# Some Bridging Results and Challenges in Classical, Quantum and Computational Randomness

Giuseppe Longo, Catuscia Palamidessi, Paul Thierry

# SOME BRIDGING RESULTS AND CHALLENGES IN CLASSICAL, QUANTUM AND COMPUTATIONAL RANDOMNESS

GIUSEPPE LONGO, CATUSCIA PALAMIDESSI AND THIERRY PAUL

Contents



To appear in "Randomness Through Computation"
Hector Zenil (Wolfram Research Inc., USA), Editor.
World Scientific. ISBN: 978-981-4327-74-9.
http://www.worldscibooks.com/print_flyer/flyers/7973flyer.html

## 1. Why were you initially drawn to the study of computation and randomness?

We encountered randomness in our different fields of interest, as unpredictable phenomena are omnipresent in natural and artificial processes. In classical physical systems (and by this we mean also relativistic ones) randomness may be defined as 'deterministic unpredictability'. That is, since Poincaré's results (on the Three Body Problem) and his invention of the geometry of dynamical systems, deterministic systems include various forms of chaotic ones, from weak (mixing) systems to ones highly sensitive to border conditions, where random behaviours are part of the deterministic evolutions. Randomness got a new status with the birth of quantum mechanics: access to information on a given systems passes through a nondeterministic process (measurement). In computer sciences, randomness is at the core of algorithmic information theory, all the while nondeterministic algorithms and networks present crucial random aspects. Finally, an extensive use of randomness is made also in biology.

Thus we wondered: all these different sciences refer to a concept of randomness, but is it really the same concept? And if they are different concepts, what is the relation between them?

Let us analyse in more detail the kind of randomness that emerges in the various disciplines.

### 1.1. **Physical randomness (classical).**

A kind of randomness can be viewed as a property of trajectories within classical dynamical systems, namely as unpredictability in finite time, over approximated physical measure with a given (non reducible) precision, [2, 3, 20, 7, 34, 35]. Moreover, ergodicity (à la Birkhoff) provides a relevant and purely mathematical way to define randomness asymptotically, in the limit of infinite trajectories, which still applies for deterministic systems inspired by physics, but independently of chaotic properties (unpredictability) of physical processes, [18, 36]. In short, within these deterministic frames, randomness can be derived from a comparison between time averages (along a trajectory starting from a point) and space averages (over the entire space) of the chosen observables.

### 1.2. **Physical randomness (quantum).**

Randomness in quantum mechanics has a special status, as it is of intrinsic origin. In contrast to other fields , including classical and relativistic physics, quantum randomness (QR) does not appear as a mean of "hiding" a kind of lack of knowledge, like, e.g., in statistical physics. The experimental evidence of the violation of the Bell's inequalities definitely proves that QR really belongs to the paradigm of the theory.

Yet, on the other side, QR fits perfectly well on the axiomatic setting of quantum mechanics, it is part of the 4 axioms of the so-called "Copenhagen" formalism, and the perfect coherence with the other postulates is a great success of the sciences of the last century.

Observe, in particular, that a quantum algorithm cannot avoid randomness, as it provides, as "output", i.e. the result of a final measurement process, a bunch of possibilities, one of them (fortunately the most probable) being the expected result. Therefore (easy) checking of the validity of a result must be part of the handled problem. The spectacular power of quantum algorithms, on the other side, overcomes this double constraint (randomness of the result and necessity of a posteriori validation of the "guess") and fully justifies this new branch of computer sciences. In this perspective, quantum randomness cannot be viewed as a form of (hidden or incomplete) determination, [21, 4].

1.3. **Algorithmic randomness.** Also recursion theory gave us a proper form of (asymptotic) randomness, for infinite sequences, in terms of Martin-Löf randomness, [39] . This has been extensively developed by Chaitin, Schnorr, Calude and many others, [15], also in relation to physics, [51]. As a matter of fact, on the grounds of this theory one can give a precise meaning to vague notions such as "easily describable" and "regularities". In short, algorithmic randomness tests enables one to detect those elements whose regularities can be effectively tested, labeling them as "non-random". The elements that remain are called "random". Yet, the existing comparisons within (classical) physical randomness and algorithmic randomness are developed in formal space with insufficient physical generality. Some recent work went beyond this limit, [51].

1.4. **Computer science randomness.** Probabilistic and nondeterministic models of computation have been extensively investigated in the computer science literature, as well as their combination. Still there is no agreement about the precise nature of nondeterminism, and its relation with probability. In different areas the term nondeterminism refers to different concepts, and even in the same area people have different intuition and interpretation of nondeterministic models or phenomena (see for example [5] for a good survey). This confusion has brought consequences sometimes dramatic, especially when trying to transfer some theory or methodology from one field to another. One community which is particularly sensible to the problem is that of Computer Security. Although it was discovered only recently, the issue has rapidly become known and recognized as crucial, to the point that the organizers of the 2006 edition of the main forum in Computer Security, the IEEE FCS, set up a panel to discuss about nondeterminism.

In sequential computation the term nondeterminism refers to models in which the transition relation goes from one state to a set of states, like nondeterministic Turing machines. This is a useful device in specification, especially for search problems, in that it allows to explore alternative solutions without having to detail the backtracking policy. A characteristic of this kind of models is that their intended meaning is in terms of may-semantics, in the sense that the computation is considered successful if at least one of the alternative branches is successful. We argue that this has nothing to do with randomness: the re-execution of the system gives always the same result(s), and a deterministic implementation is always

possible via backtracking (in a breath-first fashion to avoid that infinite branches would cause a pitfall).

In concurrency theory the situation is very different [1]: nondeterminism is inherent to the model, in the sense that it arises naturally from the concurrent execution and interaction of parallel processes. More precisely, it generates from the different ways in which processes may alternate their execution steps, cooperate with each other, compete for resources, etc. In general, these processes are assumed to run in different nodes of a distributed network, and the intended meaning is in terms of the must-semantics, in the sense that every branch must be successful, because the execution follows only one of the many alternatives, and backtracking is not an option (it would be too expensive, if possible at all, because all the processes would need to be backtracked, in order to ensure consistency). The re-execution of the system gives a different result each time, determined by run-time circumstances. In general we want to abstract from these, and we use the notion of scheduler to represent how the choices are resolved.

1.5. **Biology.** A common characteristic in the various forms of physical randomness is the predetermination of the spaces of possibilities: random results or trajectories are given among already known possible ones (the six sides of a dice, the spin-up/spin-down of a quanton...). In fact, in quantum physics, even in cases where new particles may be created, sufficiently "large" spaces are provided upstream (the Fock spaces of which Hilbert spaces): Fock's spaces capture all the possible states, infinitely many in general. The classical methods transfer successfully in molecular analysis in Biology, where only physical processes are observed, even though there are meant to happen within cells.

In System Biology, however, phase or reference spaces (that is, the spaces of possible evolutions) are far from being predetermined. Typically, the proper biological observables of Darwinian Evolution, namely phenotypes and species [26, 33], are not pre-given or there is no way to give them in advance within a space of all possible evolutions, in a sound theory. And, of course, there is no way to pre-give the possible molecular interactions (internal and systemic) as well as the feedbacks, from the forthcoming ecosystems onto molecular cascades. An analysis of Species Evolution, in terms of a diffusion equation (thus of underlying random paths) is given in [8]. Our attention to the problem of randomness in System Biology was stimulated by these analogies and differences w. r. to Physics.

## 2. What have we learned?

Randomness is nowadays part of our culture. It appears everywhere. But, as mentioned before, it reflects very different kinds of conceptual (and mathematical) settings. Let us more closely review different forms of knowledge dealing with randomness in modern sciences.

2.1. **Physical randomness (classical).** In classical dynamics, it is possible to give a notion of individual random element. More precisely, in a dynamical systems, with a transformation $T$ preserving a measure $\mu$, there exists a natural class of (asymptotic) properties allowing a definition of "random state" with respect to the dynamic $T$ and the equilibrium distribution defined by $\mu$. This class is the one associated to the Birkhoff ergodic theorem which states that for each (integrable) function $f : X \to \mathbb{R}$ (representing a quantified observation), the time average of $f$ along the orbit $O(x) = \{x, T(x), T^2(x), ...\}$ converges to the spacial mean $\int f d\mu$ with probability one. Such points are called typical for $T$ [53]. Though given asymptotically, the definition has a robust physical meaning and it may be given for weakly chaotic dynamical systems : the mixing ones (that is, dynamical systems where observable decorrelates with time, see [23], [24]).

2.2. **Physical randomness (quantum).** The appearance of non-determinism in quantum mechanics was a shock. In the '20s Physics was still very rooted in the classical deterministic view of the world. Therefore it took a lot of time to accept this fact, although it appears totally natural now to us that a description on the world could be fully statistical. This randomness flavour of quantum mechanics is usually handled in the so-called field of "conceptual aspects" of the theory,[31]. Facing these conceptual aspects with new experimental physics is not so frequent, and the relationship with other fields, as the ones presented here, are even less often considered. At the meantime recent works (see [46, 47, 48, 49]) started invoking these links. Let us finally mention a kind of philosophical morality: the high new power of quantum algorithms relies on randomness, that is, releasing determinism (in a way of keeping probability predictions) increases drastically efficiency.

2.3. **Algorithmic randomness.** As already mentioned, the notion of individual random infinite sequence has been effectively modeled with the tools of computability theory. The idea is that statistical tests may be "effectively given", that is one can effectively look for regularities along infinite sequences. Then an infinite sequence is random if it passes all effective tests. This algorithmic modelling of randomness has been formalized in different ways and there exist several definitions (the one by Martin-Löf's, in [39], being the most celebrated, see [15] for a survey book).

In these approaches, being random yields a high degree of "non-computability", as a random sequence has no infinite recursively enumerable subset. The role of algorithmic randomness in dynamical systems, especially in ergodic ones, has already be the subject of previous research. However, without a more general theory of randomness, all this work is restricted to "symbolic spaces" (spaces of strings), with little physical meaning. The non-obvious results recently obtained proved an equivalence, in very general and "physically meaningful" dynamical spaces, of the (classical) physical randomness, à la Birkhoff, and algorithmic randomness, for infinite trajectories (see the PhD theses by M. Hoyrup and C. Rojas (June 2008) and [23, 24, 38]).

As for finite time computations, Chaitin, Levin, Calude and many others, following Kolmogorof, deeply analysed also (finite) sequence incompressibility (sequences whose length coincides with their shortest generating program) and showed that for infinite sequences, under suitable conditions, the incompressibility of initial segments yields Martin-Löf asymptotic randomness. But, in our opinion, unless the physical generating process is spelled out, a finite incompressible sequence is not random, it is just algorithmically incompressible. In other words, it is pseudorandom in the strongest way and it is impossible to see in it any regularity whatsoever. Conversely, it is a reasonable thesis to assume that a physical random sequence is incompressible, in principle, but the converse is false or ill defined. That is, if one stays within theory of computation and no physical process is mentioned, there is no other way to give/conceive it but by a program, a formal/linguistic matter, a priori with no physical meaning. A closer analysis of this issue is part of our project, in view of our experience on the relation physical (dynamical) vs. algorithmic randomness.

2.4. **Randomness in computer science.** As argued in previous section, sequential systems are inherently deterministic (despite the use of the adjective 'nondeterministic' for the automata whose transition relation is one-to-many). Concurrency, on the contrary, seems to give rise to a true notion of randomness, due to the unpredictable and unbacktrable nature of interaction between independent and asynchronous agents.

The fact that computation in concurrent systems seems to have features which are basically different from those of sequential computation has inspired some intriguing lines of research, with the common goal of defining a 'good' notion of expressiveness for concurrent formalisms. One of the most successful approaches is based on the notions of 'encoding', and it has produced some interesting results concerning the mechanisms of guarded choice, which are intimately related to the nature of nondeterminism in concurrency. We mention in particular the works by Nestmann and Pierce [41], and by Palamidessi [44, 45]. The first have shown that a certain form of choice (input-guarded choice) can be encoded in parallelism, while the latter has shown that mixed-guarded choice is essentially more expressive.

Another line of investigation has been pursued by Wegner and his collaborators. Starting from the principle that interaction is more expressive than algorithms, Wagner has written an intriguing position paper where he justifies this claim, essentially on the basis of the intuition that interaction can express random computation [54]. In the technical development of this idea in subsequent papers [55, 25] the authors considered a sort of interactive Turing machines (persistent Turing machines) and showed that they cannot be reduced to standard Turing machines. However the approach is based on the conventional interpretation of nondeterminism in automata theory.

An interesting result has bee found recently by Busi and her colleagues [13]: they investigate a process calculus (CCS with replication) and show that in this calculus the existence of a divergent path is decidable. Still, in a subsequent paper

[14] they show that this formalism can encode Turing machines. The explanation of this apparent paradox is that the nondeterminism of the language is essential to achieve Turing-completeness: any attempt to eliminate it in an effective way is doomed to fail, because otherwise decidability of (existence of) divergence would imply decidability of termination.

In all the above investigations nondeterminism plays a central role: since in concurrency there is no backtracking, it becomes important to control nondeterminism as much as possible, and the expressive power of a concurrent language usually lies on the capability to exert such control.

In a more practical fashion, nondeterminism has been used in concurrency theory as a convenient abstraction from run-time information. Essentially, a concurrent program is nondeterministic because when we write it we do not know yet what will determine at run-time the choice of a particular path, so all the possibilities must be considered.

A common misconception of nondeterminism is to consider it a probabilistic mechanism with uniform distribution. The confusion probably originates from epistemic considerations: the total lack of knowledge about which of the available alternatives will be chosen, in a nondeterministic process, evokes the concept of maximum entropy. But maximum entropy represents the maximum degrees of uncertainty within the probabilistic setting. Nondeterminism is outside the realm of probability and it represents an even higher degree of uncertainty. In any case, confusing nondeterminism with uniform probability has induced wrong approaches. We argue that this due to several aspects: not only a nondeterministic property cannot express the quantitative aspects of a probabilistic one, but also this transformation requires angelic nondeterminism (nondeterminism working in favour of the property), which is a strong assumption usually not guaranteed in a concurrent setting (where nondeterminism is typically demonic).

2.5. **Biology.** We have no doubt that the issue of randomness in biology is extremely difficult, yet it is amazing to observe that leading biologists, still now and along the lines of Crick and Monod ([40]), contrapose determination and randomness according to Laplace's split: deterministic means predictable and random is its opposite (non-deterministic), to be analyzed by statistics and probabilities. Along these laplacian lines, deterministic, as it implies predictability (Laplace's conjecture), yields "programmable", which leads to the the idea that the "DNA is a program" (see [22] for an history.) Yet, since Poincaré (1890), we know that classical randomness is deterministic unpredictability and that unpredictability pops out almost everywhere in non-linear systems (see [37] for a critique of the claim that "DNA is a program" from the point of view of Physics and Programming Theory.)

In short, determination as "necessity" in life phenomena, understood in a laplacian way, is far from the frameworks of modern determination in physics, classical or quantum, even if it is supplemented by a few speckles of randomness (le "hasard"). Crick's "central dogma" ("Genetic Information" goes one-way, from

DNA to RNA to proteins - and to the phenotype) and the "one gene - one enzyme" hypothesis in Molecular Biology are good examples of this. They guided research for decades and, the first, is still nowadays believed by many, modulo the addition of a few "epigenetic factors" and "norms of reaction" (for an alternative view, see [27]; more discussions and references are in [37]). By their linear causality, these assumptions do not seem to have still integrated the views on the interplay of interactions in XXth century physics, that is the richness of the approaches to physical determination and randomness. In these modern physical frames, causes become interactions and these interactions themselves dynamically constitute the fabric of the processes and of their manifestations; reshaping this fabric modifies the interactions, intervening upon the interactions appears to reshape the fabric, [6].

Our recent work on entropy in System Biology, [8], has been extensively borrowing from the work on far-from-equilibrium thermodynamics, in particular dissipative systems ([42, 43]). Note that entropy provides a measure for "increasing randomness" also for dynamical systems and this establishes a link, developed by many, with other areas of physics (thermodynamics).

## 3. What are the most important open problems in the field?

"Random" is not the opposite of "deterministic", in spite of the opposition of these concepts that is commonly made in Computer Science and Biology. As a matter of fact, the analysis of randomness is part of the proposal for a structure of determination of physical processes, in particular in classical dynamics, where randomness is deterministic unpredictability. But it is so also when it is related the very precise and specific notion of quantum indetermination and quantum measure of "deterministic evolutions of the state function" (determined by Schrödinger equation).

As seen in the previous sections, randomness and nondeterminism appear at least in four thematic fields (mathematics, physics, biology and computer sciences). Yet, they cover different, sometimes antinomic meanings.

3.1. **Algorithmic randomness.** Since Chaitin's 1975 construction of the first random infinite word, an entire robust field has been opened concerning the combinatorial properties of randomness in discrete frames. This is leading to an interesting analysis of infinite sequences and cycles in de Bruijn graphs, for example, and a lot more in finite and infinite combinatorics.

A way to stress the difference and the strength of the approach we worked at, is that, given a measurable space of measure $\mu$, classical theorems like "property P holds for $\mu$-almost every point" can be converted into "property P holds for every $\mu$-random point", and this in physical dynamics. Now, the notion of "being ($\mu$-)random", relatively to a measure $\mu$, is fully understood, by the many result in algorithmic randomness and, in particular, by our team's work on asymptotic randomness, relating classical (dynamical) and algorithmic randomness. In short,

a major point of these results, is given by the use of discrete, though asymptotic, tools from algorithmic randomness, in applications to continuous dynamics. By this, our approach, by its relation to physically meaningful dynamical systems, complements the relevant existing work on algorithmic randomness. Further applications (or correlations between) the recent ideas in algorithmic randomness, like the ones developed by the authors above, and our understanding of classical (and quantum) dynamics is one of the paths to be explored. In particular, a typical example of cross interest is given by the analysis of normality in the sense of Borel[1]: a real number is absolutely normal with probability one, but constructing such points is extremely complicate [12]. However, it is widely accepted that computable simulations show the right ergodic behaviour [53]. Is it the case also while modelling relevant physical dynamics? and which ones? We will hint below on how a relation to our approach can be developed.

3.2. **Computer science.** In section 2, we mentioned the ambiguities we see in the transfer of notions from algorithmic randomness (an asymptotically well-defined notion) to finite time computations. Some may see our questioning as referring to a terminological nuance, yet too much confusion in computing deserves clarification. Consider, say, a so called "non-deterministic" Turing Machine. This is just a formal, deterministic device, associating a set of numbers to a number. Its evolution is determined by an ill-typed input-output function. Indeed, it is a useful device as it allows to speed up computations by a form of basic parallelism. Yet, as long a physical process, choosing, at each step, one or a few of the elements in the output set, is not proposed, one cannot discuss about "determination" nor "randomness": is it classical? quantum? This is an analogue of the problem posed for finite "random" (incompressible!) sequences mentioned above. A major clarification is needed here, as the relation between the abuses of "non-deterministic", "random" in Computer Science deserve a close analysis in terms of their relation to the underlying physical processes.

We need to tackle this problem within the relevant area which mostly interests, concurrency and networks. In particular, the following three main objectives seem relevant:

Clarify the nature of nondeterminism in concurrency. As discussed in previous sections, there is a lot of confusion about this concept, especially in the way the notions and tools developed in the area of concurrency get applied in other areas. We feel that this is because the concept of nondeterminism is still missing a proper characterization, formalization, and theoretical foundations. The way it is formalized in process calculi, indeed, makes it easy to confuse it with the 'nondeterminism' of automata theory, which, as argued previously, has a radically different nature.

[1]A "normal number" is a real number whose digits in every base show a uniform distribution, with all digits being equally likely, all pairs of digits equally likely, all triplets of digits equally likely, etc..[10]

Investigate and formalize the difference of concurrent computations with respect to sequential ones. With respect to Wegner's claim that 'interaction is more powerful than algorithms' on the basis of the fact that interactive (concurrent) systems can create real random sequences, our position is: we actually do not believe that it is a matter of interaction having a superior expressive power (if anything, it should be the reverse - randomization witnesses a lack of control capabilities), but certainly the capability of producing randomness sharply separates interactive (concurrent) computations from algorithmic (sequential) ones. Once this characterization in terms of randomness is given, we can also explore whether we can characterize different classes of random sequences, which would induce a separation in the concurrent formalisms (and mechanisms) that can produce them.

Explore the use of physical randomness (classical and quantum) for computer science applications that use randomized mechanism to protect secret information. Typically randomization is used to obfuscate the link between secrets and observables, and the use of really unpredictable mechanisms (in contrast to the pseudo random ones) is critical. Examples of such applications are protocols for privacy, anonymity, and confidentiality [52], like Crowds and DCnets. How non-linear systems, reflecting classical randomness, or intrinsic quantum randomness can help in the developments of these areas?

3.3. **Biology.** A long term ambition would be to obtain, by mathematics if possible, a clarification of the not so much explored problem of randomness in System Biology (again, in Molecular Biology, randomness plays a novel but fundamental role, but the tools and concepts are borrowed from Physics, via Chemistry). As we said, in a systemic approach to Biology, one of the challenges, as for our project, is that species (and phenotypes) are co-constituted with their environment.

To make an analogy with the reasons for chaos in planetary systems, some sort of "resonance effect" takes place in this co-constitutive process. The difference is that in the physical deterministic case, the resonance happens at one (and conceptually simple) level: the gravitational interactions between a few planets, fully determined by Newton-Laplace equations. In Evolution (but also in ontogenesis), the resonance takes place between different levels of organization, each deserving an analysis on terms of an appropriate structure of determination (typically, fractal structures or geodetics in morphogenesis, see [28], vs. networks dynamics in cellular/neural tissues, see [30].

That is, a systemic approach requires an analysis of interactions between species, individuals, physical landscapes, but also organs and tissues and, very importantly, by two ways interactions between these levels and molecular activities, starting with DNA expression. Moreover, molecular events belong to microphysics, thus possibly subject to quantum analysis, thus, quantum probabilities. By this, one would need a theory encompassing both classical randomness, which may better fit the description of macroscopic interactions, and quantum randomness, as they may be retroacting one on top of the other. We are far form having such a theory, even in Physics.

In conclusion, Physics has been able to propose two different notions of randomness in finite time: classical deterministic unpredictability and quantum randomness. As we mentioned, we proved that they merge in infinite time. Biology badly needs its own notion, while in search, of course, for unification with physical (molecular?) structures of determination. We observe that the notions of "extended criticality" and "anti-entropy" (the opposite of "increasing disorganization or randomness", yet differing from the classical negative entropy) recently proposed in [8], [9] seem pertinent. They deeply involve randomness in Biology, by the role of fluctuations in extended criticality and of random paths in the formation and growths of anti-entropy.

3.4. **Quantum mechanics.** Since the beginning of the '80s, and especially the fundamental experiments by Aspect et al, showing the violation of Bell's inequalities, quantum mechanics has got the status of "true" theory of the microscopic world. Roughly at the same time appeared the beginning of what is called now quantum information and quantum computing.

Feasibility of the construction of quantum computers is certainly one of the most challenging perspective in physics. More generally experimental exhibition of single phenomena in quantum mechanics is certainly one of the most striking success of sciences of the last 25 years. In the mean time computer science developed, independently, in a direction where non-determinism took an increasing place. An objective would be to exhibit links between these two independent developments, together with possible oppositions. As a bi-product, incidence of the rich computer network theory on quantum mechanics is also expected to be strengthened.

## 4. What are the prospects for progress?

4.1. **Quantum randomnesses.** One of the subjects that should be seriously carried out is the difference, in quantum mechanics, between two different type of randomnesses: the one obtained through decoherence and the one of the measurement process (see [29]). Indeed it is often said that decoherence presents a satisfactory "explanation" of quantum measurement. Let us remind that the phenomenon of decoherence is the action on a "small" quantum system of the big quantum surrounding system (e.g. the apparatus). In the limit of infinite "reservoir" the state of the small system gets a diagonal feature that one can identify with a statistical mixture. This last one is sometimes and wrongly presented as reflecting the quantum randomness, as randomness in statistical mechanics. This point of view, driven by a pure statistical perception of quantum phenomena, must be corrected, as more and more single events in quantum mechanics are nowadays shown experimentally. It seems to us that a clarification of the link between this dichotomy between (not intrinsic) randomness and the true (intrinsic) one on the quantum side, and the same kind of distinction in the other fields presented all a long this paper, would be a major achievement.

4.2. **Pseudo-randomness and algorithmic randomness.** Computer simulations (the trajectory given in some initial condition and drawn on the screen) has become a very important component of the analysis of physical dynamics. The problem is that an algorithmically random point is strongly non-computable, and consequently it is impossible to observe the trajectory of such a point in a computer simulation. Worst, the set of computable points has probability 0! From the simulation point of view, the fact that a given property holds with probability one says nothing about its observability with a computer. A typical example is (absolute) normality in the sense of Borel, but, as we mentioned, constructing such points is extremely complicate.

As already mentioned, in spite of this intrinsic (mathematical) difficulties, it is widely accepted that computable simulations display the right ergodic behaviour. The evidence is mostly heuristic. More precisely, most arguments are based on the various "shadowing" theorems. By these results, it is possible to prove that in a suitable system any "pseudo"-trajectory, that is a trajectory obtained by a simulation with round-off, is approximated by a real (continuous) trajectory of the system (but, in general, not the converse). The main limit of this approach is however that shadowing results hold only in particular systems ("hyperbolic" dynamics), while many physically interesting systems do not need to belong to this class. Can we extend this frame for shadowing to an analysis of randomness for the systems of biological and physical relevance, both for finite and infinite processes? What does this mean in a quantum perspective?

Moreover and as observed in the previous sections, algorithmically random points are those points which have the "generic" behavior, as prescribed by the underlying measure. In a sense, they are physically "randomized", as they do not possess any artificial feature related to the particular supporting space. An open issue would be to turn this into a mathematical frame, where the only role of the measure would be to distinguish the set of random points and give them a topological structure. Once this is done, probabilistic theorems can be formulated and proved using the structure of the random set and topological methods (without referring to the measure).

4.3. **Computer science.** The objectives proposed in previous section should be pursued by applying the following approaches and methodologies:

Clarify the nature of nondeterminism in concurrency. The results and perspectives developed in mathematics and physics and quoted above should be more closely used to get new insights that can be used to understand in depth the notion of nondeterminism in concurrency, in its intrinsically random nature. On this basis:

Formalize the difference between concurrent and sequential computation in terms of randomness. What about the applicability of Martin-Löf definition of randomness to give this characterization?

Explore the use of physical randomness (classical and quantum) for computer science applications. Typically, it should be explored the possible use of different kinds of randomness in quantum mechanics (see the paragraph on quantum randomnesses in this section), as well as the extensively studied relations between computational and dynamical randomness in enriching/clarifying randomness in finite computing: how can this affect computing? (on a conceptual basis? by the relevance of hardware?)

4.4. **Extended Criticality in Biology.** In recent work [9] we proposed to analyze the state of living matter as "extended critical state". The idea is that an organism is in a permanent critical transition, constantly reconstructing its own organization. The well established domain called "physics of criticality" [32] necessarily deals with point-wise critical transitions: this is part of the very definition of phase transition and it is used in an essential way by the main mathematical tool in the approach, the "renormalization methods" ([19]) In ongoing work, we consider, instead, a set (whose closure is) of null-measure, an extended interval of criticality w.r. t. all pertinent parameters (time, temperature, pressure...). It is as if a snow flake (a "coherence structure", formed at a critical transition) could stand variations within a relatively large interval of its control parameters by continually reconstructing itself, in a permanent "going through" the critical transition (extended criticality applies to far from equilibrium, dissipative and not necessarily steady states). One then has an extended, permanently reconstructed global organization in a dynamic interaction with local structures, as the global/local interaction is proper to critical transitions. The role of randomness in these context is crucial, yet to be explored: the structural stability of the system may be seen as stability w. r. t. perturbations within the margins of criticality. Moreover, the very construction of the coherent state is obtained from fluctuations from an initial relatively stable state. The point now is to turn these conceptually robust ideas into sound mathematics. As the normalization methods cannot work, by principle (non-pointwise nature of the critical "transition"), how to describe and handle rigorously extended criticality and its main properties (the establishment and maintainance of the global coherent structure, its structural stability and complexity, in particular in relation to random events)?

Extended criticality, a notion modeling organisms as "extended coherence structures" (our proposal for structurally stable systems), needs also to be merged with the work on entropy and anti-entropy in Species Evolution, mentioned above, see [8]. The possible technical link may reside in the role of randomness in both analyses. This shows up in fluctuations and resistance to perturbations (average behaviours?), as for extended criticality, in diffusion equations (thus, in underlying random paths) as for entropy and anti-entropy. In this frame, one needs to further analyse the role of time and of diffusion equations (which average random paths) both in phylogenesis (we already carried on a mathematical analysis of this in [8]) and in ontogenesis, an open issue.

4.5. **Comparison.** It should be clear that the many forms of randomness above differ or, in some cases, are not or ill formalized. Yet, as already mentioned, some recent results of our's prove that they merge, asymptotically. In particular, we recall, one of us proved an asymptotic merging of quantum and classical randomness at the so-called "semi-classical limit" [48] and the team of another of us proved a form of equivalence between Birkhoff physical randomness, a limit notion, and algorithmic randomness ([38] for a survey). This poses several open questions, for example in the correlations in *finite time* of classical, quantum and algorithmic randomness, an issue extensively studied by many, since the asymptotic analysis may propose a new perspective. Moreover, as we said, the computational approach (algorithmic randomness) is far from being related to the modern forms of randomness in networks and concurrency. Not to mention the very difficult and rather confusing situation we can witness in Biology, when coming from more mathematized disciplines.

## References


[1] Aceto L., Longo G., Victor B. (eds.) The difference between Sequential and Concurrent Computations. Special issue, Mathematical Structures in Computer Science, Cambridge U. Press, n. 4-5, 2003.

[2] Adler R. L. Topological entropy and equivalence of dynamical systems, American Mathematical Society, 1979.

[3] Alligood K., Sauer T., Yorke J., Chaos: an introduction to Dynamical Systems, Springer, New York, 2000.

[4] Anandan J. Causality, "Symmetries and Quantum Mechanics". Foundations of Physics Letters, vol.15, no. 5, 415 438, October, 2002.

[5] Michal Armoni and Mordechai Ben-Ari. The Concept of Nondeterminism:. Journal of Science & Education, Springer, 2008

[6] Bailly F., Longo G., Mathématiques et sciences de la nature. La singularité physique du vivant. Hermann, Paris, 2006 (English introduction, downloadable; ongoing translation).

[7] Bailly F., Longo G. "Randomness and Determination in the interplay between the Continuum and the Discrete", Mathematical Structures in Computer Science, vol. 17, n. 2, 2007.

[8] Bailly F., Longo G. "Biological Organization and Anti-Entropy", to appear in Journal of Biological Systems, 2008.

[9] Bailly F., Longo G. "Extended Critical Situations", in J. of Biological Systems, Vol. 16, No. 2, pp. 309-336, June 2008.

[10] Becher V.,Figueira S.,. Picchi R, "Turing's unpublished algorithm for normal numbers", Theoretical Computer Science, Volume 377 , 126–138, 2007,

[11] Becher V. ,Dickmann M. , "Infinite sequences on de Bruijn graphs", manuscript 2007.

[12] Becher V.and Figueira S.. An example of a computable absolutely normal number. Theor. Comput. Sci., 270(1-2):947-958, 2002.

[13] Busi N., Gabbrielli M., Zavattaro G.. Replication vs. Recursive Definitions in Channel Based Calculi. ICALP 2003: 133-144

[14] Busi N., Gabbrielli M., Zavattaro G.. Comparing Recursion, Replication, and Iteration in Process Calculi. ICALP 2004: 307-319

[15] Calude C. Information and Randomness: An Algorithmic Perspective. Springer-Verlag New York, 1994.

[16] Calude C., Stay M. "From Heisemberg to Gödel via Chaitin", International J. Theor. Phys. 44 (7), 2005.

[17] Chaitin, G. A theory of program size formally identical to information theory. Journal ACM, 22:329–340, 1975.
[18] Cornfeld I., Fomin S. and Sinai Ya. G., Ergodic Theory. New York: Springer-Verlag, 1982.
[19] Delamotte B., A hint of renormalization, American Journal of Physics 72, pp. 170-184, 2004.
[20] Devaney R. L., An introduction to Chaotic Dynamical Systems, Addison-Wesley, 1989.
[21] Feynman R., Lectures in Physics. Addison-Wesley, 1966.
[22] Fox Keller E., The Century of the Gene, Gallimard, 2000.
[23] Galatolo S., Hoyrup M. and Rojas C., "Effective symbolic dynamics, random points, statistical behavior, complexity and entropy", to appear in Information and Computation, 2009.
[24] Galatolo S., Hoyrup M. and Rojas C., "A Constructive Borel-Cantelli lemma. Constructing orbits with required statistical properties", Theoretical Computer Science, 410(21-23):2207-2222, 2009.
[25] Goldin D., Smolka S., Wegner P.. Turing Machines, Transition Systems, and Interaction. Electr. Notes Theor. Comput. Sci. 52(1), 2001
[26] Gould S. J. Wonderful Life, WW. Norton, 1989.
[27] Kupiec, J.-J. et al. (eds), Le hasard au coeur de la cellule, Sylleps, Paris, 2009.
[28] Jean R. V. Phyllotaxis : a systemic study in plant morphogenesis, Cambridge University Press, 1994,
[29] Haroche S., Raimond J.M., Exploring the quantum : atoms, cavities and photons ,Oxford U.P. graduate texts 2006.
[30] Hertz, J., Krogh, A., Palmer, R. (1991) Introduction to the Theory of Neural Computation, New York: Addison-Wesley.
[31] Jammer M.. The philosophy of quantum mechanics : the interpretations of quantum mechanics in historical perspective, Willey New York, 1976.
[32] Lagues M., Lesne A. Invariance d'echelle, Belin, Paris, 2003.
[33] Lecointre G., Le Guyader H., Classification phylogénétique du vivant, Paris, Belin 2001.
[34] Lighthill J. The recent recognized failure of predictability in Newtonian dynamics, Proc. R. Soc. Lond. A 407, 35-50, 1986.
[35] Laskar J., "Large scale chaos in the Solar System", Astron. Astrophysics, 287, L9 L12, 1994.
[36] Longo G., Paul T., "The Mathematics of Computing between Logic and Physics". Invited paper, Computability in Context: Computation and Logic in the Real World, (Cooper, Sorbi eds) Imperial College Press/World Scientific, 2008.
[37] Longo G., Tendero P.-E., "The differential method and the causal incompleteness of Programming Theory in Molecular Biology". In Foundations of Science, n. 12, pp. 337-366, 2007.
[38] Longo G. Randomness and Determination, from Physics and Computing towards Biology. Invited Lecture at the 5th International Conference on: Current Trends in Theory and Practice of Computer Science, Spindleruv mlyn (Czech Republic), January 24-30, 2009, to appear in Lecture Notes in Computer Science, Springer, 2009.
[39] Martin-Loef, P. "The definition of random sequences". Information and Control 9: 602-619, 1966.
[40] Monod J. Le Hasard et la Nécessité, PUF, 1973.
[41] Nestmann U., Pierce B.. Decoding Choice Encodings. Inf. Comput. 163(1): 1-59, 2000
[42] Nicolis G., Prigogine I., Self -Organization in Nonequilibrium Systems, J. Willey, 1977.
[43] Nicolis G., "Dissipative systems", Rev. Prog. Phys., IL, p. 873, 1986.
[44] Palamidessi C. Comparing The Expressive Power Of The Synchronous And Asynchronous Pi-Calculi. Mathematical Structures in Computer Science 13(5): 685-719, 2003
[45] Parrow J.. Expressiveness of Process Algebras. Electr. Notes Theor. Comput. Sci. 209: 173-186, 2008

[46] Paul T. "La méeanique quantique vue comme processus dynamique", in "Logique, dynamique et cognition" (dir. J.-B. Joinet), collection "Logique, langage, sciences, philosophie", Publications de la Sorbonne, Paris, 2007.
[47] Paul T. , "Échelles de temps pour l'évolution quantique à petite constante de Planck", Séminaire X-EDP, École Polytechnique, Palaiseau, 2008.
[48] Paul T. , "Semiclassical analysis and sensitivity to initial conditions", Information and Computation, **207**, p. 660-669 (2009).
[49] Paul T. , À propos du formalisme mathématique de la Mécanique Quantique , "Logique & Interaction : Géométrie de la cognition" Actes du colloque et école thématique du CNRS "Logique, Sciences, Philosophie" à Cerisy, Hermann, 2009.
[50] Pour-El M.B., Richards J.I., Computability in analysis and physics. Perspectives in mathematical logic, Springer, Berlin, 1989.
[51] Rojas C. "Computability and Information in models of Randomness and Chaos", Math. Struct. in Computer Science, vol. 18, pp 291-307, 2008.
[52] Schneider S., Sidiropoulos A. : CSP and Anonymity. ESORICS 1996: 198-218
[53] V'yugin, Vladimir V., "Ergodic Theorems for Individual Random Sequences", Theoretical Computer Science, vol. 207, p.343-361, 1998.
[54] Wegner P. Interactive Foundations of Computing. Theor. Comput. Sci. 192(2): 315-351, 1998
[55] Wegner P., Goldin D.. Coinductive Models of Finite Computing Agents. Electr. Notes Theor. Comput. Sci. 19, 1999

CNRS and Département d'Informatique UMR 8548, École Normale Supérieure, 45, rue d'Ulm - F 75730 Paris cedex 05
*E-mail address*: http://www.di.ens.fr/users/longo/

CNRS and Département de Mathématiques et Applications.UMR 8553, École Normale Supérieure, 45, rue d'Ulm - F 75730 Paris cedex 05
*E-mail address*: paul@ dma.ens.fr

INRIA-Saclay and LIX, École Polytechnique, Rue de Saclay, 91128 Palaiseau
*E-mail address*: catuscia@lix.polytechnique.fr