Physical aspects of oracles for randomness, and Hadamard's conjecture

Karl Svozil

Institute for Theoretical Physics, Vienna University of Technology,
Wiedner Hauptstraße 8-10/136, A-1040 Vienna, Austria
svozil@tuwien.ac.at, url: http://tph.tuwien.ac.at/∼svozil

Abstract. We analyze the physical aspects and origins of currently proposed oracles for (absolute) randomness.

Keywords: stochastic processes, oracle computation, indeterminism, random number generator, quantum measurement

1 Metamathematical and metaphysical origin of oracles for randomness

Jozef Gruska's extensive reviews of the *foundations of computing* [11], and *quantum computing* [12] documents his continued interest in the foundations of, and the connections between, computation and physics. This encouraged me to contribute to the physics of computation, in particular, by discussing non-algorithmic oracles for randomness certified by physical principles.

The very existence of physical unknowables [17] and indeterminism is subject to an ongoing debate that can be expected not to terminate at any time soon. Thereby, like *Odysseus* trapped between *Scylla* and *Charybdis*, our perception of how the universe is organized has been vacuously oscillating between, and irritated by, claims of complete physical determinism on the one hand, as well as indeterminism on the other hand.

Rather than arguing for one side or another, I would like to state upfront that both positions are metaphysical; more precisely: from a physical perspective, these claims are non-operational. And, formally, by reduction to the *halting problem* [11, Sec. 642], both of them are provable unprovable. Because, form a purely phenomenological point of view, that is, in terms of the symbolic behaviour of physical systems, any proof of determinism would imply solvability of the *rule inference problem*, as well as total predictability even beyond the *Busy Beaver* bound. Likewise, any claim of total indeterminism encounters the problem of enumerating an infinity of "candidate theories of everything", let alone their future behaviour, as mentioned earlier.

Nevertheless, one way of corroborating physical indeterminism, which could then be used for the construction of evidence-based oracles for randomness, would be to "screw open" physical boxes which allegedly produce random bits.

We may not be able to do so, because, say, relative to certain physical assumptions and formal theorems such as complementarity and value indefiniteness, "nothing could be in" such boxes. But even then we may, at least, put forward some theoretical arguments which are based on what we are inclined to believe [3, 866]. In what follows we shall do exactly this: we mention such oracles for randomness; that is, some boxes containing allegedly indeterministic physical resources, and why we believe (or not believe) that they act as physical sources of random bits.

A necessary and sufficient condition for this is the existence of *gaps in the natural laws,* as discussed by Frank [8, Chapter III, Sec. 12]. Such gaps allow, or rather necessitate, "unlawful behaviour" which could be utilized for physical oracles of randomness.

2 Spontaneous symmetry breakdown and deterministic chaos

Already in 1873, Maxwell identified a certain kind of *instability* at *singular points* as rendering a gap in the natural laws [4, 211-212]: *"... when an infinitely small variation in the present state may bring about a finite difference in the state of the system in a finite time, the condition of the system is said to be unstable. It is manifest that the existence of unstable conditions renders impossible the prediction of future events, if our knowledge of the present state is only approximate, and not accurate. ... the system has a quantity of potential energy, which is capable of being transformed into motion, but which cannot begin to be so transformed till the system has reached a certain configuration, to attain which requires an expenditure of work, which in certain cases may be infinitesimally small, and in general bears no definite proportion to the energy developed in consequence thereof."*

Fig. 1 depicts a one dimensional gap configuration envisioned by Maxwell: a *"rock loosed by frost and balanced on a singular point of the mountain-side, the little spark which kindles the great forest, ..."* On top, the rock is in perfect balanced symmetry. A small perturbation or (pressure or thermal) fluctuation causes this symmetry to be broken, thereby pushing the rock either to the left or to the right hand side of the potential divide. This dichotomic alternative can be coded by 0 and by 1, respectively.

One may object to this scenario of *spontaneous symmetry breaking* by maintaining that, if indeed the symmetry is perfect, there is no movement, and the particle or rock stays on top of the tip (potential). Any slightest movement might either result from a microscopic asymmetry of the initial state of the particle, or from fluctuations of any form, either in the particle's position, or by the surrounding environment of the particle. For instance, any collision of gas molecules with the rock may push the latter over the edge by thermal fluctuations. Therefore, the randomness resides in the fluctuations, amplified by the instability. Whether or not any such fluctuation may be considered as creating a gap is a question related to debates in statistical physics mentioned later.

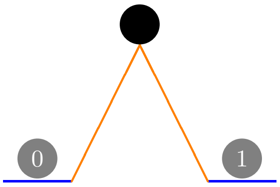

Fig. 1. (Color online) A gap created by a black particle sitting on top of a potential well. The two final states are indicated by grey circles. Their positions can be coded by 0 and 1, respectively.

A somewhat related scenario is that of *deterministic chaos,* because, as Poincaré pointed out [15, Chapter 4, Section 2, p.+56–57] *"it can be the case that small differences in the initial values produce great differences in the later phenomena; a small error in the former may result in a large error in the latter. The prediction becomes impossible and we have a "random phenomenon."*

3 Quantum beam splitter

A quantum mechanical gap can be realized by a beam splitter, such as a *half-silvered mirror*, with a 50:50 chance of transmission and reflection, as depicted in Fig. 2. A gap certified by quantum value indefiniteness necessarily has to operate with more than two exclusive outcomes [2]. Ref. [1] presents such a qutrit configuration.

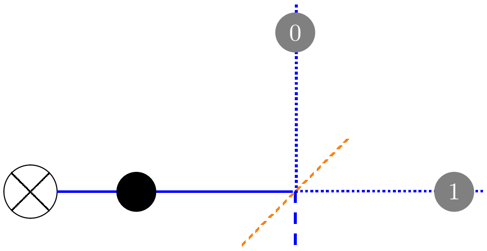

Fig. 2. (Color online) A gap created by a quantum coin toss. A single quantum (symbolized by a black circle from a source (left crossed circle) impinges on a semi-transparent mirror (dashed line), where it is reflected and transmitted with a 50:50 chance. The two final states are indicated by grey circles. The exit ports of the mirror can be coded by 0 and 1, respectively.

One may object to this scenario of *quantum indeterminism* by pointing out that it is merely based on a believe – actually, Born's *inclinations "to give up determinism in the world of atoms"* [3, p. 866] – with provable formal improvability. We shall come back to related issues later.

One may also object that a lossless beam splitter has a quantum mechanical representation as an invertible unitary operator U, and therefore is reversible. Indeed, this can be readily demonstrated operationally by serially composing a lossless Mach-Zehnder interferometer with two beam splitters, thereby reconstructing the original quantum state (signal); that is, more formally, $\mathsf{U}^\dagger\mathsf{U} = \mathsf{I}$, where "†" indicates the Hermitian adjoint, and I stands for the identity operator. How this kind of unitarity conforms with the view that a beam splitter can be considered an "active element" of quantum randomness remains unresolved, and is actually highly questionable [6, 20]. Often vacuum fluctuations originating from the second, empty, input port are mentioned, but, pointedly stated [10, p. 249], these *"mysterious vacuum fluctuations … may be regarded as sugar coating for the bitter pill of quantum theory."*

A lossless 50:50 beam splitter can be modelled by a normalized 2 × 2 Hadamard transformation $\mathsf{U} = \frac{1}{\sqrt{2}}\mathsf{H}_2$ with rows $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ and $(-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$, respectively.

More generally, suppose we would like to construct a $\underbrace{\frac{1}{n} : \frac{1}{n} : \ldots : \frac{1}{n}}_{n \text{ times}}$ beam splitter represented by a normalized Hadamard matrix $\frac{1}{\sqrt{n}}\mathsf{H}_n$; that is, an Hadamard matrix H_n divided by the square of (the dimension) n. An $n \times n$ Hadamard matrix H_n has entries in $\{-1, 1\}$ such that any two distinct rows or columns of H_n, interpreted as vectors in a Hilbert space, have scalar product zero; that is, they are orthogonal (or, equivalently, by requiring that its transpose H_n^T satisfies $\mathsf{H}_n\mathsf{H}_n^T = n\mathsf{I}_n$).

A *necessary* condition for such a construction is that $n = 1$, $n = 2$, or $n = 4k$ for any $k \in \mathbb{N}$. *Hadamard's conjecture* claims that this is also a *sufficient* condition for the existence of an n-dimensional Hadamard transformation; and thus, for a corresponding equi-decomposition of quantum states into coherent superpositions. (Of course, a quantum state can be decomposed into any fraction of unity by suitable unitary transformations; this just represents a permutation of the original state, or, in a different interpretation, a base change [16].)

A quantum oracle for Hadamard's conjecture would be one which would, for any $k \in \mathbb{N}$, output $4k$ orthogonal $\frac{1}{4k}$-equi-weighted mixtures of orthogonal states spanning the entire $4k$-dimensional (real) Hilbert space. A beam splitter realizing Hadamard's conjecture would possess the remarkable property that it converts a signal input in any one of the $4k$ input ports into a coherent equi-superposition of all output ports; with relative phase differences equal to 0 (corresponding to equal relative sign), and π (corresponding to relative sign "$-$").

At the same time, in terms of quantum states forming bases (or, by other namings, blocks, subalgebras or contexts), Hadamard's conjecture translates into the existence of a particular kind of pure states equivalent to the projectors corresponding to the row (column) vector of a normalized Hadamard matrix. The set of row vectors of $\frac{1}{\sqrt{4k}}\mathsf{H}_{4k}$ correspond to an orthogonal basis which is *(mutually) unbiased* with respect to the Cartesian standard basis in $\mathbb{R}^{4k}$.

Schwinger's construction [16] can be used for the rendition of mutually unbiased bases in arbitrary dimensions n; alas the base vectors may have complex coordinates. The construction starts with the Cartesian standard basis $\{|e_1\rangle, |e_2\rangle, \ldots, |e_n\rangle\}$ and involves three steps: (i) a cyclic shift of the basis vectors $\{|f_1 = e_2\rangle, \ldots, |f_{n-1} = e_n\rangle, |f_n = e_1\rangle\}$, (ii) the construction of a unitary operator $\mathbf{U}$ by $\mathbf{U} = \sum_{i=1}^{n} |e_i\rangle\langle f_i|$; and finally (iii) the identification of the normalized eigenvectors of $\mathbf{U}$ with the elements of a basis which is unbiased with respect to the Cartesian standard basis. The associated normalized complex Hadamard matrix is just the row (column) matrix of the elements of this basis. For the sake of an example, we can readily write an algorithm [18] yielding a complex Hadamard matrix of dimension 8; that is,

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
-1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\
i & -1 & -i & 1 & i & -1 & -i & 1 \\
-i & -1 & i & 1 & -i & -1 & i & 1 \\
(-1)^{1/4} & i & (-1)^{3/4} & -1 & -(-1)^{1/4} & -i & -(-1)^{3/4} & 1 \\
-(-1)^{3/4} & -i & -(-1)^{1/4} & -1 & (-1)^{3/4} & i & (-1)^{1/4} & 1 \\
(-1)^{3/4} & -i & (-1)^{1/4} & -1 & -(-1)^{3/4} & i & -(-1)^{1/4} & 1 \\
-(-1)^{1/4} & i & -(-1)^{3/4} & -1 & (-1)^{1/4} & -i & (-1)^{3/4} & 1
\end{pmatrix}.$$

Whether the Schwinger construction, for $n = 4k$, $k \in \mathbb{N}$, can be extended to produce only the real entries in $\{-1, 1\}$ instead of complex numbers of modulus unity remains unknown. One may conjecture that in this case the Dita decomposition [5] of unitary matrices into products of diagonal phase matrices (with modulus one entries) and orthogonal matrices – which in turn can be written as compositions of rotations in two-dimensional subspaces – yields the appropriate real Hadamard matrices by substituting 0 or π for all phases in the phase matrices (thereby rendering diagonal elements 1 and -1, respectively), as well as by identifying all rotation angles with $\pm\pi/4$ (thereby rendering factors whose absolute value is $1/\sqrt{2}$).

4 Quantum vacuum fluctuations

As stated by Milonni [13, p. xiii] and others, *"... there is no vacuum in the ordinary sense of tranquil nothingness. There is instead a fluctuating quantum vacuum."* One of the observable vacuum effects is the *spontaneous emission of radiation* [19]: *"... the process of spontaneous emission of radiation is one in which "particles" are actually created. Before the event, it consists of an excited atom, whereas after the event, it consists of an atom in a state of lower energy, plus a photon."* Recent experiments achieve single photon production by spontaneous emission, for instance by electroluminescence. Indeed, most of the visible light emitted by the sun or other sources of blackbody radiation, including incandescent bulbs, is due to spontaneous emission [13, p. 78] and thus is subject to *creatio ex nihilo.*

A gap based on vacuum fluctuations is schematically depicted in Fig. 3. It consists of an atom in an excited state, which transits into a state of lower energy, thereby producing a photon. The photon (non-)creation can be coded by the symbols 0 and 1, respectively.

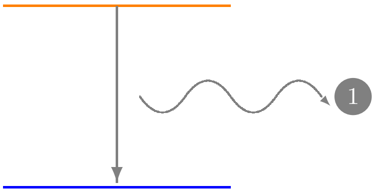

Fig. 3. (Color online) A gap created by the spontaneous creation of a photon.

5 Analogies in statistical physics

In the following we shall briefly glance at two related physical issues – the purported (ir-)reversibility of quantum measurements, as well the character of the second law of thermodynamics [14].

5.1 Wigner's and Everett's arguments against quantum measurement

An extension of the observation context is what Wigner [20] and, in particular, Everett [6, 7] had in mind when they argued against (irreversible and, in principal, for reversible) measurement. Because quantum mechanics allows for two types of evolution: (i) the first type comprises irreversible measurements, whereas (ii) the second mode is characterized by the unitary, that is, reversible permutation, of quantum states in-between aforementioned measurements.

Alas, this is true only *for all practical purposes*, that is, relative to the physical means [14] available to resolve the huge number of degrees of freedom involving a "macroscopic" measurement apparatus. And yet, at least in principle, if the unitary quantum evolution is taken to be universally valid, then any distinction or cut between the observer and the measurement apparatus on the one side, and the quantized object on the other side, is not absolute or ontic, but epistemic, means-relative, subjective and conventional.

5.2 Analogies to the second law of thermodynamics

There are good reasons to believe that also irreversibility in statistical physics is means relative [14] and thus epistemic: if we cannot resolve individual constituents of a group, and their degrees of freedom, then irreversibility is the epistemic expression of our incapacity to do so. In contradistinction, suppose the molecules are taken individually. In this case the second law might "dissolve into thin air" because of reversibility on the micro-description level. In Maxwell's own words [9, Document 15, p. 422] *"I carefully abstain from asking the molecules which enter where they last started from. I only count them and register their mean velocities, avoiding all personal enquiries which would only get me into trouble."*

6 *Caveats* and afterthoughts

Stated pointedly, we have essentially been talking about the emergence of events *out of nothing* (e.g. *creatio ex nihilo*), and without any cause. Thereby, and for the sake of accepting classical and quantum oracles for randomness, we are denying the *principle of sufficient reason,* as well as negating Parmenides' *nothing comes from nothing,* which so powerfully guided the ancient Greek and modern western Enlightenments.

More technically, we note without further discussion that any "diluted" indeterminism, or gap mechanism, could be "concentrated" to Borel normality by assuming independence of bits in binary sequences.

As a last speculation, it might not be too unreasonable to contemplate that all gap scenarios, including spontaneous symmetry breakdown and quantum oracles, are ultimately based on vacuum fluctuations.

Acknowledgments

This research has been partly supported by FP7-PEOPLE-2010-IRSES-269151-RANPHYS.

References

1. Abbott, A.A., Calude, C.S., Conder, J., Svozil, K.: Strong Kochen-Specker theorem and incomputability of quantum randomness. Physical Review A 86, 062109 (Dec 2012), http://dx.doi.org/10.1103/PhysRevA.86.062109
2. Abbott, A.A., Calude, C.S., Svozil, K.: Value-indefinite observables are almost everywhere. Physical Review A 89, 032109 (Mar 2014), http://dx.doi.org/10.1103/PhysRevA.89.032109
3. Born, M.: Zur Quantenmechanik der Stoßvorgänge. Zeitschrift für Physik 37, 863–867 (1926), http://dx.doi.org/10.1007/BF01397477
4. Campbell, L., Garnett, W.: The life of James Clerk Maxwell. With a selection from his correspondence and occasional writings and a sketch of his contributions to science. MacMillan, London (1882), http://www.sonnetsoftware.com/bio/maxbio.pdf
5. Dita, P.: Factorization of unitary matrices. Journal of Physics A: Mathematical and General 36(11), 2781 (2003), http://dx.doi.org/10.1088/0305-4470/36/11/309
6. Everett III, H.: 'Relative State' formulation of quantum mechanics. Reviews of Modern Physics 29, 454–462 (1957), http://dx.doi.org/10.1103/RevModPhys.29.454

7. Everett III, H.: The Everett interpretation of quantum mechanics: Collected works 1955-1980 with commentary. Princeton University Press, Princeton, NJ (2012), http://press.princeton.edu/titles/9770.html
8. Frank, P., R. S. Cohen (Editor): The Law of Causality and its Limits (Vienna Circle Collection). Springer, Vienna (1997), http://link.springer.com/book/10.1007/978-94-011-5516-8
9. Garber, E., Brush, S.G., Everitt, C.W.F.: Maxwell on Heat and Statistical Mechanics: On “Avoiding All Personal Enquiries” of Molecules. Associated University Press, Cranbury, NJ (1995)
10. Garrison, J.C., Chiao, R.Y.: Quantum Optics. Oxford University Press, Oxford (2008)
11. Gruska, J.: Foundations of computing. International Thompson Computer Press, London (April 1997)
12. Gruska, J.: Quantum Computing. McGraw-Hill, London (1999), http://www.fi.muni.cz/usr/gruska/qbook1.pdf
13. Milonni, P.W.: The Quantum Vacuum. An Introduction to Quantum Electrodynamics. Academic Press, San Diego (1994)
14. Myrvold, W.C.: Statistical mechanics and thermodynamics: A Maxwellian view. Studies in History and Philosophy of Science Part B: Studies in History and Philosophy of Modern Physics 42(4), 237–243 (2011), http://dx.doi.org/10.1016/j.shpsb.2011.07.001
15. Poincaré, H.: Wissenschaft und Hypothese. Teubner, Leipzig (1914)
16. Schwinger, J.: Unitary operators bases 46, 570–579 (1960), http://dx.doi.org/10.1073/pnas.46.4.570
17. Svozil, K.: Physical unknowables. In: Baaz, M., Papadimitriou, C.H., Putnam, H.W., Scott, D.S. (eds.) Kurt Gödel and the Foundations of Mathematics, pp. 213–251. Cambridge University Press, Cambridge, UK (2011), http://arxiv.org/abs/physics/0701163
18. Svozil, K.: Mathematica code for the generation of mutually unbiased bases (2012, 2104), http://tph.tuwien.ac.at/ svozil/publ/2012-schwinger.m
19. Weinberg, S.: The search for unity: Notes for a history of quantum field theory. Daedalus 106(4), 17–35 (1977), http://www.jstor.org/stable/20024506
20. Wigner, E.P.: Remarks on the mind-body question. In: Good, I.J. (ed.) The Scientist Speculates, pp. 284–302. Heinemann and Basic Books, London and New York (1961), http://www.phys.uu.nl/igg/jos/foundQM/wigner.pdf