sufficiently large N, even in the case of large M.* $\cdots$*. In order to measure two (or several) quantities R,S simultaneously, we need two sub-ensembles, say* $[S_1 , \cdots S_M]$, $[S_{M+1} , \cdots S_{2\,M}]$ $(2M \leq N)$ *of such a type that the first is employed obtaining the statistics of R, and the second is obtaining those of S. The two measurements therefore do not disturb each other, although they are performed in the same ensemble* $[S_1 , \cdots S_N]$ *and they can change this ensemble only by an arbitrarily small amount, if* $2M/N$ *is sufficiently small, which is possible for sufficiently large N even in the case of large M* $\cdots$*". From the section4.1 of [Neu83]*

As it has been lucidly observed by Miklos Redei [Red01], implicit in this reasoning is the assumption that the subensembles are representative of the larger ensemble in the sense that the relative frequency of every attribute is the same both in the original and in the subensemble.

This not-trivial assumption is nothing but the requirement that the a **quantum ensemble**, as a collective, statisfies the **Law of stability of Statistic Relative Frequencies** and the **Law of Excluded Quantum Gambling Strategies**, i.e., respectively, the Axiom of Covergence, namely axiom4.1.1, and the Axiom of Randomness, namely axiom4.1.2, of Von Mises's frequentistic axiomatization of Classical Probability Theory, or some quantum analogue of them.

As Miklos Redei observes:

"Von Neumann does not elaborate on the details and significance for his interpretation of quantum probability of the randomness requirement; apparentely hid did not see any problem with taking advantage of this not trivial (and controversial) feature of Von Mises' interpretation." From [Red01]

One could then think of formalizing a frequentistic axiomatization of Quantum Probability explicitely formulating quantum analogues of the Axiom of Von Mises' Axiom of Convergence an the Axiom of Randomness, some way in the spirit of the Hartle's and Lesniewski-Coleman's analysis discussed in section6.1.

The corner-stone of such an axiomatization would be, clearly, the Law of Excluded Quantum Gambling Systems, formalizing the not-existence of winning gambling strategies in suitable quantum casinos.

It must be observed, anyway, that the link of such a frequentistic formulation of Noncommutative Probability with the noncommutative-measure theoretic one would be far from obvious, owing to the fact that the space of states S(A) over a noncommuative space A is not a Choquet's simplex, so that states on A has multiple extremal decomposition.

We saw in chapter4 that, from inside the usual measure-theoretic foundation of Classical Probability Theory, Von Misese's theory results in the characterization of a notion of classical algorithmic randomness, namely Church's randomness, weaker than the Martin Löf-Solovay-Chaitin's one.

In an analogous way, our attitude in the next sections will consist in attempting to extract the more possible information on the set $RANDOM(\Sigma_{NC}^{\infty})$ of random qubits' sequences.

9.2 Different kind of quantum casinos

Quantum Decision Theory was invented by P.A. Benioff [Ben72] and extensively developed by C.W. Helstrom [Hel76] [Hol99]. A renewed interest in such field has recentely grown up in the framework of Quantum Game Theory [Lew99], [Bou00].

As in the classical case we can always interpret a quantum decision problem as a quantum gambling situation, with the utility function playing the rule of the payoff.

Let us consider a gambler going to a ***Quantum Casino*** in which the croupier, at each turn n , **throws a quantum coin**.

Such a situation may be interpreted in different ways giving rise to different types of *Quantum Casinos*.

DEFINITION 9.2.1

FIRST KIND QUANTUM CASINO:
a quantum casino specified by the following rules:

1. At each turn n the croupier extracts with unbiased probability a **pure state** $|\psi>(n) \in \mathcal{H}_2$, where $\mathcal{H}_2$ is the **one qubit Hilbert space**.

2. Before each quantum coin toss the gambler can decide, according to a **direct gambling strategy**, among the following possibilities:

   - to bet one fiche on a vector $|\alpha> \in \mathcal{H}_2$
   - not to bet at the turn

3. If he decides for the first option it will happens that:

   - he wins a fiche if the distance among $|\psi>(n)$ and $|\alpha>$ is less or equal to fixed quantity ϵ_{Casino}.
   - he loses the betted fiche if the distance among $|\psi>(n)$ and $|\alpha>$ is greater than ϵ_{Casino}

But it is also possible to see the result of a quantum coin toss as a **mixed state**, resulting in the following:

DEFINITION 9.2.2

SECOND KIND QUANTUM CASINO:
a quantum casino specified by the following rules:

1. At each turn n the croupier extracts with unbiased (quantum) probability a density matrix ρ_n on the **one qubit alphabet** $\mathcal{H}_2$.

2. Before each quantum coin toss the gambler can decide, according to a **direct gambling strategy**, among the following possibilities:

- to bet one fiche on a density matrix $\sigma \in \mathcal{H}_2$
- not to bet at the turn

3. If he decides for the first option it will happens that:
   - he wins a fiche if the distance among σ and ρ_n is less or equal to fixed quantity ϵ_{Casino}
   - he loses the betted fiche if the distance among σ and ρ_n is greater than ϵ_{Casino}

To complete the definition of first and second kind quantum casinos (definition9.2.1 and definition9.2.2) we have to clarify:

1. which is the adopted notion of distance among states on an Hilbert space $\mathcal{H}$.
2. what we mean by a **direct gambling strategy**

In section5.2 we saw that, despite the noncommutative-information-geometric strategy of considering the noncommutative geodesic distance w.r.t. a suitable spectral triple, there exist two natural notions of distance among two density operators on an Hilbert space, the **quantum trace distance** and the **quantum angle distance**, introduced respectively by definition5.2.33 and definition5.2.43.

Fortunately they are qualitatively equivalent [Chu00]:

Theorem 9.2.1

QUALITATIVE EQUIVALENCE OF TRACE AND ANGLE DISTANCES ON STATES:

$$1 - F(\rho_1 , \rho_2) \ \leq \ D(\rho_1 , \rho_2) \ \leq \ \sqrt{1 - F(\rho_1 , \rho_2)} \ \ \forall \rho_1 , \rho_2 \ \in \ \mathcal{D}(\mathcal{H}_2) \quad (9.2.9.1)$$

and, conseguentially, it doesn't matter which of them we use in order to define a **second kind Quantum Casino**.

For the case we are interested to in which the underlying Hilbert space is the **one qubit Hilbert space** $\mathcal{H}_2$, the adoption of the **trace distance** may be preferred since it satisfies the following:

Theorem 9.2.2

QUANTUM TRACE DISTANCE IN TERMS OF THE BLOCH SPHERE:

$$D(Bloch(\vec{r}_1), Bloch(\vec{r}_2)) \ = \ \frac{\|\vec{r}_1 - \vec{r}_2\|}{2} \ \ \forall \vec{r}_1, \vec{r}_2 \in Ball^{(2)} \qquad (9.2.9.2)$$

with:

DEFINITION 9.2.3

BLOCH SPHERE BIJECTION:
$Bloch : Ball^{(2)} \rightarrow \mathcal{D}(\mathcal{H}_2)$:

$$Bloch(\vec{r}) := \frac{\mathbb{I} + \vec{r} \cdot \vec{\sigma}}{2} \tag{9.2.9.3}$$

where $Ball^{(2)} := \{\vec{r} \in \mathbb{R}^3 : \|\vec{r}\| \leq 1\}$ is the unit-radius 2-ball while $\vec{\sigma} := \begin{pmatrix} \sigma_x \\ \sigma_y \\ \sigma_z \end{pmatrix}$ is the vector of the Pauli matrices.

Let us observe that the extraction with unbiased probability of an element of $\mathcal{D}(\mathcal{H}_2)$ involved in the definition9.2.2 may be reconducted, through the definition9.2.3, to the extraction of a value of uniform-distributed random point on the unit radius 2-ball $Ball^{(2)}$.

Let us, now, clarify what we mean by a **direct gambling strategy**.

To make his decision at the n^{th} turn, the gambler can take in consideration the result of all the previous n-1 quantum coin tosses.

He can do this in two different ways:

- he can think on the **direct products** of the previous outcomes; we will call such a strategy a **direct gambling strategy**
- he can think on the **tensor products** of the previous outcomes; we will call such a strategy a **tensor gambling strategy**

In a **first kind** and **second kind Quantum Casino** the gambler has to play according to a **direct gambling strategy**.

We will introduce, later a **third kind of Quantum Casino**, in which the gambler has to play according to a **tensor gambling strategy**.

The **direct gambling strategies** according to which the gambler plays in a **first kind** and **second kind Quantum Casino** will be called, respectively, **first kind** and **second kind quantum gambling strategies** and defined in the following way:

DEFINITION 9.2.4

FIRST KIND QUANTUM GAMBLING STRATEGY:
$S : \mathcal{H}_2^{\star} \stackrel{\circ}{\rightarrow} \mathcal{H}_2$

DEFINITION 9.2.5

SECOND KIND QUANTUM GAMBLING STRATEGY:
$S : \mathcal{D}(\mathcal{H}_2^{\star}) \stackrel{\circ}{\rightarrow} \mathcal{D}(\mathcal{H}_2)$

Let us now consider the sets $\mathcal{H}_2^{\infty}$ and $\mathcal{D}(\mathcal{H}_2)^{\infty}$ of sequences of, respectively, **one qubit vectors** and **one qubit density matrices**.

Our objective is to characterize two subsets $\mathcal{QC}ollectives^{1} \subset \mathcal{H}_{2}^{\infty}$ and $\mathcal{QC}ollectives^{2} \subset \mathcal{D}(\mathcal{H}_{2})^{\infty}$, that we will call, respectively, **first kind quantum collectives** and **second kind quantum collectives**, defined by the condition of satisfying Von Mises's axiom4.1.2 when the class of the **first kind quantum admissible gambling strategies** $\mathcal{QS}trategies_{admissible}(\mathcal{QC}ollectives^{1})$ and the class of the **second kind quantum admissible gambling strategies** $\mathcal{QS}trategies_{admissible}(\mathcal{QC}ollectives^{2})$ are chosen according to a proper algorithmic-effectiveness characterization specular to the classical one of eq.4.2.4.8.

We arrive, conseguentially, to the following definitions:

DEFINITION 9.2.6

FIRST KIND QUANTUM COLLECTIVES:

$\mathcal{QC}ollectives^{1} \subset \mathcal{H}_{2}^{\infty}$ induced by the axiom4.1.2 and the assumptions that the **first kind quantum admissible gambling strategies** are nothing but the **quantum algorithms** on $\mathcal{H}_{2}^{\infty}$:

$$\mathcal{QS}trategies_{admissible}(\mathcal{QC}ollectives^{1}) := Q_{\Phi} - \Delta_{0}^{0} - \overset{\circ}{MAP} (\mathcal{H}_{2}^{\infty}) \quad (9.2.9.4)$$

DEFINITION 9.2.7

SECOND KIND QUANTUM COLLECTIVES:

$\mathcal{QC}ollectives^{2} \subset \mathcal{D}(\mathcal{H}_{2})^{\infty}$ induced by the axiom4.1.2 and the assumption that the **second kind quantum admissible gambling strategies** are nothing but the **quantum algorithms** on $\mathcal{D}(\mathcal{H}_{2})^{\infty}$:

$$\mathcal{QS}trategies_{admissible}(\mathcal{QC}ollectives^{2}) := Q_{\Phi} - \Delta_{0}^{0} - \mathcal{D}(\mathbb{H}_{2})^{\infty}) \quad (9.2.9.5)$$

Let us finally introduce Third Kind Quantum Casinos.

Let us finally introduce the following notions:

DEFINITION 9.2.8

ALGEBRAIC QUANTUM COIN: a **quantum random variable** on the **quantum probability space** $(M_{2}(\mathbb{C}) , \tau_{2})$

DEFINITION 9.2.9

THIRD KIND QUANTUM CASINO:

a quantum casino specified by the following rules:

1. At each turn n the croupier throws an **algebraic quantum coin** A_{n} obtaining a value $a_{n} \in \Sigma_{NC}$
2. Before each algebraic quantum coin toss the gambler can decide, by adopting a **quantum gambling strategy**, among the following possibilities:
   - to bet one fiche on an a letter $b \in \Sigma_{NC}$

- not to bet at the turn

3. If he decides for the first option it will happens that:

    - he wins a fiche if the distance among a_n and b $d(a_n, b) := \|a_n - b\|$ is less or equal to a fixed quantity ϵ_{Casino}.
    - he loses the betted fiche if the distance among a_n and a $d(a_n, b) := \|a_n - b\|$ is greater than ϵ_{Casino}

where the adoption of a **tensor gambling strategy** is formalized in terms of the following notion:

DEFINITION 9.2.10

THIRD KIND QUANTUM GAMBLING STRATEGY:
$S : \Sigma_{NC}^{\star} \stackrel{\circ}{\rightarrow} M_2(\mathbb{C})$

The concrete way in which the gambler applies, in every kind of Quantum Casino, the chosen strategy S is always the same:

- if S doesn't halt on the **previous game history** he doesn't bet at the next turn
- if S halts on on the past game history he bets S(previous game history)

Lets us denote by $\bar{a} \in \Sigma_{NC}^{\infty}$ the occured quantum sequence of qubits and with $\vec{a}(n) := a_1 \bigotimes \cdots \bigotimes a_n \in \Sigma_{NC}^{n}$ its **quantum prefix of length n**, i.e. the quantum string of the results of the first n quantum coin tosses.

Example 9.2.1

BETTING ON PAULI MATRICES CHOOSING ACCORDING TO THE HEIGHT OF THE UNBIASED QUANTUM PROBABILITY MEASURE

Let us consider the following **third kind quantum gambling strategy**:

$$S(\vec{a}(n)) := \begin{cases} \uparrow & \text{if } \vec{a}(n) = \lambda \ , \\ \sigma_x & \text{if } P_{unbiased}(\vec{a}(n)^{\dagger}\vec{a}(n)) \ = \ 0, \\ \sigma_y & \text{if } P_{unbiased}(\vec{a}(n)^{\dagger}\vec{a}(n)) < 2^n, \\ \sigma_z & \text{otherwise.} \end{cases} \tag{9.2.9.6}$$

where λ denotes the empty quantum string.

Let us imagine that the results of the first three quantum coin tosses are:

$$a(1) \ = \ \begin{pmatrix} 5.21295 - 0.543424I & -5.83373 - 1.51207I \\ -5.72507 + 5.64286I & 0.264194 - 5.36408I \end{pmatrix}$$

$$a(2) \ = \ \begin{pmatrix} -2.21604 - 8.29818I & 2.29687 - 9.22925I \\ -7.10612 + 4.25443I & -8.19842 + 6.03258I \end{pmatrix}$$

$$a(3) \;=\; \begin{pmatrix} 9.80519 - 7.0523I & -7.72367 - 6.40421I \\ -0.227234 + 7.87254I & 6.36604 + 6.81784I \end{pmatrix}$$

so that:

$$\vec{a}(1) \;=\; \begin{pmatrix} 5.21295 - 0.543424I & -5.83373 - 1.51207I \\ -5.72507 + 5.64286I & 0.264194 - 5.36408I \end{pmatrix}$$

$$\vec{a}(2) \;=\; a(1) \bigotimes a(2) \;=$$

$$\begin{pmatrix} -16.0615 - 42.0538I & 6.95806 - 49.3598I & 0.380344 + 51.7601I & -27.3546 + 50.3679I \\ -34.7319 + 26.0397I & -39.4597 + 35.9027I & 47.8881 - 14.0742I & 56.949 - 22.7959I \\ 59.5124 + 35.0029I & 38.9296 + 65.799I & -45.0976 + 9.69467I & -48.8996 - 14.7589I \\ 16.6759 - 64.4557I & 12.8955 - 80.7994I & 20.9437 + 39.2418I & 30.1933 + 45.5707I \end{pmatrix}$$

$$\vec{a}(3) \;=\; a(1) \bigotimes a(2) \bigotimes a(3) \;=$$

$$\begin{pmatrix} -454 - 299I & -145 + 428I & -280 - 533I & -370 + 337I & 369 + 505I & 329 - 402I & 87 + 687I & 534 - 214I \\ 335 - 117I & 184 - 377I & 387 + 66I & 381 - 267I & -408 - 8.8I & -350 + 332I & -390 - 227I & -518 + 134I \\ -157 + 500I & 435 + 21I & -134 + 630I & 535 - 25I & 370 - 476I & -460 - 198I & 398 - 625I & -586 - 189I \\ -197 - 279I & -399 - 71I & -274 - 319I & -496 - 41I & 100 + 380I & 401 + 237I & 167 + 454I & 518 + 243I \\ 830 - 76I & -235 - 651I & 846 + 371I & 121 - 758I & -374 + 413I & 410 + 214I & -584 + 200I & 283 + 427I \\ -289 + 461I & 140 + 629I & -527 + 292I & -201 + 684I & -66 - 357I & -353 - 246I & 127 - 382I & -211 - 427I \\ -291 - 750I & -542 + 391I & -443 - 883I & -617 + 541I & 482 + 237I & 90 - 437I & 617 + 234I & 59 - 545I \\ 504 + 146I & 546 - 297I & 633 + 120I & 633 - 426I & -314 + 156I & -134 + 393I & -366 + 227I & -118 + 496I \end{pmatrix}$$

where we have passed from four to zero decimal digits to save space.

Gambler's evening to a third kind quantum casino may be told in the following way:

- at the beginning he has $PAYOFF(0) \;=\; 0$; since at the first turn he doesn't bet we have obviously that $PAYOFF(1) \;=\; 0$
- since:

$$P_{un}(\begin{pmatrix} 5.21295 - 0.543424I & -5.83373 - 1.51207I \\ -5.72507 + 5.64286I & 0.264194 - 5.36408I \end{pmatrix}^{\dagger} \begin{pmatrix} 5.21295 - 0.543424I & -5.83373 - 1.51207I \\ -5.72507 + 5.64286I & 0.264194 - 5.36408I \end{pmatrix})$$

$$= \; P_{un}(\begin{pmatrix} 5.21295 + 0.543424I & -5.72507 - 5.64286I \\ -5.83373 + 1.51207I & 0.264194 + 5.36408I \end{pmatrix} \begin{pmatrix} 5.21295 - 0.543424I & -5.83373 - 1.51207I \\ -5.72507 + 5.64286I & 0.264194 - 5.36408I \end{pmatrix})$$

$$P_{unbiased}(\begin{pmatrix} 92.0884 & -61.3705 + 18.1664I \\ -61.3705 - 18.1664I & 65.1619 \end{pmatrix}) \;=\; 157.25 \;>\; 2$$

  he bets on σ_z.
- since:

$$\|a(2) \;-\; \sigma_z\| \;=\; \| \begin{pmatrix} -3.21604 - 8.29818I & 2.29687 - 9.22925I \\ -7.10612 + 4.25443I & -7.19842 + 6.03258I \end{pmatrix} \| \;=\; 11.5984 \;>\; 10$$

  he loses his fiche. Consequentially $PAYOFF(1) \;=\; -1$

- since:

$$P_{un}(\begin{pmatrix} -16.0615-42.0538I & 6.95806-49.3598I & 0.380344+51.7601I & -27.3546+50.3679I \\ -34.7319+26.0397I & -39.4597+35.9027I & 47.8881-14.0742I & 56.949-22.7959I \\ 59.5124+35.0029I & 38.9296+65.799I & -45.0976+9.69467I & -48.8996-14.7589I \\ 16.6759-64.4557I & 12.8955-80.7994I & 20.9437+39.2418I & 30.1933+45.5707I \end{pmatrix}^{\dagger} \begin{pmatrix} -16.0615-42.0538I & 6.95806-49.3598I & 0.380344+51.7601I & -27.3546+50.3679I \\ -34.7319+26.0397I & -39.4597+35.9027I & 47.8881-14.0742I & 56.949-22.7959I \\ 59.5124+35.0029I & 38.9296+65.799I & -45.0976+9.69467I & -48.8996-14.7589I \\ 16.6759-64.4557I & 12.8955-80.7994I & 20.9437+39.2418I & 30.1933+45.5707I \end{pmatrix})$$

$$= P_{un}(\begin{pmatrix} -16.0615+42.0538I & -34.7319-26.0397I & 59.5124-35.0029I & 16.6759+64.4557I \\ 6.95806+49.3598I & -39.4597-35.9027I & 38.9296-65.799I & 12.8955+80.7994I \\ 0.380344-51.7601I & 47.8881+14.0742I & -45.0976-9.69467I & 20.9437-39.2418I \\ -27.3546-50.3679I & 56.949+22.7959I & -48.8996+14.7589I & 30.1933-45.5707I \end{pmatrix} \begin{pmatrix} -16.0615-42.0538I & 6.95806-49.3598I & 0.380344+51.7601I & -27.3546+50.3679I \\ -34.7319+26.0397I & -39.4597+35.9027I & 47.8881-14.0742I & 56.949-22.7959I \\ 59.5124+35.0029I & 38.9296+65.799I & -45.0976+9.69467I & -48.8996-14.7589I \\ 16.6759-64.4557I & 12.8955-80.7994I & 20.9437+39.2418I & 30.1933+45.5707I \end{pmatrix}) =$$

$$P_{un}(\begin{pmatrix} 13110.4 & 14312.4+2902.95I & -8737.18+2586.31I & -10110.9+888.808I \\ 14312.4-2902.95I & 17870.7 & -8965.55+4758.04I & -11909.6+3525.38I \\ -8737.18-2586.31I & -8965.55-4758.04I & 9276.95 & 10127.5+2054.13I \\ -10110.9-888.808I & -11909.6-3525.38I & 10127.5-2054.13I & 12645.4 \end{pmatrix}) = 26451.7 > 4$$

he bets on σ_z.

- since:

$$\|a(3) - \sigma_z\| = \| \begin{pmatrix} 8.80519-7.0523I & -7.72367-6.40421I \\ -0.227234+7.87254I & 7.36604+6.81784I \end{pmatrix} \| = 15.3175 > 10$$

he loses his fiche. Consequentially $PAYOFF(2) = -1$

- since:

$$P_{un}(\vec{a}(3)^{\dagger}\vec{a}(3)) = 6.97591\,10^{6} > 8$$

he bets on σ_z.

- since:

$$\|a(4) - \sigma_z\| = \| \begin{pmatrix} 3.55982-1.58403I & 2.19976-1.67009I \\ 0.284886+2.77311I & -7.06443-6.30601I \end{pmatrix} \| = 10.0665 > 10$$

he loses his fiche. Consequentially $PAYOFF(3) = -2$

- since:

$$P_{un}(\vec{a}(4)^{\dagger}\vec{a}(4)) \;=\; 7.5079\,10^{8} \;>\; 16$$

he bets on σ_z.

- since:

$$\|a(4) \;-\; \sigma_z\| \;=\; \| \begin{pmatrix} -8.49908 + 1.07129I & -0.361299 - 7.07676I \\ 9.60704 + 6.81686I & -1.16288 - 3.10934I \end{pmatrix} \| \;=\; 14.1717 \;>\; 10$$

he loses his fiche. Consequentially $PAYOFF(3) \;=\; -3$

Exactly as it happened for the other kinds of Quantum Casinos, the notion of a **third kind Quantum Casino** induces naturally the notion of a **third kind collective**:

DEFINITION 9.2.11

THIRD KIND QUANTUM COLLECTIVES:

$\mathcal{QC}ollectives^{3} \;\subset\; \Sigma_{alg}^{\bigotimes\infty}$ induced by the axiom4.1.2 and the assumption that the **third kind quantum admissible gambling strategies** are nothing but the **quantum algorithms** on $\Sigma_{alg}^{\bigotimes\infty}$:

$$\mathcal{QS}trategies_{admissible}(\mathcal{QC}ollectives^{3}) \;:=\; Q_{\Phi} - \Delta_{0}^{0} - \overset{\circ}{MAP}\;(\Sigma_{NC}^{\infty}) \quad (9.2.9.7)$$

9.3 The censorship of winning quantum gambling strategies

As we explained section9.1 our excursion in Quantum Gambling Theory is motivated by the assumption of the following constraing on $RANDOM(\Sigma_{NC}^{\infty})$:

CONSTRAINT 9.3.1

QUANTUM ALGORITHMIC RANDOMNESS IS STRONGER THAN OWNERSHIP TO THIRD KIND QUANTUM COLLECTIVES

$$\mathcal{QC}ollectives^{3} \subseteq RANDOM_{NC}(\Sigma_{NC}^{\infty}) \tag{9.3.9.1}$$

Can we give an assurance to a third kind Quantum Casinos' owner that in the long run he doesn't risk anything?

The positive answer is stated by the following:

Conjecture 9.3.1

LAW OF EXCLUDED QUANTUM GAMBLING STRATEGIES FOR THIRD KIND QUANTUM CASINOS

For $n \rightarrow \infty$ the set of the *lucky-winning strategies* tends to the null set $\forall \epsilon_{Casino} \in \mathbb{R}_{+}$.

Part IV

Classical Algorithmic Randomness of the results of quantum measurements

Appendix A

Mathematica package for Quantum Algorithmic Information Theory

Many of the concept discussed in this work may be concretelly implemented by the alleged Mathematica notebook *Noncommutative Algorithmic Information Theory.nb* not incorporated in the text owing to the bad behaviour of TexSave's outputs on greek letters.

It is not a package (in the sense of section2.6.10 of [Wol96]).

Furthermore many of instructions will still require some debugging process.

Bibliography

[Acc88] L. Accardi. Foundations of Quantum Mechanics: A Quantum Probabilistic Approach. In G. Tarozzi A. van der Merwe, editor, *The Nature of Quantum Paradoxes*. Kluwer Academic Publishers, Dordrecht, 1988.

[Alv95] O. Alvarez. Lectures on Quantum Mechanics and the Index Theorem. In D.S. Freed K.K. Uhlenbeck, editor, *Geometry and Quantum Field Theory*, pages 271–322. American Mathematical Society, 1995.

[Ama85] S. Amari. *Differential-Geometrical Methods in Statistics*. Springer-Verlag, Singapore, 1985.

[Ana98] J. Anandan. Quantum Measurement Problem and the Gravitational Field. In K.P. Tod S.A. Huggett, L.J. Mason, editor, *The Geometric Universe: Science, Geometry and the work of Roger Penrose*, pages 357–368. Oxford University Press, Oxford, 1998.

[Ara97] H. Araki. The work of Alain Connes. In M. Atiyah D. Iagolnitezer, editor, *Fields Medallists' Lectures*, pages 329–333. World Scientific, Singapore, 1997.

[Bek01] J.D. Bekenstein. Quantum information and quantum black holes. *gr-qc/0107049*, 2001.

[Bel93] J.S. Bell. *Speakable and unspeakable in quantum mechanics*. Cambridge University Press, Cambridge, 1993.

[Ben72] P.A. Benioff. Decision Procedures in Quantum Mechanics. *Journal of Mathematical Physics*, 13:908–915, 1972.

[Ben73] P. Benioff. Possible strenghtening of the interpretative rules of quantum mechanics. *Physical Review D*, 7(12):3603–3609, 1973.

[Ben74] P. Benioff. Some consequences of the strenghtened interpretative rules of quantum mechanics. *Journal of Mathematical Physics*, 15(5):552–559, 1974.

[Ben77] P. Benioff. Finite and infinite measurements sequences in quantum mechanics and randomness: The Everett interpretation. *Journal of Mathematical Physics*, 18(12):2289–2295, 1977.

[Ben78] P. Benioff. A note on the Everett interpretation of quantum mechanics. *Foundations nof Physics*, 8(9/10):709–720, 1978.

[Ben88] C.H. Bennett. Logical depth and physical complexity. In R.H. Herken, editor, *The Universal Turing machine; A Half-Century Survey*, pages 227–258. Oxford University Press, Oxford, 1988.

[Ben90a] C.H. Bennett. Logical reversibility of computation. In H.S. Leff A.F. Rex, editor, *Maxwell's Demon. Entropy, Information, Computing*, pages 197–204. Adam Hilger, Bristol, 1990.

[Ben90b] C.H. Bennett. The thermodynamic of computation - a review. In H.S. Leff A.F. Rex, editor, *Maxwell's Demon. Entropy, Information, Computing*, pages 213–248. Adam Hilger, Bristol, 1990.

[Ben93] F. Benatti. *Deterministic Chaos in Infinite Quantum Systems*. Springer Verlag, Berlin, 1993.

[Ben96] F. Benatti. Entropy of a subalgebra and quantum estimation. *Journal of Mathematical Physics*, 37(10):5244–5258, October 1996.

[Ben98] P. Benioff. A Simple Example of Definitions of Truth, Validity, Consistency and Completeness in Quantum Mechanics. *quanth-ph/9811055*, 1998.

[Bil65] P. Billingsley. *Ergodic Theory and Information*. John Wiley and Sons Inc., 1965.

[Bil95] P. Billingsley. *Probability and Measure*. Wiley and Sons Inc., 1995.

[Bin00] D.P. Landau K. Binder. *A Guide to Monte Carlo Simulations in Statistical Physics*. Cambridge University Press, Cambridge, 2000.

[Boh79] D. Bohm. *Quantum Theory*. Dover Publication Inc., New York, 1979.

[Boh93] A. Bohm. The geometric phase in Quantum Physics. In L.A. Ibort M.A. Rodriguez, editor, *Integrable Systems, Quantum Groups and Quantum Field Theories*, pages 347–416. Kluwer Academic Publisher, Dordrecht, 1993.

[Bol95] L. Boltzmann. *Lectures on Gas Theory*. Dover Publication Inc., New York, 1995.

[Bou00] A. Boukas. Quantum Formulation of Classical Two-Person Zero-Sum Games. *Opens Systems and Information Dynamics*, 7(1):19–32, March 2000.

[BR92] L. Bing-Ren. *Introduction to Operator Algebras*. World Scientific, Singapore, 1992.

[Bri90] L. Brillouin. Maxwell's demon cannot operate: information and entropy I. In H.S. Leff A.F. Rex, editor, *Maxwell's Demon. Entropy, Information, Computing*, pages 134–137. Adam Hilger, Bristol, 1990.

[Bri98] D.S. Bridges. Constructive Truth in practice. In H.G. Dales G.Olivieri, editor, *Truth in Mathematics*, pages 53–69. Oxford University Press, Oxford, 1998.

[Bru78] A.A. Brudno. The complexity of the trajectories of a dynamical system. *Russian Mathematical Surveys*, 33(1):197–198, 1978.

[Bru83] A.A. Brudno. Entropy and the complexity of the trajectories of a dynamical system. *Trans. Moscow Math. Soc.*, 44:127, 1983.

[Cal94] C. Calude. *Information and Randomness. An Algorithmic Perspective.* Springer Verlag, Berlin, 1994.

[Cal96] C. Calude. Algorithmic Information Theory: Open Problems. *Journal of Universal Computer Science*, 5:439–441, 1996.

[Car60] J. Mc Carthy. Recursive Functions of Symbolic Expressions and Their Computation by Machine I. *ACM Communications*, 3:184, 1960.

[Cav00] R. Schack T.A. Brun C.M. Caves. Quantum Bayes rule. *quant-ph/0008113*, 2000.

[Cha87] G.J. Chaitin. *Algorithmic Information Theory.* Cambridge University Press, Cambridge, 1987.

[Cha90] G.J. Chaitin. *Information Incompleteness and Randomness.* World Scientific, 1990.

[Cha95] A. Arslanov C. Calude G.J. Chaitin. Program-size complexity computes the halting problem. Technical Report 8, Centre for Discrete Mathematics and Theoretical Computer Science, Auckland, New Zealand, September 1995.

[Cha98] G.J. Chaitin. *The Limits of Mathematics.* Springer-Verlag, 1998.

[Cha99] G.J. Chaitin. *The Unwknowable.* Springer-Verlag, Singapore, 1999.

[Cha01] G.J. Chaitin. *Exploring Randomness.* Springer Verlag, London, 2001.

[Chr00] D. Christodulou. *The Action Principle and Partial Differential Equations.* Princeton University Press, Princeton, 2000.

[Chu00] M.A. Nielsen I.L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, Cambridge, 2000.

[Cle98] C.P. Williams S.H. Clearwater. *Explorations in Quantum Computing.* Springer-Verlag, New York, 1998.

[Con92] A. Connes. Noncommutative Geometry. In C. Casacuberta M. Castellet, editor, *Mathematical Research Today and Tomorrow. Viewpoints of Seven Fields Medalists*, pages 40–58. Springer-Verlag, Berlin, 1992.

[Con94] A. Connes. *Noncommutative Geometry.* Academic Press, San Diego, 1994.

[Con98] A. Connes. Noncommutative Geometry: The Spectral Aspect. In A. Connes K. Gawedzki J. Zinn-Justin, editor, *Quantum Symmetries*, pages 643–685. Elsevier Science, Amsterdam, 1998.

[Cru97] C. Moore J.P. Crutchfield. Quantum Automata and Quantum Grammars. *quanth-ph/9707031*, 1997.

[Cut80] N.J. Cutland. *Computability.* Cambridge Univesrity Press, Cambridge, 1980.

[Dan98] T.D. Kieu M. Danos. The halting problem for universal quantum computers. *quant-ph/9811001*, 1998.

[Dav65] M. Davis. *the Undecidable. Basic Papers On Undecidable Propositions, Unsolvable Problems And Computable Functions.* Raven Press, New York, 1965.

[Deu85] D. Deutsch. Quantum Theory, the Church-Turing principle and the universal quantum computer. *Proc. R. Soc. Lond. A*, 400:97–117, 1985.

[dL51] P.S. Marquis de Laplace. *A Phylosophical Essay on Probabilities.* Dover Publications Inc., Toronto, 1951.

[Dro89a] C. Itzykson J.M. Drouffe. *Statistical Field Theoory. Vol.1: from brownian motion to renormalization and lattice gauge theory.* Cambridge University Press, Cambridge, 1989.

[Dro89b] C. Itzykson J.M. Drouffe. *Statistical Field Theoory. Vol.2: strong coupling, Monte Carlo methods, conformal invariance and random systems.* Cambridge University Press, Cambridge, 1989.

[Ell73] S.W. Hawking G.F.R. Ellis. *The large scale structure of space-time.* Cambridge University Press, Cambridge, 1973.

[Esp98] G. Esposito. *Dirac Operators and Spectral Geometry.* Cambridge University Press, Cambridge, 1998.

[Fal90] K. Falconer. *Fractal Geometry: Mathematical Foundations and Applications.* John Wiley ans Sons, Baffins Lane, Chichester, 1990.

[Fey96] R.P. Feynman. *Feynman Lectures on Computation.* Addison-Wesley, 1996.

[Fey99] R.P. Feynman. Simulating Physics with Computers. In A.G.J. Hey, editor, *Feynman and Computation. Exploring the Limits of Computers*, pages 133–154. Perseus Book, Reading, 1999.

[Fig01] J. Gracia-Bondia J.C. Varilly H. Figueroa. *Elements of Noncommutative Geometry*. Birkhauser, Boston, 2001.

[Fin97] D.R. Finkelstein. *Quantum Relativity*. Springer-Verlag, Berlin, 1997.

[For92] J. Ford. Che cosa é il caos, e perché preoccuparsene. In P. Davies, editor, *La Nuova Fisica*, pages 362–387. Bollati Boringhieri, Torino, 1992.

[Fuc01] C. Fuchs. Notes on a Paulian Idea. Foundational, Historical, Anecdotal and Forward-Looking Thought on the Quantum. *quant-ph/0105039*, 2001.

[Gab90] J. Balcázar J. Diaz J. Gabarró. *Structural Complexity 2*. Springer Verlag, Berlin, 1990.

[Gab95] J. Balcázar J. Diaz J. Gabarró. *Structural Complexity 1*. Springer Verlag, Berlin, 1995.

[Gal99] G. Gallavotti. *Statistical Mechanics. A Short Treatise*. Springer-Verlag, Berlin, 1999.

[Gil95] P.G. Gilkey. *Invariance Theory, the Heat Equation, and the Atiyah-Singer Index Theorem*. CRC Press Inc., Boca Raton (Florida), 1995.

[Gil00] D. Gillies. *Philosophical Theories of Probability*. Routledge, New York, 2000.

[Giv01] V.I. Arnold A.B. Givental. Symplectic Geometry. In V.I. Arnold S.P. Novikov, editor, *Dynamical Systems 4. Symplectic Geometry and its Applications*, pages 4–138. Springer Verlag, Berlin, 2001.

[Gol01] O. Goldreich. Computational Complexity. In B. Engquist W. Schmid, editor, *Mathematics Unlimited - 2001 and Beyond*, pages 507–524. Springer Verlag, Berlin, 2001.

[Gri99] P. Grillet. *Algebra*. John Wiley and sons, New York, 1999.

[Gru01] J. Gruska. Quantum Computing Challenges. In B. Engquist W. Schmid, editor, *Mathematics Unlimited - 2001 and Beyond*, pages 529–564. Springer Verlag, Berlin, 2001.

[Gut95] S. Guttmann. Using Classical Probability to Guarantee Properties of Infinite Quantum Systems. *quanth-ph/9506016*, 1995.

[Haa96] R. Haag. *Local Quantum Physics. Fields, Particles, Algebras*. Springer-Verlag, New York, 1996.

[Har68] J.B. Hartle. Quantum Mechanics of Individual Systems. *Am. Jour. Physics*, 36:704–712, 1968.

[Hav00] D. Bridges R. Havea. A constructive analysis of the proof that the numerical range is convex. *LMS Journal of Computation and Mathematics*, 3:191–206, 2000.

[Hel76] C.W. Helstrom. *Quantum Detection and Estimation Theory.* Academic Publisher, New York, 1976.

[Hib65] R.P. Feynman A.R. Hibbs. *Quantum Mechanics and Path Integrals.* Mc Graw Hill, 1965.

[Hol99] A.S. Holevo. Lectures on statistical structure of quantum theory. available at the web-link http://134.169.50.206/$skripte\_$.html, March 1999.

[Hug98] D.C. Brody L.P. Hughston. Geometric Models for Quantum Statistical Inference. In K.P. Tod S.A. Huggett, L.J. Mason, editor, *The Geometric Universe: Science, Geometry and the work of Roger Penrose*, pages 265–276. Oxford University Press, Oxford, 1998.

[Iha93] S. Ihara. *Information Theory for Continuous Systems.* World Scientific, Singapore, 1993.

[Ins00] S. French D. Rios Insua. *Statistical Decision Theory.* Oxford University Press, New York, 2000.

[Ish93] C. Isham. Canonical Quantum Gravity and the Problem of Time. In L.A. Ibort M.A. Rodriguez, editor, *Integrable Systems, Quantum Groups and Quantum Field Theories*, pages 347–416. Kluwer Academic Publisher, Dordrecht, 1993.

[Izq95] J. De Azcarrega J.M. Izquierdo. *Lie Groups, Lie algebras, cohomology and some applications in physics.* Cambridge University Press, Cambridge, 1995.

[Jaf87] J. Glimm A. Jaffe. *Quantum Physics.* Springer-Verlag, New York, 1987.

[Jaf91] A. Jaffe. Quantum Physics as Non-commutative Geometry. In K. Schmudgen, editor, *Mathematical Physics X*, pages 281–290. Springer Verlag, Berlin, 1991.

[Jaf00] A. Jaffe. Constructive Quantum Field Theory. In A. Fokas A. Grigoryan T. Kibble B. Zegarlinski, editor, *Mathematical Physics 2000*, pages 111–127. Imperial College Press, London, 2000.

[Joz98] R. Jozsa. Entanglement and Quantum Computation. In K.P. Tod S.A. Huggett, L.J. Mason, editor, *The Geometric Universe: Science, Geometry and the work of Roger Penrose*, pages 369–382. Oxford University Press, Oxford, 1998.

[Joz99] G. Mitchison R. Jozsa. Counterfactual Computation. *quanth-ph/9907007*, 1999.

[Jup01] O.E. Barndorff-Nielsen R.D. Gill P.E. Jupp. Quantum Information. In B. Engquist W. Schmid, editor, *Mathematics Unlimited - 2001 and Beyond*, pages 83–108. Springer Verlag, Berlin, 2001.

[Kad01] R.V. Kadison. Operator Algebras - An overview. In J. Glimm J. Impagliazzo I. Singer, editor, *The Legacy of John Von Neumann*, pages 61–90. American Mathematical Society, Providence Rhode Island, 2001.

[Kak99] Y. Kakihara. *Abstract Methods in Information Theory.* World Scientific, Singapore, 1999.

[Khi57] A.I. Khinchin. *Mathematical Foundations of Information Theory.* Dover Publications Inc., New York, 1957.

[Khr99] A. Khrennikov. *Superanalysis.* Kluwer Academic Publishers, Dordrecht, 1999.

[Kir01] A.A. Kirillov. Geometric Quantization. symplectic geometry and its applications. In V.I. Arnold S.P. Novikov, editor, *Dynamical Systems 4*, pages 139–176. Springer Verlag, Berlin, 2001.

[Kni00] V. Vedral M.B. Plenio P.L. Knight. Entanglement Quantification. In D. Bouwmeester A. Ekert A. Zeilinger, editor, *The Physics of Quantum Information*, pages 210–220. Springer-Verlag, Berlin, 2000.

[Knu98] D.E. Knuth. *The Art of Computer Programming. Vol.2: Seminumerical Algorithms.* Addison-Wesley, 1998.

[Kol56] A.N. Kolmogorov. *Foundations of the Theory of Probability.* Chelsea, 1956.

[Lam87] M. Van Lambalgen. *Random Sequences.* PhD thesis, Department of Informatics, University of Amsterdam, 1987.

[Lan90] R. Landauer. Irreversibility and heat generation in the computing process. In H.S. Leff A.F. Rex, editor, *Maxwell's Demon. Entropy, Information, Computing*, pages 188–196. Adam Hilger, Bristol, 1990.

[Lan97] G. Landi. *An Introduction to Noncommutative Spaces and Their Geometries.* Springer Verlag, Berlin, 1997.

[Laz98] D. Shasha C. Lazerre. *Out of Their Minds.* Copernicus, Springer-Verlag, New York, 1998.

[Leb73] H. Lebesgue. *Lecons sur l'integration et la recherche des fonctions primitives.* Chelsea Publishing Company, New York, 1973.

[Lew99] J. Eisert M. Wilkens M. Lewenstein. Quantum Games and Quantum Strategies. *Phys.Rev.Lett.*, (83):3077, 1999.

[Lin99] G. Lindblad. A general no-cloning theorem. *Letters in Mathematical Physics*, 47(2):189–196, 1999.

[Llo89] S. Lloyd. Quantum Mechanical Computers and Uncomputability. *available at Toffoli's Quantum Computation Library http://pks.bu.edu/qcl*, 1989.

[Lon92] L. Longpré. Resources Bounded Kolmogorov Complexity and Statistical Tests. In O. Watanabe, editor, *Kolmogorov Complexity and Computational Complexity*, pages 66–84. Springer-Verlag, Berlin, 1992.

[Loy01] S. Loyd. Physical Limits to Computation. In P. Tombesi O. Hirota, editor, *Quantum Communication, Computing and Measurement 3*, pages 189–198. Kluwer Academic - Plenum Publishers, New York, 2001.

[Man98] Yu. I. Manin. Truth, rigour, and common sense. In H.G. Dales G.Olivieri, editor, *Truth in Mathematics*, pages 147–159. Oxford University Press, Oxford, 1998.

[Mat01] Yuri Matiyasevich. Hilbert's Tenth Problem: A Two-way Bridge between Number Theory and Computer Science. In C. Calude, editor, *People and Ideas in Theoretical Computer Science*, pages 177–204. Springer Verlag, Singapore, 2001.

[Max71] J.C. Maxwell. *Theory of Heat*. Logmans, Green and co., London, 1871.

[May96] P. Mayimin. Extending the Lambda Calculus to Express Randomized and Quantumized Algorithms. *quanth-ph/9612052*, 1996.

[Mis81] R. Von Mises. *Probability, Statistics and Thruth*. Dover Publications Inc., New York, 1981.

[Mit01] P. Mittelstaedt. Quantum Mechanics without probabilities. In M. Redei N. Stöltzner, editor, *John Von Neumann and the Foundations of Quantum Physics*, pages 189–200. Kluwer Academic Publisher, Dordrecht, 2001.

[Mon99] J.R. Mondragón. Algorithms on Finite Automata. available at the Mathsource software's archive at http:
www.mathsource.com, 1999.

[Mye97] J.M. Myers. Can a Universal Computer Be Fully Quantum? *Physical Review Letters*, 78(9):1823–1824, March 1997.

[Nah01] P.J. Nahin. *Time Machines. Time Travel in Physics, Metaphysics, and Science Fiction*. Springer-Verlag, New York, 2001.

[Nak95] M. Nakahara. *Geometry, Topology and Physics.* Institute of Physics Publishing, Bristol, 1995.

[Neu83] J. Von Neumann. *Mathematical Foundations of Quantum Mechanics.* Princeton Unicersity Press, Princeton, 1983.

[Ö98] B. Öemer. *A Procedural Formalism for Quantum Computing.* Masters thesis, Department of Theoretical Physics, Technical University of Vienna, 1998.

[Odi89] P. Odifreddi. *Classical Recursion Theory: vol. 1.* Elsevier Science, Amsterdam, 1989.

[Odi96] P. Odifreddi. Kreisel's Church. In P. Odifreddi, editor, *Kreiseliana*, pages 389–415. A.K. Peters Ltd., Wellesley MA, 1996.

[Odi99a] P. Odifreddi. *Classical Recursion Theory: vol. 2.* Elsevier Science, Amsterdam, 1999.

[Odi99b] P. Odifreddi. Reducibilities. In E.R. Griffor, editor, *Handbook of Computability Theory*, pages 89–120. Elsevier Science B.V., Amsterdam, 1999.

[Odi00] P. Odifreddi. Ultrafilters, Dictators and Gods. In C.S. Calude G. Păun, editor, *Finite VS Infinite. Contribution to an Eternal Dilemma*, pages 239–246. Springer-Verlag, London, 2000.

[Ohy97] R.S. Ingarden A. Kossakowski M. Ohya. *Information Dynamics and Open Systems. Classical and Quantum Approach.* Kluwer Academic Publishers, Dordrecht, 1997.

[Ohy98] M. Ohya. Foundation of entropy, complexity and fractals in quantum systems. In L. Accardi C.C. Heyde, editor, *Probability Towards 2000*, pages 263–286. Springer Verlag, New York, 1998.

[Opr94] I. Cuculescu A.G. Oprea. *Noncommutative Probability.* Kluwer Academic Publisher, Dordrecht, 1994.

[Oza97] M. Ozawa. Quantum state reduction and the Quantum Bayes Principle. In O. Hirota A.S. Holevo C.M. Caves, editor, *Quantum Communication, Computing and Measurement*, pages 233–242. Plenum Press, New York, 1997.

[Oza98a] M. Ozawa. Measurability and Computability. *quant-ph/9809048*, 1998.

[Oza98b] M. Ozawa. Quantum Nondemolition Monitoring of Universal Quantum Computers. *Physical Review Letters*, 80(3):631–634, January 1998.

[Oza98c] M. Ozawa. Quantum Turing Machines: Local Transition, Preparation, Measurement and Halting. In G.M. D'Ariano O. Hirota P. Kumar, editor, *Quantum Communication, Computing and Measurement 2*, pages 241–248. Kluwer, New York, 1998.

[Pap98] H.L. Lewis C.H. Papadimitriou. *Elements of the Theory of Computation.* Prentice-Hall International Inc., Upper Saddle River, 1998.

[Par92] K.R. Parthasarathy. *An Introduction to Quantum Stochastic Calculus.* Birkhauser, Basel, 1992.

[Pas00] L. Pastur. Random matrices as paradigm. In A. Fokas A. Grigoryan T. Kibble B. Zegarlinski, editor, *Mathematical Physics 2000*, pages 216–265. Imperial College Press, London, 2000.

[Pau01] C. Calude F. Paun. *Computing with cells and atoms.* Taylor and Francis, London, 2001.

[PE99] M.B. Pour-El. The structure of computability in analysis and physical theory: an extension of Church's thesis. In E.R. Griffor, editor, *Handbook of Computability Theory*, pages 449–472. Elsevier Science B.V., Amsterdam, 1999.

[Pen89] R. Penrose. *The Emperor's New Mind.* Oxford University Press, Oxford, 1989.

[Pen96] R. Penrose. *Shadows of the mind.* Oxford University Press, Oxford, 1996.

[Pen00] R. Penrose. Wavefunction collapse as a Real Gravitational Effect. In A. Fokas A. Grigoryan T. Kibble B. Zegarlinski, editor, *Mathematical Physics 2000*, pages 266–282. Imperial College Press, London, 2000.

[Per95] A. Peres. *Quantum Theory: Concepts and Methods.* Kluwer Academic Publishers, 1995.

[Pet93] M. Ohya D. Petz. *Quantum Entropy and Its Use.* Springer-Verlag, Berlin, 1993.

[Pet97] H. Hasegawa D. Petz. Non-commutative extension of Information Geometry. In O. Hirota A.S. Holevo C.M. Caves, editor, *Quantum Communication, Computing and Measurement*, pages 109–118. Plenum Press, New York, 1997.

[Pet00] F. Hiai D. Petz. *The Semicircle Law, Free Random Variables and Entropy.* American Mathematical Society, 2000.

[Pet01] D. Petz. Entropy, von Neumann and the von Neumann Entropy. In M. Redei N. Stöltzner, editor, *John Von Neumann and the Foundations of Quantum Physics*, pages 83–96. Kluwer Academic Publisher, Dordrecht, 2001.

[Pop98] N. Linden S. Popescu. The Halting Problem for Quantum Computers. *quant-ph/9806054*, 1998.

[Pre98] J. Preskill. Quantum information and computation. available at the web-link: http://www.theory.caltech.edu/ $\sim$ /preskill/ph229, september 1998.

[Pru92] E. Prugovečki. *Quantum Geometry. A Framework for Quantum General Relativity.* Kluwer Academic Publisher, Dordrecht, 1992.

[Red95] D. Petz M. Redei. Legacy of John Von Neumann in the Theory of Operator Algebras. In F. Brody T.Vamos, editor, *The Neumann Compendium*, pages 163–185. World Scientific, Singapore, 1995.

[Red98] M. Redei. *Quantum Logic in Algebraic Approach.* Kluwer Academic Publishers, Dordrecht, 1998.

[Red01] M. Redei. Von Neumann's Concept of Quantum Logic and Quantum Probability. In M. Redei N. Stöltzner, editor, *John Von Neumann and the Foundations of Quantum Physics*, pages 153–176. Kluwer Academic Publisher, Dordrecht, 2001.

[Rex90] H.S. Leff A.F. Rex. *Maxwell's Demon. Entropy, Information, Computing.* Adam Hilger, Bristol, 1990.

[Ric89] M.B. Pour-El J.I. Richards. *Computability in Analysis and Physics.* Springer-Verlag, Berlin, 1989.

[Rin97a] R.V. Kadison J.R. Ringrose. *Fundamental of the Theory of Operator Algebras. Vol 1: Elementary Theory.* American Mathematical Society, New York, 1997.

[Rin97b] R.V. Kadison J.R. Ringrose. *Fundamental of the Theory of Operator Algebras. Vol 2: Advanced Theory.* American Mathematical Society, New York, 1997.

[Rob87] O. Bratteli D.W. Robinson. *Operator Algebras and Quantum Statistical Mechanics, vol.1.* Springer-Verlag, New York, 1987.

[Rob97] O. Bratteli D.W. Robinson. *Operator Algebras and Quantum Statistical Mechanics, vol.2.* Springer-Verlag, New York, 1997.

[Ros83] A. Einstein B. Podolski N. Rosen. Can quantum mechanical description of physical reality be considered complete? In J.A. Wheeler W.H. Zurek, editor, *Quantum Theory and Measurement*, pages 138–141. Princeton University Press, Princeton, 1983.

[Rov88] C. Rovelli. Is there incompatibility between the ways time is treated in General Relativity and in Standard Quantum Mechanics ? In A. Ashtekar J. Stackel, editor, *Conceptual Problems of Quantum Gravity*, pages 126–140. Birkauser, 1988.

[Rue99] D. Ruelle. *Statistical Mechanics: Rigorous Results.* Imperial College Press and World Scientific, London, 1999.

[Rus98] A. Lesniewski M.B. Ruskai. Monotone Riemannian Metrics and Relative Entropies on Non-commutative Probability Spaces. *math-ph/9808016*, 1998.

[Sak91] S. Sakai. *Operator Algebras in Dynamical Systems.* Cambridge University Press, Cambridge, 1991.

[Sak98] S. Sakai. *$C^\star$-Algebras and $W^\star$-algebras.* Springer-Verlag, Berlin, 1998.

[Sal98] D. Mc Duff D. Salamon. *Introduction to Symplectic Topology.* Oxford University Press, Oxford, 1998.

[Sch81] L.S. Schulman. *Techniques and Applications of Path Integration.* John Wiley and Sons, New York, 1981.

[Sch01] C.M. Caves C.A. Fuchs R. Schack. Unknown Quantum States: The Quantum de Finetti Representation. *quant-ph/0104088*, 2001.

[Sem93] V. Uspensky A. Semenov. *Algorithms: Main Ideas and Applications.* Kluwer Academic Publisher, Dordrecht, 1993.

[Shi93] A.N. Shiryayev. *Selected Works of A.N. Kolmogorov - Volume3: Information Theory and the Theory of Algorithms.* Kluwer Academic Publishers, Dordrecht, 1993.

[Shi00] A. Shimony. New aspects of Bell's theorem. In J. Ellis D. Amati, editor, *Quantum Reflections*, pages 136–164. Cambridge University Press, Cambridge, 2000.

[Sim75] M. Reed B. Simon. *Methods of Modern Mathematical Physics: vol.2 - Fourier Analysis, Self-adjointness.* Academic Press, 1975.

[Sim80] M. Reed B. Simon. *Methods of Modern Mathematical Physics: vol.1 - Functional Analysis.* Academic Press, 1980.

[Sim93] B. Simon. *The Statistical Mechanics of Lattice Gases.* Princeton University Press, Princeton, 1993.

[Sin00] I.P. Kornfeld Y.G. Sinai. General Ergodic Theory of Groups of Measure Preseving Trasformations. In Y.G. Sinai, editor, *Dynamical Systems, Ergodic Theory abd Applications.* Springer Verlag, Berlin, 2000.

[Sla99] T.A. Slaman. The global structure of the Turing degrees. In E.R. Griffor, editor, *Handbook of Computability Theory*, pages 155–168. Elsevier Science B.V., Amsterdam, 1999.

[Sla01] A. Kučera T.A. Slaman. Randomness and recursive enumerability. *SIAM J. Comput.*, 31(1):199–211, 2001.

[Sma92] S. Smale. Theory of Computation. In C. Casacuberta M. Castellet, editor, *Mathematical Research Today and Tomorrow. Viewpoints of Seven Fields Medalists*, pages 59–69. Springer-Verlag, Berlin, 1992.

[Smi00] J.M. Bernardo A.F. Smith. *Bayesian Theory.* John Wiley and Sons, Ltd., New York, 2000.

[Smu92] R.M. Smullyan. *Gödel Incompleteness Theorems.* Oxford University Press, New York, 1992.

[Soc00] Am. Math. Society London Math. Society. *Kolmogorov in Perspective.* American Mathematical Society, 2000.

[Sol00] R.M. Solovay. A Version of Ω for Which ZFC Cannot Predict a Single Bit. In C. S. Calude G. Paun, editor, *Finite VS Infinite*, pages 323–334. Springer Verlag, London, 2000.

[S.S98] L.Blum F.Cucker M.Shub S.Smale. *Complexity and real computation.* Springer-Verlag, New York, 1998.

[Sta99] L. Staiger. The Kolmogorov Complexity of Real Numbers. In G. Ciobanu Gh. Paun, editor, *Fundamentals of Computation Theory*, pages 536–546. Springer Verlag, Berlin, 1999. available at author's homepage: http://www.informatik.uni-halle.de/ staiger/.

[Str85] F. Strocchi. *Elements of Quantum Mechanics of Infinite Systems.* World Scientific, Singapore, 1985.

[Str93] F. Strocchi. *Selected Topics on the General Properties of Quantum Field Theory.* World Scientific, Singapore, 1993.

[Str95] R.F. Streater. *Statistical Dynamics. A Stochastic Approach to Nonequilibrium Thermodymanics.* Imperial College Press, London, 1995.

[Str00a] R.F. Streater. The analytic quantum information manifold. In J. Jost S. Paycha M. Röckner S. Scarlatti F. Getsztesy, H. Holden, editor, *Stochatic Processes, Physics and Geometry: new interplays. Vol.2*, pages 603–612. American Mathematical Society, Providence, Rhode Island, 2000.

[Str00b] R.F. Streater. Classical and Quantum Probability. *J. Mathematical Phys.*, 41:3556–3603, 2000.

[Sud99] D. Petz Cs. Sudar. Extending the Fisher metric to density matrices. In E.B. Vendel Jensen O.E. Barndorff-Nielsen, editor, *Geometry in Present Days Science*, pages 21–34. World Scientific, Singapore, 1999.

[Sun87] V.S. Sunder. *An Invitation to von Neumann Algebras.* Springer-Verlag, New York, 1987.

[Svo93] K. Svozil. *Randomness and Undecidability in Physics.* World Scientific, 1993.

[Svo96] K. Svozil. Quantum Algorithmic Information Theory. *Journal of Universal Computer Science*, 2:311–346, 1996.

[Svo00] C. Calude M.J. Dinneen K. Svozil. Reflections on quantum computing. Technical Report 130, Centre for Discrete Mathematics and Theoretical Computer Science, Auckland, New Zealand, March 2000.

[Szi90] L. Szilard. On the decreaese of entropy in a thermodynamic system by the intervantion of intelligent beings. In H.S. Leff A.F. Rex, editor, *Maxwell's Demon. Entropy, Information, Computing*, pages 124–133. Adam Hilger, Bristol, 1990.

[Tak94] M. Fukushima Y. Oshima M. Takeda. *Dirichlet Forms and Symmetric Markov Process.* Walter de Gruyter, Berlin, 1994.

[Tei92] M. Henneaux C. Teitelboim. *Quantization of Gauge Systems.* Princeton University Press, Princeton, 1992.

[Thi81] W. Thirring. *A Course in Mathematical Physics - vol.3: Quantum Mechanics of Atoms and Molecules.* Springer-Verlag, Berlin, 1981.

[Thi83] W. Thirring. *A Course in Mathematical Physics - vol.4: Quantum Mechanics of Large Systems.* Springer-Verlag, Berlin, 1983.

[Thi97] W. Thirring. *Classical Mathematical Physics. Dynamical Systems and Field Theories.* Springer-Verlag, New York, 1997.

[Thi98] W.E. Thirring. *Selected papers of Walter E. Thirring with commentaries.* American Mathematical Society, Providence, Rhode Island, 1998.

[Thi01] W. Thirring. J. V. Neumann Influence in Mathematical Physics. In M. Redei N. Stöltzner, editor, *John Von Neumann and the Foundations of Quantum Physics*, pages 5–10. Kluwer Academic Publisher, Dordrecht, 2001.

[Tho83] V.B. Braginsky Y.I. Vorontsov K.S. Thorne. Quantum Nondemolition Measurements. In J.A. Wheeler W.H. Zurek, editor, *Quantum Theory and Measurement*, pages 749–768. Princeton University Press, Princeton, 1983.

[Tho91] T.M. Cover J.A. Thomas. *Elements of Information Theory.* John Wiley and sons, 1991.

[Uhl99] F. Benatti H. Narnhofer A. Uhlmann. Optimal Decompositions with Respect to Entropy and Symmetries. *Letters in Mathematical Physics*, 47(3):237–253, February 1999.

[Usp92] V.A. Uspensky. Complexity and Entropy: An Introduction to the Theory of Kolmogorov Complexity. In O. Watanabe, editor, *Kolmogorov Complexity and Computational Complexity*, pages 85–102. Springer-Verlag, Berlin, 1992.

[Var84] S.R.S. Varadhan. *Large Deviations and Applications.* Capital City Press, Montpelier (Vermont, U.S.A.), 1984.

[Č82] N.N. Čencov. *Statistical Decision Rules and Optimal Inference.* American Mathematical Society, Providence, 1982.

[vDSL00] A. Berthiaume W. van Dam S. Laplante. Quantum Kolmogorov Complexity. *quanth-ph/0005018*, May 2000.

[Vin92] G. Castagnoli M. Rasetti A. Vincenti. Steady, simultaneous quantum computation: a paradigm for the investigations of nondeterministic and non-recursive computation. *Int. J. Mod. Phys.*, C(3):661–689, 1992.

[Vit97] M. Li P. Vitanyi. *An Introduction to Kolmogorov Complexity and Its Applications.* Springer Verlag, New York, 1997.

[Vit99] P. Vitanyi. Two approaches to the Quantitative Definition of Information in an Individual Pure Quantum State. *quanth-ph/9907035*, July 1999.

[Vit01] P.M.B. Vitanyi. Quantum Kolmogorov Complexity based on Classical Descriptions. *IEEE Transactions on Information Theory - to appear*, 2001. quanth-ph/0102108.

[vN95] G. Birkhoff J. von Neumann. The Logic of Quantum Mechanics. In F. Brody T.Vamos, editor, *The Neumann Compendium*, pages 103–123. World Scientific, Singapore, 1995.

[vN01] J. von Neumann. Unpublished Correspondence. In M. Redei N. Stöltzner, editor, *John Von Neumann and the Foundations of Quantum Physics*, pages 225–229. Kluwer Academic Publisher, Dordrecht, 2001.

[Wal84] R.M. Wald. *General Relativity.* The University of Chicago Press, Chicago, 1984.

[Wal94] R.M. Wald. *Quantum Field Theory in Curved Spacetime and Black Hole Thermodynamics.* The University of Chicago Press, Chicago, 1994.

[Wea71] C.E. Shannon W. Weaver. *La Teoria Matematica delle Comunicazioni.* Gruppo Editoriale Fabbri, Bompiani, Sonzogno, 1971.

[Wer01] R.F. Werner. Quantum Information Theory - an invitation. In G. Alber T. Beth M. Horodecki P. Horodecki R. Horodecki R. Werner A. Zeilinger, editor, *Quantum Information. An introduction to Basic Theoretical Concepts and Experiments*, pages 14–53. Springer-Verlag, Berlin, 2001.

[Wey94] M.D. Davis R. Sigal E.J. Weyuker. *Computability, Complexity, and Languages.* Academic Publisher, London, 1994.

[Wig95] A.S. Wightman. Superselection rules; old and new. In G. Jona-Lasinio C. Di Castro, F. Guerra, editor, *Mesoscopic Physics and Fundamental Problems in Quantum Mechanics*, pages 751–769. Societá Italiana di Fisica, 1995.

[Win99] A. Winter. *Coding Theorems of Quantum Information Theory.* PhD thesis, Fakultät für Mathematik, Universität Bielefeld, Bielefeld, April 1999. available as quanth-ph/9907077.

[Wit92] B. De Witt. *Supermanifolds.* Cambridge University Press, Cambridge, 1992.

[Wit95] E. Witten. Some Questions for Constructive Field Theorists. In V. Rivasseu, editor, *Constructive Physics. Results in Field Theory, Statistical Mechanics and Condensed Matter Physics*, pages 1–5. Springer Verlag, Berlin, 1995.

[Wit99a] P. Deligne P. Etingof D.S. Freed L.C. Jeffrey D. Kazhdan J.W. Morgan D.R. Morrison E. Witten. *Quantum Fields and Strings: A Course for Mathematicians, vol. 1.* American Mathematical Society, 1999.

[Wit99b] P. Deligne P. Etingof D.S. Freed L.C. Jeffrey D. Kazhdan J.W. Morgan D.R. Morrison E. Witten. *Quantum Fields and Strings: A Course for Mathematicians, vol. 2.* American Mathematical Society, 1999.

[Wol94] S. Wolfram. *Cellular Automata and Complexity.* Addison-Wesley, 1994.

[Wol96] S. Wolfram. *The Mathematica Book.* Cambridge University Press, 1996.

[Woy98] M. Denker W.A. Woyczynski. *Introductory Statistics and Random Phenomena: uncertainty, complexity and chaotic behaviour in engineering and science.* Birkhauser, Boston, 1998.

[Yak81] V.M. Alekseev M.V. Yakobson. Symbolic dynamics and hyperbolic dynamic systems. *Physics Reports*, 75(5):287–325, 1981.

[Yan00] S.Y. Yan. *Number Theory for Computing.* Springer Verlag, Berlin, 2000.

[Zei98] A. Dembo O. Zeitouni. *Large Deviations Techniques and Applications.* Springer-Verlag, New York, 1998.

[Zie98] D.J. Collins H. Zieschang. Combinatorial Group Theory and Fundamental Groups. In D.J. Collins R.I. Grigorchuk P.F. Kurchanov H. Zieschang, editor, *Combinatorial Group Theory and Applications to Geometry*, pages 3–166. Sppringer Verlag, Berlin, 1998.

[ZJ93] J. Zinn-Justin. *Quantum Field Theory and Critical Phenomena.* Oxford University Press, New York, 1993.

[Zur89] W.H. Zurek. Algorithmic randomness and physical entropy. *Physical Review A*, 40(8):4731–4751, October 1989.

[Zur90a] W.H. Zurek. Algorithmic Information Content, Church-Turing Thesis, Physical Entropy, and Maxwell's Demon. In W.H. Zurek, editor, *Complexity, Entropy and the Physics of Information*, pages 73–90. Addison-Wesley, Redwood City, 1990.

[Zur90b] W.H. Zurek. Maxwell's demon, Szilard's engine and quantum measurements. In H.S. Leff A.F. Rex, editor, *Maxwell's Demon. Entropy, Information, Computing*, pages 249–259. Adam Hilger, Bristol, 1990.

[Zur99] W.H. Zurek. Algorithmic Randomness, Physical Entropy, Measurements, and the Demon of Choice. In A.G.J. Hey, editor, *Feynman and Computation. Exploring the Limits of Computers*, pages 393–410. Perseus Book, Reading, 1999.