The quantum coin toss — testing microphysical undecidability

Karl Svozil*

Institute for Theoretical Physics,

Technical University Vienna,

Karlsplatz 13, A–1040 Vienna, Austria.

Abstract

A critical review of randomness criteria shows that no–go theorems severely restrict the validity of actual "proofs" of undecidability. It is suggested to test microphysical undecidability by physical processes with low extrinsic complexity, such as polarized laser light. The publication and distribution of a sequence of pointer readings generated by such methods is proposed. Unlike any pseudorandom sequence generated by finite deterministic automata, the postulate of microscopic randomness implies that this sequence can be safely applied for *all* purposes requireing stochasticity and high complexity.

*Computer address: Bitnet (EARN): E1360DAB at AWIUNI11.

1. In a strictly formal sense, any "proof" of randomness is among the most demanding tasks perceivable [1, 2] — indeed it is equivalent to finding all *true* (not merely all *provable*) mathematical theorems in an attempt to "solve the unsolvable"[3]. This idealistic goal turns out to be impossible [4, 2, 5]. For this and deeper [6] reasons it is suggested to drop a rather speculative terminology and substitute the humbler term *undecidable* for "randomness" when it comes to physical operationalizations. *A sequence of physical events is said to be undecidable if it is not possible to predict the forthcoming events by knowledge of previous ones.* The term *randomness* will be reserved for the formal notion defined below.

Undecidability is a relative concept. The ability to find a law predicting events depends on rather subjective criteria: Experience and intuition are very often the only guiding principles, and finding laws is nothing less but a great and rare art. If these attempts fail, then the events are undecidable *with respect to the corresponding trials and efforts*. Of course that does not imply that there are no laws. — These heuristic considerations are supported by the provable fact that there exists no systematic ("deductive") method to derive laws even for arbitrary finite sequences of data [7]. The same is true for statistical tests: statistical tests correspond to "laws" in the sense that failure of statistical tests (of randomness) implies that significant predictions are possible. A sequence "looking" perfectly random may pass various statistical tests but fail others. Thus it should always be clearly spelled out *with respect to which test(s)* undecidability has been proved.

The following *Gedankenexperiment* illustrates the relativity of the notion of undecidability (and of randomness). Consider a physical system Σ producing numbers on a display. Assume an observer A, for whom Σ for all practical purposes is a "black box"; i.e., despite the display A has no knowledge of Σ. Assume a second observer B, who by intuition or other insight knows that Σ calculates the digits of π, displays them, and in doing so has arrived at a specific n'th digit. In this case one may ask the following questions. *(i)* How does A without communicating with B learn about the "meaning" of Σ, i.e., how could A find out that Σ outputs the digits of π ? *(ii)* To what extend is the predictive power of B restricted by finite computational resources ? — What sense makes any "knowledge" claimed by B that Σ has arrived at the $n = 10^{200}$'th decimal place of π ? For even if one uses a whole galaxy as computer, and even if one is willing to wait for the result of the computation for a time comparable to the age of the universe, at least with

present–day mathematical means, it is impossible to confirm this statement and to predict the $10^{200}+1$'th decimal place of π [8, 9].[1] Although ideally π can be calculated deterministically to an arbitrary precision, one is forced to a probabilistic description by restrictions in computational resources and intuition — this was, after all, the perception of Laplace's "old" probability theory.[2]

The above *Gedankenexperiment* is no exception. There are rather few physical systems whose evolution can be predicted [3]. Statistical tests sometimes are very weak hints on the stochastic nature of the underlying evolution. Take for instance the simplest nontrivial sequence build from natural numbers 1, 2, 3, $\cdots$, enumerated in binary notation: $11011\cdots$. It can be shown that it is a Bernoulli–sequence [12], i.e. any arbitrary partial sequence occurs with the expected limiting frequency. The same has been demonstrated numerically [10] for the decimal expansion of π up to 26 million places and for partial sequences of length 6. What can be learned from these examples is that *sequences looking rather chaotic may stem from extremely low–complex deterministic evolution.*

The reverse is true as well. Randomness is prevalent in classical deterministic physics, where it is introduced *via* the continuum postulate [3]. Classical chaos is modeled by "unfolding" the randomness of the *real* initial values by a deterministic evolution. In quantum physics the situation is different. Although the quantum phase space is discrete and the Schrödinger equation for the wave function Ψ is deterministic, the probabilistic interpretation of $|\Psi|^2$ is mostly perceived as introducing indeterminism. This is most strongly felt for the occurrence of single microphysical events, when the ensemble interpretation may no longer be comfortably used. In what follows, emphasis is layed on this feature of quantum theory (see also ref. [13]).

2. Before concentrating on an operationalization, some mathematical

[1] To put it pointedly, although A may have no access to a CRAY 2 supercomputer, he might be willing to believe Bailey's claim [10] that the next ten digits following the 29 359 000'th digit in the decimal expansion of π are 3, 4, 1, 9, 2, 8, 4, 1, 7, 8, but he wont accept a claim such as *"with a probability greater than* $1/10$*, the* 10^8*'th digit in a decimal expansion of* π *is* 7*".*

[2] For completeness another problem will be mentioned here which is treated elswhere [6]: If the measurement process is intrinsic and selfreferential, i.e., the measuring device cannot be arbitrarily separated from the system to be measured, to what extent could the resulting data be used to make predictions ?

concepts of randomness are reviewed. Besides the intuitively evident but not very practical approach by von Mises [14, 15, 16], there are two relevant definitions of randomness, which are equivalent [2]. A sequence $x(n) = x_0 \cdots x_{n-1}$ is defined to be random if *(i)* it passes all statistical tests of randomness; or *(ii)* if there exists no finite size description of a "law" which is able to reproduce the sequence with arbitrary length.

The latter requirement of "lawlessness" can be represented in terms of *algorithmic complexity theory* envisioned by Chaitin, Kolmogorov and others [1, 2]. The algorithmic complexity $H(x(n))$ of a sequence $x(n)$ is the minimal program length necessary to output $x(n)$ on a computer, i.e., if p symbolizes the program running on a computer model C, then $H(x(n)) = \min_{C(p)=x(n)} \text{length}(p)$. A sequence is defined to be random if, as $x(n)$ increases in length n, $H(x(n))$ increases as well such that $\lim_{n\to\infty}[n - H(x(n))] < \infty$. Heuristically speaking, this definition implies that a random sequence cannot be substantially "compressed" by computational efforts, and any program outputting $x(n)$ boils down to mere enumeration, at best.[3]

In a strictly formal sense, randomness is undecidable [1, 2]. This is due to the fact that it is not systematically (i.e., deductively) possible to find the shortest program generating $x(n)$, or correspondingly, to perform all statistical tests on $x(n)$.

In practice one is restricted to a finite number of trial programs (or, correspondingly, of statistical tests) with no guarantee whatsoever that this is a proper collection. Moreover, all sequences of physical pointer readings are bounded in length ($n < \infty$). The pedagogical lesson to be learned from these kind of formalistic considerations again is that all practical "proofs" of undecidability (and even more so of randomness) are severely hampered by no–go theorems. Their preliminarity and relativity strongly restrict their validity and applicability.

3. We next turn our attention to the generation of suitable sequences of pointer readings $\psi(n) = \psi_0 \cdots \psi_{n-1}$ from "quantum coin tosses". These can then be subject to statistical and complexity tests, as suggested below (see also ref. [13]). For any test of quantum mechanical undecidability it is essential to use signals with no (extrinsic) noise from a controllable source

[3]There is no space here to discuss different definitions of randomness, such as *normalized* randomness, i.e., $K(x(n)) \equiv \lim_{n\to\infty} H(x(n))/n > 0$, which has important applications in *symbolic dynamics* [17, 6], or definitions of randomness based upon complexity measures [18, 16, 19].

of very low extrinsic complexity.[4] To the author's knowledge the optimal realization of such a source is a laser emitting coherent and polarized light. All emitted quanta from such a source are in an identical state. The polarized laser light is then directed towards a material with anomalous refraction, such as a $CaCO_3$ crystal, which is capable of separating light of different polarizations. Its separation axis should be arranged at $\pm 45^\circ$ with respect to the direction of polarization of the incident laser beam. Then each of the two resulting beams, denoted by 0 and 1, respectively, has a polarization direction $\pm 45^\circ$ from the original beam polarization. A detector is in each of the beam passes (see Fig. 1). For an ideal anomalous refractor, the probability that a light quantum from the polarized source will be in either one of the two beams is 1/2.

A binary sequence $\psi(n)$ can be generated by the time–ordered observation of subsequent quanta. Whenever the quantum is detected in beam 0 or 1, a corresponding digit 0 or 1 is written in the next position of $\psi(n)$, producing $\psi(n+1)$. In this way, n observations generate a sequence [11] $\psi(n)$.

It is suggested that such a sequence is published and suitably distributed (e.g. by electronic mail) by a *bureau of standards* [20]. This sequence could then be taken as a reference for statistical tests, some of which are suggested below, and more generally, as a standard for a generic random sequence.

This should be understood as follows. Compare ψ to any pseudorandom sequence φ, generated by a finite deterministic automaton. Whereas φ could be applicable to a great variety of purposes such as numerical integration or optimization of database retrieval, it will inevitably fail specific statistical tests. Take for example the statistical test corresponding to the generating algorithm of φ itself — the law which is encoded by this algorithm is *per definitionem* capable of generating ("predicting") all digits of φ. Thus, at least with respect to its own generation law, φ is provable nonrandom.

The postulate of microphysical indeterminism and randomness on the other hand asserts that there is no such "generating" law and hence no statistical test to "disprove" the randomness property of ψ. In fact, with this postulate ψ is characterized by the fact that it passes *all* statistical tests with probability one. Thus ψ can serve as generic source for a random bit sequence.

[4]The term "extrinsic" has been chosen to refer to external configurations only. Microphysical indeterminism is equivalent to the postulate of infinite "intrinsic" complexity.

4. In what follows several statistical and algorithmic tests are suggested which could be applied to $\psi(n)$.

(i) Frequency counting: for $\psi(n)$ to pass this test it has to be proven that any arbitrary sequence of m digits occurs in $\psi(x)$ with a limiting frequency 2^{-m}. In order to obtain a reasonable confidence level (see ref. [15] for details), m has to be smaller than approximately $n-7$. An infinite sequence passing this test for arbitrary m is called *Bernoulli sequence*. As has already been mentioned, this criterion is rather weak. It is satisfied by the enumeration of the natural numbers [12] and within finite accuracy, by the decimal expansion of π [10]. Actually, in the above experimental setup, the statistics of a 1–digit string ($m = 1$) should be used for calibration of a suitable angle, which is defined by the requirement that 0 and 1 should occur in $\psi(n)$ with frequency 1/2.

(ii) Algorithmic compressibility: $\psi(n)$ could be the input of various compression algorithms (e.g. the Huffman algorithm), which should produce a (compressed) string of length $H_c(n)$ with $H(\psi(n)) \leq H_c(n) \leq n$. On the average, $H_c(n)$ should increase as n increases, i.e., $\langle \Delta H_c(n)/\Delta n \rangle = 1$. Every compression algorithm is a kind of "code breaking device" based upon a hypothesis on "laws" governing sequences. Some of them are used for commercial applications and are readily available.

(iii) Spectral test: This is a critical test at least for linear congruential sequences. For a detailed discussion see ref. [15]. The idea is to investigate the "granular" structure of $\psi(n)$ in D–dimensional space in the following way. Split $\psi(n)$ into $N \equiv n/k$ subsequent partial sequences $\psi(n,i)$ of length k. Generate N binary numbers $0 \leq x_i < 1$ by $x_i \equiv \psi(n,i)/2^k$. For a D–dimensional analysis, arrange subsequent x_i's into $M \equiv N/D$ D–touples X_j. The X_j's could be perceived as points in $\mathbf{R}^D$. Consider further all families of $(D-1)$–dimensional parallel hyperplanes with points X_j. If $1/\nu(D)$ denotes the maximal distance of these hyperplanes, $\nu(D)$ is called the D–dimensional *"accuracy"* of $\psi(n)$. $\nu(D)$ should on the average be independent of the dimension, i.e., $\langle \Delta\nu(D)/\Delta D \rangle = 0$. For statistical reasons, one cannot achive a D–dimensional accuracy of more than about $2^{k/D}$ and $1/M^D$. Thus the spectral test is relyable only for $\nu(D) < 2^{k/D}$ and sequence length $n > kD(\nu(D))^D$.

(iv) High–dimensional integration: Assume an analytically computable D–dimensional integral $F(D) \equiv \int_0^1 \cdots \int_0^1 dx_1 \cdots dx_D f(x_1, \ldots, x_D)$. Consider again a representation of $\psi(n)$ into $M = n/kD$ points X_j in the D–dimensional

unit interval. Define $F'(D) \equiv (1/M) \sum_j f(X_j)$. Then for arbitrary test functions f and with probability 1, the discrepancy $|F(D) - F'(D)| \propto M^{-1/2}$ only depends on the number of points and not on the dimension.[5]

The proposed tests are not independent. Certain compression algorithms use tables of repeating sequences and are thus connected to frequency counting methods. The spectral test analizes the distribution of points generated from sequences in a unit interval of highdimensional space. It is thus a criterion for the quality of approximation in numerical integration.

There are other fairly strong statistical tests such as the law of the iterated logarithm [21, 14], but many of them turn out to be unpractical for their low confidence levels in applications.

5. In summary, it is proposed to investigate the postulate of undecidability of microphysical events by statistical and algorithmic tests. None of these actions can actually prove randomness, since due to no–go theorems which are ultimately based on Gödel's incompleteness theorems, such a proof is impossible. All one can attempt to do is to at least ensure the applicability of undecidable physical measurement series for particular tasks, such as theorem proving [22], Monte Carlo integration and database retrieval. It is further suggested to create and distribute such a sequence for testing and as a generic standard.

This work was supported in part by the Erwin Schrödinger–Gesellschaft für Mikrowissenschaften.

Figure captions

FIG.1 Experimental setup for generation of a sequence $\psi(n)$. Light from a polarized laser source is split into two beams of equal intensity, each having a polarisation direction of $\pm 45^\circ$ with respect to the original direction of polarisation. Incoming light quanta are then detected. Subsequent countings in detectors 0 and 1 correspond to subsequent bits of $\psi(n)$.

[5]For the Simpson method of numerical integration, in order to obtain accuracies of the order of $M^{-1/2}$, one needs at least $M^{D/8}$ points to obtain the same order of discrepancy. There the number of points depends on the dimension.

References

[1] G. J. Chaitin, *Information, Randomness and Incompleteness* (World Scientific, Singapore 1987)

[2] G. J. Chaitin, *Algorithmic Information Theory* (Cambridge University press, Cambridge 1987)

[3] J. Ford, *Chaos: solving the unsolvable, predicting the unpredictable*, in *Chaotic Dynamics and Fractals*, ed. by M. F. Barnsley and S. G. Demko (Akademic Press, New York 1986)

[4] K. Gödel, *Monatshefte für Mathematik und Physik* **38**, 173 (1931); english translation in M. Davis, *The Undecidable* (Raven Press, New York 1965)

[5] A *constructive* (i.e., realizable) *proof* of randomness would require a computable decoding scheme for random sequences. This would result in an effective solution of intractable problems, which is contradictory. For more details, see M. Baaz, N. Brunner and K. Svozil, *Gödel Jahrbuch* **2**, in print

[6] K. Svozil, *Physical undecidability as a result of Gödel's incompleteness theorem*, TU Vienna preprint 1987, unpublished

[7] This is equivalent to the *Turing problem*, see for instance M. Davis, *The Undecidable* (Raven Press, New York 1965)

[8] R. O. Gandy, *Limitations to Mathematical Knowledge*, in *Logic Colloquium '82*, ed. by D. van Dalen, D. Lascar and J. Smiley (North Holland, Amsterdam 1982)

[9] R. O. Gandy, *Church's Thesis and Principles for Mechanics*, in *The Kleene Symposium*, ed. by J. Barwise, H. J. Kreisler and K. Kunen (North Holland, Amsterdam 1980)

[10] D. H. Bailey, *Mathematics of Computation* **60**, 283 (1988)

[11] One perception of this process is the amplification of noise from the vacuum fluctuations of the photon field [see for instance R. J. Glauber,

Amplifyers, Attenuators and the Quantum Theory of Measurement, in *Frontiers in Quantum Optics*, ed. by E. R. Pikes and S. Sarkar (Adam Hilger, Bristol 1986)]. If, for any reason, this noise would exhibit *regular nonrandom* characteristics (rendering, for instance, amplitude oscillations $|\psi_t\rangle = \sin(\Omega t)\,|0\rangle + \cos(\Omega t)\,|1\rangle$ with constant frequency Ω), one could detect these regularities and find discrepancies with the postulate of microscopic randomness.

[12] D. G. Champernowne, *J. London Math. Soc.* **8**, 254 (1933)

[13] T. Erber, P. Hammerling, G. Hockney, M. Porrati and S. Putterman, *Annals of Physics (N.Y.)* **190**, 254 (1989)

[14] M. van Lambalgen, *Journal of Symbolic Logic* **52**, 725 (1987)

[15] D. E. Knuth, *The Art of Computer Programming (Vol. 2, 2nd edition)* (Addison–Wesley, Reading 1981)

[16] K. Svozil, *Logical Physics I — Foundations of Chaos*, TU Vienna preprint 1989

[17] V. M. Alekseev and M. V. Yakobson, *Physics Reports* **75**, 287 (1981); see also

G. Kreisel, *Synthese* **29**, 11 (1974);

R. P. Feynman, *International Journal of Theoretical Physics* **21**, 467 (1982);

C. H. Woo, *Phys. Lett.* **168B**, 376 (1986);

M. Minsky, *International Journal of Theoretical Physics* **21**, 537 (1982)

[18] St. Wolfram, *Physical Review Letters* **54**, 735 (1985); *Physica* **10D**, 1 (1984); *Rev. Mod. Phys.* **55**, 601 (1983)

[19] K. Svozil, *Are physical systems dynamically random ?*, TU Vienna preprint 1989

[20] A. Zeilinger, *private communication*

[21] W. Feller, *An Introduction to Probability Theory and Its Applications (Vol. 1)* (Wiley, New York 1950)

[22] The Babylonians allegedly "proved" an algebraic theorem (such as $n+m=m+n$), verifying it inductively by inserting "large" numbers. If the complexity of the numbers is much larger than the complexity of the theorem to be proven (i.e. intuitively speaking: there is nothing "special" about this number), then this inductive form of proof is legitimate. A deductive proof would require an equal amount of complexity. One arrives at this result by the following intuitive argument: one could attempt to prove an algebraic theorem $t(v)$ (v stands for the free variables) *deductively* by deriving it from axioms and rules of inference. The global derivation of t, containing all intermediate derivation steps, can be represented by a whole Gödel number $\#(t)$. $\#(t)$ is a sequence of characters which can be given a complexity measure $C(\#(t))$. One could define a proof to be "effective" if $\#(t)$ is finite random, that is if $C(\#(t)) \approx \#(t)$. Assume suitable representations of (finite) random numbers $r > \#(t)$. Intuitively, substitution of r for the free variables v in $t(v)$ yields an effective proof, since the computational complexity "investment" for the verification of $t(r)$ is greater than the complexity of an effective deductive proof of t. In this strange sense, *both inductive and deductive methods of proof are equivalent*. Of course, the inductive method requires sequences with a "guaranteed" amount of complexity.