

Curriculum Vitae Karl Svozil

Personal data

18. 12. 1956 born in Vienna; Austrian nationality; roman catholic;

4. 6. 1992 birth of son Alexander;

22. 6. 1996 birth of daughter Anna;

Academic data

1975 – 1981 physics studies at the University of Vienna and Heidelberg (1978/79);

18. 12. 1981 Promotion Dr. phil. in *physics* at Vienna University

1982/83 Visiting Scholar at the University of California at Berkeley and at the Lawrence Berkeley Laboratory/U.S.A.;

9. – 10. 1986 Visiting Scholar at the Moscow State University, at the Lebedev Institute and at the Ioffe Institute/St. Petersburg;

12. 3. 1988 Dozentur in *Theoretical Physics* at the University of Technology, Vienna;

Positions held

11. 1984 – 5. 1990 Austrian Ministry for Science & research;

6. 1990 permanent position ("wissenschaftlicher Beamter") at the Institute für Theoretische Physik of the University of Technology Vienna.

3. 1997 Assistentprofessor at the Institute für Theoretische Physik of the University of Technology Vienna.

10. 1997 A.o Univ.Professor at the Institute für Theoretische Physik of the University of Technology Vienna.

since 1998 Visiting Scholar at the Centre for Discrete Mathematics and Theoretical Computer Science of Auckland University, New Zealand.

Teaching

I have an extensive experience in teaching (also “crash courses” ;-) quantum information and computation at various academic institutions in Austria and abroad. Enclosed is a current list of courses at my home university.

Lectures

Course search (2010W/2011S)

Search string

[Extended Search](#)

Number	Type	Title	Hours	Semester	Lecturer	Subscribe
136.003	PA	Decoherence and Quantum Informations	8.0	2011S	Svozil, Karl	✓
136.022	VO	Logical methods in theoretical physics	2.0	2011S	Svozil, Karl	✓
132.015	PA	Physical models of chaotic systems	8.0	2011S	Svozil, Karl	✓
132.028	PV	Privatissimum for Diplomands	3.0	2011S	Svozil, Karl	✓
132.002	VO	Quantum Computation and Complexity Theory	2.0	2011S	Svozil, Karl	✓
136.020	VU	Statistical Physics I	3.0	2011S	Svozil, Karl	✓
136.003	PA	Decoherence and Quantum Informations	8.0	2010W	Svozil, Karl	✓
136.022	VO	Logical methods in theoretical physics	2.0	2010W	Leitsch, Alexander	✓
135.044	UE	Mathematical Methods in Physics	2.0	2010W	Svozil, Karl	✓
132.015	PA	Physical models of chaotic systems	8.0	2010W	Svozil, Karl	✓
132.028	PV	Privatissimum for Diplomands	3.0	2010W	Svozil, Karl	✓

[Support](#) | [Policies](#) | [Legal Notice](#)

Technische Universität Wien – Karlsplatz 13 | A-1040 Wien | Tel. +43/(0)1/58801-0 | Fax +43/(0)1/58801-41099

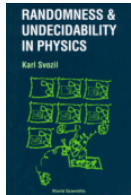
Publication list Karl Svozil

- [Monographs](#)
- [Journal articles](#)
- [Contributions to conferences & scientific books](#)
- [Patents](#)
- [Preprints](#)

Monographs






















1. K. Svozil, ``Quantum Logic" (Springer, Singapore, 1998), xviii+214 pages.



2. K. Svozil, ``Randomness and Undecidability in Physics" (World Scientific, Singapore, 1993), xvi+292 pages.










Journal articles




1. K. Svozil, ``[Quantum value indefiniteness](#)", *Natural Computing* **NN**(NN), 1-12 (2010)   , [[DOI: 10.1007/s11047-010-9241-x](#)], [[L^AT_EX](#)], [[BibT_EX](#)].
2. Martin Schaller and Karl Svozil, ``[Zeno Squeezing of Cellular Automata](#)", *International Journal of Unconventional Computing* **6**(5), 399-416 (2010),   , [[L^AT_EX](#)], [[BibT_EX](#)].
3. Maria Schimpf and Karl Svozil, ``[A glance at singlet states and four-partite correlations](#)", *Mathematica Slovaca* **60**(5), 701-722 (2010),   , [[DOI: 10.2478/s12175-010-0041-7](#)], [[L^AT_EX](#)], [[BibT_EX](#)] (Special issue in honour of Professor Sylvia Pulmannova).
4. Cristian S. Calude, Elena Calude and Karl Svozil, ``[The complexity of proving chaoticity and the Church–Turing thesis](#)", *Chaos* **20**, 037103 (2010) [5 pages],   , [[DOI: 10.1063/1.3489096](#)], [[L^AT_EX](#)], [[BibT_EX](#)].
5. Cristian S. Calude, Michael J. Dinneen, Monica Dumitrescu and Karl Svozil, ``[Experimental evidence of quantum randomness incomputability](#)", *Phys. Rev. A* **82**, 022102 (2010) [8 pages],   , [[DOI: 10.1103/PhysRevA.82.022102](#)], [[L^AT_EX](#)], [[BibT_EX](#)].
6. Karl Svozil, ``[On the plasticity of nonlocal quantum correlations](#)", *Ukrainian Journal of Physics* **55**(5), 547-553 (2010),    , [[L^AT_EX](#)], [[BibT_EX](#)].
7. Karl Svozil, ``[The diagonalization method in quantum recursion theory](#)", *Quantum Information*































Processing **9**(2), 295-305 (2010),   , [[DOI: 10.1007/s11128-009-0115-z](https://doi.org/10.1007/s11128-009-0115-z)], [[L^AT_EX](#)], [[BibT_EX](#)].

8. Karl Svozil, "[Proposed direct test of a certain type of noncontextuality in quantum mechanics](#)", *Phys. Rev. A* **80**, 040102 (2009),   , [[DOI: 10.1103/PhysRevA.80.040102](https://doi.org/10.1103/PhysRevA.80.040102)], [[L^AT_EX](#)], [[BibT_EX](#)].
9. Karl Svozil, "[Three criteria for quantum random-number generators based on beam splitters](#)", *Phys. Rev. A* **79**, 054306 (2009),   , [[DOI: 10.1103/PhysRevA.79.054306](https://doi.org/10.1103/PhysRevA.79.054306)], [[L^AT_EX](#)], [[BibT_EX](#)].
10. Martin Schaller and Karl Svozil, "[Scale-invariant cellular automata and self-similar Petri nets](#)", *The European Physical Journal B* **69**, 297–311 (2009),   , [[DOI: 10.1140/epjb/e2009-00147-x](https://doi.org/10.1140/epjb/e2009-00147-x)], [[L^AT_EX](#)], [[BibT_EX](#)].
11. K. Svozil and J. Tkadlec, "[On the solution of trivalent decision problems by quantum state identification](#)", *Natural Computing* **8**(3), 539-546 (2009)   , [[DOI: 10.1007/s11047-009-9112-5](https://doi.org/10.1007/s11047-009-9112-5)], [[L^AT_EX](#)], [[BibT_EX](#)].
12. Cristian S. Calude and Karl Svozil, "[Quantum Randomness and Value Indefiniteness](#)", *Advanced Science Letters* **1**(2), 165–168 (2008)   , [[DOI:10.1166/asl.2008.016](https://doi.org/10.1166/asl.2008.016)], [[L^AT_EX](#)], [[BibT_EX](#)].
13. K. Svozil, "[Quantum Scholasticism: On Quantum Contexts, Counterfactuals, and the Absurdities of Quantum Omniscience](#)", *Information Sciences* **179**(5), 535–541 (2009)   , [[DOI:10.1016/j.ins.2008.06.012](https://doi.org/10.1016/j.ins.2008.06.012)], [[L^AT_EX](#)], [[BibT_EX](#)].
14. Alexander Leitsch, Günter Schachner and Karl Svozil, "[How to Acknowledge Hypercomputation?](#)", *Complex Systems* **18**(1), 131-143, (2008)   , [[L^AT_EX](#)], [[BibT_EX](#)].
15. F.A. Bovino, M. Giardina, K. Svozil and V. Vedral, "[Spatial Orientation by Quantum Telepathy](#)", *International Journal of Quantum Information (IJQI)* **5**(1/2), 43-49 (2007)   , [[DOI:10.1142/S0219749907002517](https://doi.org/10.1142/S0219749907002517)], [[L^AT_EX](#)], [[BibT_EX](#)].
16. Karl Svozil, "[Staging quantum cryptography with chocolate balls](#)", *American Journal of Physics* **74**(9), 800-803 (2006)   , [[DOI:10.1119/1.2205879](https://doi.org/10.1119/1.2205879)], [[L^AT_EX](#)], [[BibT_EX](#)].

Extended German version: "[Dramatisierte Quantenkryptographie](#)", *Wissenschaftliche Nachrichten* **129**(November/Dezember), 37-40 (2005) .

17. Karl Svozil, "[Are simultaneous Bell measurements possible?](#)", *New J. Phys.* **8**, 39 (2006)   , [[DOI:10.1088/1367-2630/8/3/039](https://doi.org/10.1088/1367-2630/8/3/039)], [[L^AT_EX](#)], [[BibT_EX](#)].
18. Karl Svozil, "[Communication cost of breaking the Bell barrier](#)", *Physical Review A* **72**, 050302(R) (2005)   , [[DOI:10.1103/PhysRevA.72.050302](https://doi.org/10.1103/PhysRevA.72.050302)], [[L^AT_EX](#)], [[BibT_EX](#)].
19. Karl Svozil, "[Noncontextuality in multipartite entanglement](#)", *J. Phys. A: Math. Gen.* **38**(25), 5781-5798 (2005)   , [[DOI:10.1088/0305-4470/38/25/013](https://doi.org/10.1088/0305-4470/38/25/013)], [[L^AT_EX](#)], [[BibT_EX](#)].
20. Karl Svozil, "[Feasibility of the interlock protocol against man-in-the-middle attacks on quantum cryptography](#)", *International Journal of Quantum Information* **3**(4), 649-654 (2005) [[DOI:](#)

[10.1142/S0219749905001511](https://doi.org/10.1142/S0219749905001511)], , , , [[L^AT_EX](#)], [[BibT_EX](#)].


















21. Karl Svozil, "[Logical Equivalence Between Generalized Urn Models and Finite Automata](#)", *International Journal of Theoretical Physics* **44**(7), 745-754 (2005) , , , [[DOI: 10.1007/s10773-005-7052-0](#)], [[L^AT_EX](#)], [[BibT_EX](#)].
22. Karl Svozil, "[Computational universes](#)", *Chaos, Solitons & Fractals* **25**(4), 845-859 (2005) , , , [[DOI: 10.1016/j.chaos.2004.11.055](#)], [[L^AT_EX](#)], [[BibT_EX](#)].
23. Cristian S. Calude, Ludwig Staiger and Karl Svozil, "[Randomness relative to Cantor expansions](#)", *Communications in Nonlinear Science and Numerical Simulation* **10**(8), 921-930 (2005) , , , [[DOI: 10.1016/j.cnsns.2004.05.003](#)], [[L^AT_EX](#)], [[BibT_EX](#)].
24. Stefan Filipp and Karl Svozil, "[Generalizing Tsirelson's Bound on Bell Inequalities Using a Min-Max Principle](#)", *Physical Review Letters* **93**, 130407 (2004) , , , [[DOI: 10.1103/PhysRevLett.93.130407](#)], [[L^AT_EX](#)], [[BibT_EX](#)].
25. Karl Svozil, "[Eutactic quantum codes](#)", *Physical Review A* **69**, 034303 (2004). [[DOI:10.1103/PhysRevA.69.034303](#)], , , , [[L^AT_EX](#)], [[BibT_EX](#)]. This article has been selected by the APS for the *Virtual Journal of Quantum Information* **4**(3) (March 2004) [[VJQI issue](#)].
26. Volkmar Putz and Karl Svozil, "[Quantum electrodynamics in the squeezed vacuum state: electron mass shift](#)", *Il Nuovo Cimento B* **119**, 175-179 (2004). [[DOI:10.1393/ncb/i2004-10051-8](#)], , .
27. Karl Svozil, "[Quantum information via state partitions and the context translation principle](#)", *Journal of Modern Optics* **51**, 811-819 (2004). [[DOI:10.1080/09500340410001664179](#)], , , , [[L^AT_EX](#)], [[BibT_EX](#)].
28. Stefan Filipp and Karl Svozil, "[Testing the bounds on quantum probabilities](#)", *Physical Review A* **69**, 032101 (2004) [[DOI:10.1103/PhysRevA.69.032101](#)], , , , [[L^AT_EX](#)], [[BibT_EX](#)]. This article has been selected by the APS for the *Virtual Journal of Quantum Information* **4**(3) (March 2004) [[VJQI issue](#)].
29. Karl Svozil, "[Quantum information in base \$n\$ defined by state partitions](#)", *Physical Review A* **66**, 044306 (2002) [[DOI:10.1103/PhysRevA.66.044306](#)], , , , , [[L^AT_EX](#)], [[BibT_EX](#)]. This article has been selected by the APS for the *Virtual Journal of Quantum Information* **2**(11) (November 2002) [[VJQI issue](#)].
30. Niko Donath and Karl Svozil, "[Finding a state among a complete set of orthogonal states](#)" *Physical Review A* **65**, 044302 (2002) [[DOI:10.1103/PhysRevA.65.044302](#)], , , , , [[L^AT_EX](#)], [[BibT_EX](#)]. This article has been selected by the APS for the *Virtual Journal of Quantum Information* **2**(4) (April 2002) [[VJQI issue](#)].
31. Karl Svozil, "[Conventions in relativity theory and quantum mechanics](#)" *Foundations of Physics* **32**(4), 479-502 (2002); An appendix contains a complete proof of Alexandrov's theorem using methods of affine geometry. [[DOI:10.1023/A:1015017831247](#)], , , , [[L^AT_EX](#)].

(Karl Svozil, "[The chromatic number of a sphere. Solution of problem nr. 10769](#)" *The American*


























Mathematical Monthly **108**, 774-775 (2001) [[MAA online](#)], [[gif image](#)], , [[L^AT_EX](#)], [[BibT_EX](#)].













32. Itamar Pitowsky and Karl Svozil, "[Optimal tests of quantum nonlocality](#)" *Physical Review A* **64**, 014102 (2001) [[DOI:10.1103/PhysRevA.64.014102](#)], , , , [[L^AT_EX](#)], [[BibT_EX](#)]. This article has been selected by the APS for the *Virtual Journal of Quantum Information* **1**(2) (July 2001) [[VJQI issue](#)].
33. Hans Havlicek, Guenther Krenn, Johann Summhammer and Karl Svozil, "[Coloring the rational quantum sphere and the Kochen-Specker theorem](#)", *J. Phys. A: Math. Gen.* **34**(14), 3071-3077 (13 April 2001) [[DOI:10.1088/0305-4470/34/14/312](#)], [[htm](#)], [[qhant-physics](#)], , .
- K. Svozil, "[\[Book Review:\] Quantum Logic in Algebraic Approach, by Miklos Redei](#)", *Studies In History and Philosophy of Science Part B: Studies In History and Philosophy of Modern Physics* **32**(1), 113-115 (2001) [[DOI:10.1016/S1355-2198\(00\)00005-8](#)], , .
34. C.S. Calude, M.J. Dinneen and K. Svozil "[Reflections on Quantum Computing](#)", *Complexity* **6**(1), 35-37 (2000) [[DOI:10.1002/1099-0526\(200009/10\)6:1<35::AID-CPLX1005>3.0.CO;2-T](#)], , , .
35. Georges Chevalier, Anatolij Dvurecenskij and Karl Svozil, "[Piron's and Bell's Geometric Lemmas and Gleason's Theorem](#)", *Foundations of Physics* **30**(10), 1737-1755 (2000) [[DOI:10.1023/A:1026458519154](#)], , .
36. K. Svozil, "[Relativizing Relativity](#)", *Foundations of Physics* **30**(7), 1001-1016 (2000) [[DOI:10.1023/A:1003600519752](#)], , .
37. G. Franck-Oberaspach, D. B. Schweiger and K. Svozil, "[A Packing Problem, Solved by Genetic Algorithms](#)", *Journal of Universal Computer Science (Springer)* **5**, 464-470 (1999) .
38. G. Krenn, J. Summhammer and K. Svozil, "[Interferometric information gain versus interaction-free measurement](#)" *Physical Review A* **61**, 052102 (2000) [[DOI:10.1103/PhysRevA.61.052102](#)], .
39. Karl Svozil and Douglas Bridges, "[Constructive mathematics and quantum physics](#)", *International Journal of Theoretical Physics* **39**(3), 503-515 (2000) [[DOI:10.1023/A:1003613131948](#)], , .
40. Karl Svozil, "[Logic of reversible automata](#)", *International Journal of Theoretical Physics* **39** (3), 893-899 (2000) [[DOI:10.1023/A:1003639232374](#)], , , .
41. R. Sedivy, Ch. Windischberger, K. Svozil, E. Moser and G. Breiteneker, "[Fractal Analysis: An Objective Method for Identifying Atypical Nuclei in Dysplastic Lesions of the Cervix Uteri](#)", *Gynecologic Oncology* **75**(1), October 1999, 78-83 (1999) [[DOI:10.1006/gyno.1999.5516](#)], .
42. Cristian S. Calude, Peter H. Hertling and Karl Svozil, "[Embedding Quantum Universes in Classical Ones](#)", *Foundations of Physics* **29**(3), 349-390 (1999) [[DOI:10.1023/A:1018862730956](#)], , , [[L^AT_EX](#)], [[BibT_EX](#)].
43. Klaus Ehrenberger, Dominik Felix and Karl Svozil, "Stochastic resonance in cochlea signal transduction", *Acta Oto-Laryngologica* **118**, 7-8 (1998); **119**, 166-170 (1999) [[DOI:10.1080/00016489950181594](#)].

44. Klaus Ehrenberger and Karl Svozil, "[Aging and Complexity in Equilibrium Dynamics](#)", *Chaos, Solitons & Fractals* **10**, 1085-1086 (1999) , , [[L^AT_EX](#)], [[Bib_TE_X](#)], [[DOI:10.1016/S0960-0779\(98\)00146-5](#)].
45. Karl Svozil, "[One-to-one](#)", *Complexity* **4**(1), 25-29 (1998) [[DOI:10.1002/\(SICI\)1099-0526\(199809/10\)4:1<25::AID-CPLX8](#)], , .
46. Cristian S. Calude, Peter H. Hertling and Karl Svozil, "Kochen-Specker theorem: two geometrical proofs", *Quantum Structures II. Tatra Mountains Mathematical Publications* **15**, 133-142 (1998)
47. Karl Svozil, "[Analogues of quantum complementarity in the theory of automata](#)", *Studies In History and Philosophy of Science Part B: Studies In History and Philosophy of Modern Physics* **29**, 61-80 (1998) [[DOI:10.1016/S1355-2198\(97\)00028-2](#)], , .
48. G. Krenn and K. Svozil, "[Stronger-than-quantum correlations](#)", *Foundation of Physics* **28**(6), 971-984 (1998) [[DOI:10.1023/A:1018821314465](#)], , .
49. S. Pulmannová and K. Svozil, "[Ideals in ortholattices, Bell inequalities and simultaneously definite properties](#)", *International Journal of Theoretical Physics* **36**(7), 1547-1564 (1997).
50. Cristian Calude, Elena Calude, Karl Svozil and Sheng Yu, "[Physical versus Computational Complementarity I](#)", *International Journal of Theoretical Physics* **36**, 1495-1523 (1997).
51. Anatolij Dvurecenskij and K. Svozil, "[Product of Partition Logics, Orthoalgebras and Automata](#)", *International Journal of Theoretical Physics* **35**(11), 2377-2390 (1996) [[DOI:10.1007/BF02302454](#)], .
52. Karl Svozil and Josef Tkadlec, "[Greechie diagrams, nonexistence of measures in quantum logics and Kochen-Specker type constructions](#)", *Journal of Mathematical Physics* **37**, 5380-5401 (1996) [[DOI:10.1063/1.531710](#)], .
53. K. Svozil, D. Felix and K. Ehrenberger, "[Amplification by stochastic interference](#)", *J. Phys. A: Math. Gen.* **29**, L351-L354 (1996) [[DOI:10.1088/0305-4470/29/13/007](#)], , .
54. Hans Havlicek and K. Svozil, "[Density conditions for quantum propositions](#)", *Journal of Mathematical Physics* **37**, 5337-5341 (1996) [[DOI:10.1063/1.531738](#)], .
55. K. Svozil, "[Quantum algorithmic information theory](#)", *Journal of Universal Computer Science* **2**, 311-346 (1996) , , .
56. K. Svozil and R. R. Zapatin, "[Empirical logic of finite automata: microstatements versus macrostatements](#)", *International Journal of Theoretical Physics*, **35**, 1541-1548 (1996) [[DOI:10.1007/BF02084959](#)].
57. Wolfgang Gstoettner, Wolf Baumgartner, Jafar Hamzavi, Dominik Felix, Karl Svozil, Reiner Meyer und Klaus Ehrenberger, "Auditory fractal random signals: Experimental data and clinical application", *Acta Oto-Laryngologica* **116**, 222-223 (1996).
58. K. Svozil and N. Neufeld, "['Linear' chaos via paradoxical set decompositions](#)", *Chaos, Solitons & Fractals* **7**(5), 785-793 (1996) [[DOI:10.1016/0960-0779\(95\)00116-6](#)], , .



59. M. Schaller and K. Svozil, "[Automaton logic](#)", *International Journal of Theoretical Physics* **35**, 911-940 (1996) [[DOI:10.1007/BF02302381](#)], .
60. N. Brunner, K. Svozil and M. Baaz, "The axiom of choice in quantum theory" *Mathematical Logic Quarterly* **42** 319-340 (1996).
61. G. Krenn, J. Summhammer and K. Svozil, "[Interaction-Free Preparation](#)" *Physical Review A* **53**, 1228-1231 (1996) [[DOI:10.1103/PhysRevA.53.1228](#)], , .
62. K. Svozil, "[How real are virtual realities, how virtual is reality? The constructive re-interpretation of physical undecidability](#)", *Complexity*, **1**, 43-54 (1996).
63. K. Svozil, "[Time paradoxa reviewed](#)", *Phys. Lett. A* **199**, 323-326 (1995). [[DOI:10.1016/0375-9601\(95\)00129-Q](#)], , .
64. K. Svozil, "[Halting probability amplitude of quantum computers](#)", *Journal of Universal Computer Science* **1**, nr. 3, 1-4 (March 1995) [[DOI:10.3217/jucs-001-03-0201](#)], , .
65. K. Svozil, "[Set Theory and Physics](#)", *Foundations of Physics*, **25**, 1541-1560 (1995) [[DOI:10.1007/BF02055507](#)], , .
66. K. Ehrenberger, D. Felix and K. Svozil, "Origin of Auditory Fractal Random Signals in Guinea Pigs", *NeuroReport* **6**, 2117-2120 (1995).
67. A. Dvurecenskij, S. Pulmannová and K. Svozil, "[Partition Logics, Orthoalgebras and Automata](#)". *Helvetica Physica Acta* **68**, 407-428 (1995), .
68. K. Svozil, "[Consistent use of paradoxes in deriving constraints on the dynamics of physical systems and of no-go-theorems](#)", *Foundations of Physics Letters* **8**, 523-535 (1995) [[DOI:10.1007/BF02186244](#)], , .
69. M. Schaller and K. Svozil, "[Automaton partition logic versus quantum logic](#)" *International Journal of Theoretical Physics* **34**, 1741-1749 (1995) [[DOI:10.1007/BF00676288](#)], [[htm](#)], .
70. N. Brunner, K. Svozil and M. Baaz, "Effective quantum observables" *Il Nuovo Cimento* **B110**, 1397-1413 (1995).
71. M. Schaller and K. Svozil, "[Partition logics of automata](#)". *Il Nuovo Cimento B* **109**, 167-176 (1994).
72. K. Svozil, D. Felix and K. Ehrenberger, "Multiple-channel fractal information coding of mammalian nerve signals", *Biochemical and Biophysical Research Communications* **199**, 911-915 (1994).
73. K. Svozil, "[Squeezed fermion states](#)", *Physical Review Letters* **65**, 3341-3343 (1990) [[DOI:10.1103/PhysRevLett.65.3341](#)], , .
74. P. W. Milonni and K. Svozil, "[Impossibility of measuring faster-than-light signaling by the Scharnhorst effect](#)", *Phys. Lett. B* **248**, 437-438 (1990) [[DOI:10.1016/0370-2693\(90\)90317-Y](#)], [[L^AT_EX](#)], , .
75. K. Svozil, "[Constructive chaos by Cellular Automata and possible sources of an arrow of time](#)", *Physica* **D45**, 420-427 (1990); reprinted *Cellular Automata, Theory and Experiment*, ed. by H.

Gutowitz (MIT Press, Cambridge, MA, 1991).


76. K. Svozil, [``Comment on `Comment on quantum cosmology and the initial state of the universe' "](#), Physical Review D **41**, 1353-1354 (1990) [[DOI:10.1103/PhysRevD.41.1353](#)], , , ``Erratum: Comment on `Comment on quantum cosmology and the initial state of the universe' ", Physical Review D **44**, 567-568 (1991) , .
77. K. Svozil, [``Test of local causality with very short light pulses"](#), Physical Review A **39**, 2222-2224 (1989) [[DOI:10.1103/PhysRevA.39.2222](#)], , , ``Reply to ``Comment on `Test of local causality with very short light pulses' " Physical Review A **41**, 1729 (1990) [[DOI:10.1103/PhysRevA.41.1729](#)], , .
78. K. Svozil, [``The quantum coin toss-testing microphysical undecidability"](#), Phys. Lett. A **143**, 433-437 (1990). [[DOI:10.1016/0375-9601\(90\)90408-G](#)], , .
79. K. Svozil, [``Are chaotic systems dynamically random?"](#), Phys. Lett. A **140**, 5-9 (1989) [[DOI:10.1016/0375-9601\(89\)90536-7](#)], .
80. K. Svozil and R. Lassnig, [``Raman spectroscopy in high-temperature superconducting materials"](#), Physical Review B **37**, 3654-3656 (1988) [[DOI:10.1103/PhysRevB.37.3654](#)], , .
81. K. Svozil and A. Zeilinger, [``Is there a breakdown of QED in \(g-2\)-measurements?"](#), Physica Scripta **T21**, 122 (1988) [[DOI:10.1088/0031-8949/1988/T21/022](#)], .
82. K. Svozil, ``Heavy fermion superconductivity via Kondo type pairing", phys. stat. sol. (b) **147**, 635-647 (1988)
83. K. Svozil, [``New form of pair interaction in superconductivity in pressure-sensitive systems"](#), Physical Review B **36**, 715-717 (1987) [[DOI:10.1103/PhysRevB.36.715](#)], , .
84. V. V. Moshchalkov and K. Svozil, [``Phenomenological model of superconductivity in \$U_{1-x}Th_xBe_{13}\$ "](#), Phys. Lett. A **120**, 356-360 (1987). [[DOI:10.1016/0375-9601\(87\)90731-6](#)], .
85. O.V.Dolgov, E.P.Fetisov, D.I.Khomskii and K. Svozil, ``Model of interband pairing in mixed valence and heavy fermion systems", Z. Phys. B **67**, 63-68 (1987) [[DOI:10.1007/BF01307308](#)].
86. K. Svozil, [``Test of s-wave pairing in heavy-fermion systems due to Kondo volume collapse"](#), Physical Review B **35**, 7113-7114 (1987) [[DOI:10.1103/PhysRevB.35.7113](#)], , .
87. K. Svozil, [``Quantum field theory on fractal space-time"](#), J. Phys. A: Math. Gen. **20**, 3861-3875 (1987) [[DOI:10.1088/0305-4470/20/12/033](#)], , .
88. K. Svozil, ``Renormalization of the quantum theory of the solid state", Fortschritte der Physik (Progress of Physics) **35**, 65-85 (1987).
89. K. Svozil, [``Model for p- and d-wave superconductivity in heavy fermion systems"](#), Physical Review B **33**, 602-604 (1986) [[DOI:10.1103/PhysRevB.33.602](#)], , .
90. M. Kreuzer and K. Svozil, [``QED between plates: mass and anomalous magnetic moment of an electron"](#), Physical Review D **34**, 1429-1437 (1986) [[DOI:10.1103/PhysRevD.34.1429](#)], , .

91. K. Svozil, [``Connections between deviations from Lorentz transformation and relativistic energy-momentum relation''](#), Europhysics Letters **2**, 83-85 (1986) [[DOI:10.1209/0295-5075/2/2/002](#)], .
92. K. Svozil, [``Operational perception of space-time coordinates in a quantum medium''](#), Il Nuovo Cimento **96B**, 127-139 (1986) .
93. K. Svozil and A. Zeilinger, [``Dimension of space-time''](#), International Journal of Modern Physics A ([IJMPA](#)) **1**(4), 971-990 (1986). [[DOI:10.1142/S0217751X86000368](#)], .
94. K. Svozil, [``Dimensional reduction via dimensional shadowing''](#), J. Phys. A: Math. Gen. **19**, L1125-L1127 (1986) [[DOI:10.1088/0305-4470/19/18/002](#)], , .
95. K. Svozil, [``Are quantized fields Cellular Automata?''](#), Phys. Lett. A **119**, 153-156 (1986) [[DOI:10.1016/0375-9601\(86\)90436-6](#)], .
96. A. Zeilinger and K. Svozil, [``Measuring the dimension of space-time''](#), Physical Review Letters **54**, 2553-2555 (1985) [[DOI:10.1103/PhysRevLett.54.2553](#)], , .
97. K. Svozil, [``Mass and anomalous magnetic moment of an electron between two conducting parallel plates''](#), Physical Review Letters **54**, 742-744 (1985) [[DOI:10.1103/PhysRevLett.54.742](#)], , .
98. K. Svozil, [``Raman scattering on superconductors in the presence of charge-density states''](#), Physical Review B **31**, 4688-4689 (1985) [[DOI:10.1103/PhysRevB.31.4688](#)], , .
99. K. Svozil, [``A new type of charge screening due to phonon-Coulomb mixing in many-body physics''](#), Phys. Lett. A **106**, 264 - 266 (1984). [[DOI:10.1016/0375-9601\(84\)91024-7](#)], .
100. K. Svozil, [``Comprehensive study of the renormalization of the theory of strong-coupling superconductors''](#), Physical Review B **30**, 1357-1361 (1984) [[DOI:10.1103/PhysRevB.30.1357](#)]. .
.
101. K. Svozil, [``Weak spectral functions and their application to the decay of the W-boson''](#), Lettere al Nuovo Cimento **39**, 294 - 298 (1984).
102. K. Svozil, [``Remarks on a lower bound for the critical temperature from the real-frequency Eliashberg equations''](#), Acta Physica Austr. **55**, 229 - 232 (1984).
103. H. Pietschmann, H. Rupertsberger and K. Svozil, [``Possible tests of the weak boson self-coupling below the -threshold''](#), Z. Physik C **12**, 367 - 368 (1982) [[DOI:10.1007/BF01557582](#)]. .
104. H. Rupertsberger and K. Svozil, [``Hadronic final states in the decay and the weak boson self-energy''](#), Acta Physica Austr. **54**, 255-263 (1982).









Contributions to conferences & scientific books

1. Karl Svozil, [``Indeterminism and Randomness Through Physics''](#), in [Randomness Through Computation. Some Answers, More Questions](#), ed. by Hector Zenil (World Scientific, Singapore, 2011), pp. 109-120 , , [[L^AT_EX](#)], [[BibT_EX](#)].

2. Karl Svozil, "[On the Brightness of the Thomson Lamp: A Prolegomenon to Quantum Recursion Theory](#)", in [Unconventional Computation. 8th International Conference, UC 2009, Ponta Delgada, Portugal, September 7-11, 2009, Proceedings \(Series: Lecture Notes in Computer Science, Subseries: Theoretical Computer Science and General Issues, Vol. 5715\)](#), ed. by C.S. Calude, J.F.G.d. Costa, N. Dershowitz, E. Freire and G. Rozenberg (Springer, Berlin, Heidelberg, 2009), pp. 236-246 , [[DOI: 10.1007/978-3-642-03745-0_26](#)], , , [[L^AT_EX](#)].
3. Karl Svozil, "[Contexts in quantum, classical and partition logic](#)", in [Handbook of Quantum Logic and Quantum Structures](#), ed. by Kurt Engesser, Dov M. Gabbay and Daniel Lehmann (Elsevier, Amsterdam, 2008), pp. 551-586 , , [[L^AT_EX](#)].
4. Karl Svozil, "[Omega and the time evolution of the N-body problem](#)", in *Randomness and Complexity, from Leibniz to Chaitin*, ed. by Cristian S. Calude (World Scientifics, Singapore, 2007), pp. 235-242 [[Publisher](#)], , , [[L^AT_EX](#)], ,
5. S. Rieder and Karl Svozil, "[Probability Distributions and Gleason's Theorem](#)", in *AIP Conference Proceedings 889. Foundations of Probability and Physics-4*, ed. by Guillaume Adenier and Andrei Yu. Khrennikov (American Institute of Physics, Melville, NY, 2007), pp. 235-242 [[DOI:10.1063/1.2713462](#)], , , [[L^AT_EX](#)], ,
6. Karl Svozil, "[Characterization of quantum computable decision problems by state discrimination](#)", in *AIP Conference Proceedings 810. Quantum Theory. Reconsideration of Foundations--3*, ed. by Guillaume Adenier, Andrei Yu. Khrennikov and Theo M. Nieuwenhuizen (American Institute of Physics, Melville, NY, 2006), pp. 271-279 [[DOI:10.1063/1.2158729](#)], , , [[L^AT_EX](#)], ,
7. Karl Svozil, "[Physics and metaphysics look at computation](#)", in *Church's Thesis after 70 years*, ed. by Adam Olszewski, Jan Wolenski and Robert Janusz (Ontos Verlag, Frankfurt, Paris, 2006), pp. 491-517 , [physics/0508207](#), , [[L^AT_EX](#)].
8. Karl Svozil, "[Computational Universes](#)", in *Space Time Physics and Fractality*, ed. by Peter Weibel, Garnet Ord and Otto E. Rössler (Springer Verlag, Wien, New York, 2005), pp. 144-173 ]. , [[L^AT_EX](#)].
9. Daniel M. Greenberger and Karl Svozil, "[Quantum Theory Looks at Time Travel](#)", in *Quo Vadis Quantum Mechanics?*, ed. by A. Elitzur, S. Dolev and N. Kolenda (Springer Verlag, Berlin, 2005), pp. 63-72 ]. , [[L^AT_EX](#)].
10. Stefan Filipp and Karl Svozil, "[Tracing the Bounds on Bell-Type Inequalities](#)", in *AIP Conference Proceedings 750. Foundations of Probability and Physics-3*, ed. by Andrei Khrennikov (American Institute of Physics, Melville, NY, 2005), pp. 87-94 [[DOI:10.1063/1.1874561](#)], ,
11. Karl Svozil, "[On Counterfactuals and Contextuality](#)", in *AIP Conference Proceedings 750. Foundations of Probability and Physics-3*, ed. by Andrei Khrennikov (American Institute of Physics, Melville, NY, 2005) pp. 351-360 [[DOI:10.1063/1.1874586](#)], , , [[L^AT_EX](#)], [[BibT_EX](#)].
12. K. Svozil, "Conventions in Relativity Theory and Quantum Mechanics," *La nuova Critica. Nuova Serie* **43-44**(1-2), 59-70 (2004).

Klaus Eberhard and Karl Svozil, [Abstract 101. Stochastic inference and auditory perception](#), 7th European Symposium. Pediatric Cochlear Implantation, May 2004, Geneva, Switzerland (2004) ,

13. Karl Svozil, ["Finite Automata models of quantized system: conceptual status and outlook"](#), in *Developments in Language Theory. Proceedings of the 6th International Conference, DLT 2002, Kyoto, Japan, September 2002*, ed. by Masami Ito and Masafumi Toyama (Springer, Berlin 2003), pp. 93-102, [[DOI:10.1007/3-540-45005-X_8](#)], , , [[L^AT_EX](#)], [[BibT_EX](#)].
14. Stefan Filipp und Karl Svozil, ["Boole-Bell-type inequalities in Mathematica"](#), in *Challenging the Boundaries of Symbolic Computation, Proceedings of the 5th International Mathematica Symposium, Imperial College London 7-11 July 2003*, ed. by Peter Mitic, Philip Ramsden and Janet Carne (Imperial College Press, London 2003), pp. 215-222, , [[Mathematica Notebook](#)].
15. Daniel Greenberger and Karl Svozil, ["A quantum mechanical look at time travel and free will"](#), in *Between Chance and Choice*, ed. by Harald Atmanspacher and Robert Bishop (Imprint Academic, Thorverton 2002), pp. 293-308, [[pdf \(scan\)](#)], , [[L^AT_EX](#)], [[BibT_EX](#)].
16. Karl Svozil, ["Science at the crossroad between randomness and determinism"](#) in *Millennium III*, ed. by Cristian Calude and Karl Svozil (Black Sea University Foundation, in collaboration with the Romanian Academy of Sciences and the Club of Rome, Bucharest 2001), pp. 73-84, [[pdf \(scan\)](#)], , [[L^AT_EX](#)], [[BibT_EX](#)].
17. Karl Svozil, ["Quantum interfaces"](#), in *Sciences of the Interface*, ed. by Hans H. Diebner, Timothy Druckrey and Peter Weibel, (Genista Verlag, Tübingen 2001), pp. 76-88, .
18. K. Svozil, ["Quantum information: the new frontier"](#) *Unconventional Models of Computation UMC'2K*, ed. by I. Antiniou, C.S. Calude and M.J. Dinneen, (Springer, London, Berlin, Heidelberg 2001), pp. 248-272.
19. C. S. Calude, E. Calude, K. Svozil, "Computational Complementarity for Probabilistic Automata", in *Where Mathematics, Computer Science, Linguistics and Biology Meet*, ed. by C. Martin-Vide, G. Paun (Kluwer Academic Publishers, Amsterdam 2000), pp. 99-113, , [[abstract](#)].
20. C. S. Calude, E. Calude, K. Svozil, Quantum Correlations Conundrum, in *Recent Topics in Mathematical and Computational Linguistics*, ed. by C. Martin-Vide, G. Paun (Editura Academiei Romane, Bucharest 2000), pp. 55-67.
21. K. Svozil, ["Information and Complementarity"](#), *The Quest for a Unified Theory of Information*, ed. b. Wolfgang Hofkirchner (Gordon and Breach Publishers, Amsterdam, 1999), pp. 305-314.
22. Karl Svozil, ["Quantum logic. A brief outline"](#), *Mathematical and Quantum Logic. Proceedings of the 4th Summer School on Analysis, Geometry and Mathematical Physics on August 3-9, 1997 in Karlovassi, Samos*, ed. by K. Keremedis (Sete, Karlovassi, 1998). , [[L^AT_EX](#)], [[BibT_EX](#)].
23. Karl Svozil, ["The limits of mathematics. A book review"](#), *Complexity* **3**, 63 (1998).
24. K. Svozil, ["Reversible computation as a model for the quantum measurement process"](#), in *Cybernetics and Systems '98 Volume I*, ed. by R. Trappl (Austrian Society for Cybernetic Studies, Vienna, 1998), pp. 102-106 [[L^AT_EX](#)], , .

25. Karl Svozil, "[The Church-Turing Thesis as a Guiding Principle for Physics](#)", in *Unconventional Models of Computation*, ed. by Cristian S. Calude, John Casti and Michael J. Dinneen (Springer, Singapore, 1998), pp. 371-385.
26. K. Svozil, "[Information and the Complementarity Game](#)", *World Futures* **50**, 523-532 (1997).
27. K. Svozil, "[On self-reference and self-description](#)", *La nuova Critica. Nuova Serie* **29**(1), 75-86 (1997). Reprinted in *Functional Models of Cognition*; ed. by A. Carsetti (Kluwer, Dordrecht, 2000), p. 189-197 [[book-reference](#)].
28. K. Svozil, "[Undecidability everywhere?](#)", in *Boundaries and Barriers. On the Limits to Scientific Knowledge*, ed. by J. L. Casti and A. Karlquist (Addison-Wesley, Reading, MA, 1996), pp. 215-237. [[BibT_EX](#)], [[L^AT_EX](#)], ,
29. K. Svozil, "The physics of virtual realities", in *Endophysics: The World From Within*, ed. by George Kampis and Peter Weibel (Aerial, Santa Cruz, 1993).
30. K. Svozil, "[Time generated by intrinsic observers](#)", *Cybernetics and Systems '96, Proceedings of the 13th European Meeting on Cybernetics and Systems Research*, ed. by Robert Trappl (Austrian Society for Cybernetic Studies, Vienna, 1996), pp. 162-166 [[L^AT_EX](#)], , ,
31. K. Svozil, "[Quantum computation and complexity theory I](#)", *Bulletin of the European Association of Theoretical Computer Sciences* **55**, 170-207 (1995).
32. K. Svozil, "[Quantum computation and complexity theory II](#)", *Bulletin of the European Association of Theoretical Computer Sciences* **56**, 116-136 (1995).
33. Cristian Calude, Douglas I. Campbell, Karl Svozil and Doru Stefanescu, "[Strong Determinism vs. Computability](#)", *The Foundational Debate, Complexity and Constructivity in Mathematics and Physics*, Werner DePauli Schimanovich, Eckehart Köhler and Friedrich Stadler, eds. (Kluwer, Dordrecht, Boston, London, 1995), p. 115-131. , [[L^AT_EX](#)], .
34. K. Svozil, "[On the computational power of physical systems, undecidability, the consistency of phenomena and the practical uses of paradoxa](#)", in *Fundamental Problems in Quantum Theory: A Conference Held in Honor of Professor John A. Wheeler*, ed. by D. M. Greenberger and A. Zeilinger, *Annals of the New York Academy of Sciences* **755**, 834-841 (1995)  [[BibT_EX](#)] [[L^AT_EX](#)]
35. K. Svozil, "[A constructivist manifesto for the physical sciences - Constructive re-interpretation of physical undecidability](#)", in *The Foundational Debate, Complexity and Constructivity in Mathematics and Physics*, Werner DePauli Schimanovich, Eckehart Köhler and Friedrich Stadler, eds. (Kluwer, Dordrecht, Boston, London, 1995), p. 65-88. [[L^AT_EX](#)], .
36. K. Svozil, "[Extrinsic-Intrinsic Concept and Complementarity](#)", in *Inside Versus Outside*, ed. by H. Atmanspacher, G. J. Dalenoort (Springer, Berlin, 1994), p. 273-288.  [[BibT_EX](#)] [[L^AT_EX](#)]
37. K. Svozil, "How many physical parameters form a minimal and complete description of the world?" in *Nuclei in the Cosmos*, ed. by H. Oberhummer (Springer, Berlin, 1991).
38. M. Dea, M. Dea and K. Svozil, "Interpretations of combinatorial algebras" in *Philosophy of*

38. M. Baaz, N. Brunner and K. Svozil, "Interpretations of combinatory algebras", in *Philosophy of Mathematics, Part I*, ed. by J. Czermak (Hölder-Pichler-Tempsky, Berlin, 1993), p. 393-406.
39. K. Svozil, "Mathematical foundation of physical chaos", in *Gödel Jahrbuch* **1**, ed. by N. Brunner *et al.* (Vienna 1988), 53-85.
40. K. Svozil and R. Lassnig, "Test of phonon mediated pairing from Raman scattering on high-temperature superconducting materials", in *High- superconductors*, ed. by W. Weber (Plenum Press, New York 1988), p. 177-182.
41. K. Svozil, "Metrology of space-time dimension", in *Fundamental Aspects of Quantum Theory (Proc. NATO Advanced Research Study Seminar, Como 1985)*, eds. V. Gorini and A. Frigerio, (Plenum, New York), p. 447-449.

Patent

- Vorrichtung zur Abkühlung von punktförmigem Kühlgut durch Strahlungswärme, *Patent Nr. 393900*, erteilt am 12. 11. 1991.

Preprints (this is not a complete listing of recent preprints)

Please have a look at [arXiv.org](https://arxiv.org) for some of my later preprints & papers.

- Karl Svozil, "[Suggestion of a problem](#)"
- K. Svozil, "[On The Setting Of Scales For Space And Time In Quantized Media](#)", *LBL-16097*, May 1983. 7pp. , ,

Ten recent publications

Experimental evidence of quantum randomness incomputabilityCristian S. Calude^{*} and Michael J. Dinneen[†]*Department of Computer Science, University of Auckland, Private Bag 92019, Auckland, New Zealand*Monica Dumitrescu[‡]*Faculty of Mathematics and Computer Science, University of Bucharest, Str. Academiei 14, RO-010014 Bucharest, Romania*Karl Svozil[§]*Institute for Theoretical Physics, Vienna University of Technology, Wiedner Hauptstrasse 8-10/136, A-1040 Vienna, Austria*

(Received 9 April 2010; revised manuscript received 4 June 2010; published 6 August 2010)

In contrast with software-generated randomness (called pseudo-randomness), quantum randomness can be proven incomputable; that is, it is not exactly reproducible by any algorithm. We provide experimental evidence of incomputability—an asymptotic property—of quantum randomness by performing finite tests of randomness inspired by algorithmic information theory.

DOI: [10.1103/PhysRevA.82.022102](https://doi.org/10.1103/PhysRevA.82.022102)

PACS number(s): 03.65.Ta, 02.50.Fz, 03.67.Lx, 89.70.Cf

I. QUANTUM INDETERMINACY

The irreducible indeterminacy of individual quantum processes postulated by Born [1–3] implies that there exist physical “oracles,” which are capable of effectively producing outputs which are incomputable. Indeed, quantum indeterminism has been proved [4] under some “reasonable” side assumptions implied by Bell-, Kochen-Specker-, and Greenberger-Horne-Zeilinger-type theorems. Yet, as quantum indeterminism is nowhere formally specified, it is important to investigate which (classes of) measurements lead to randomness, what are the reasons for possible distinctions, whether or not the kinds of randomness “emerging” in different classes of quantum measurements are “the same” or “different,” and what are the phenomenologies or signatures of these randomness classes. Questions about “degrees of (algorithmic) randomness” are studied in algorithmic information theory. Here are just four types, among an infinity of others: (i) standard pseudo-randomness produced by software such as MATHEMATICA or MAPLE which are not only Turing computable but cyclic; (ii) pseudo-randomness produced by software which is Turing computable but not cyclic (e.g., digits of π , the ratio between the circumference and the diameter of an ideal circle, or Champernowne’s constant); (iii) Turing incomputable, but not algorithmically random; and (iv) algorithmically random [5–7]. In which of these four classes do we find quantum randomness? Operationally, in the extreme form, Born’s postulate could be interpreted to allow for the production of “random” finite strings; hence quantum randomness could be of type (iv). (Here the quotation marks refer to the fact that randomness for finite strings is too “subjective” to be meaningful for our analysis. The legitimacy of the experimental approach comes from characterizations of random sequences in terms of the

degrees of incompressibility of their finite prefixes [5–7].) A sequence which is not algorithmically random but Turing incomputable can, for instance, be obtained from an algorithmically random sequence $x_1x_2 \cdots x_n \cdots$ by inserting a 0 in between any adjacent original bits, i.e., obtaining the sequence $x_10x_20 \cdots 0x_n0 \cdots$. This transformation destroys algorithmic randomness because obvious correlations have appeared; Turing incomputability is invariant under this transformation because a copy of the original sequence is embedded in the new one. Yet much more subtler correlations among subsequences of Turing incomputable sequences may exist, thus making them compressible and algorithmically nonrandom. There is no *a priori* reason to interpret Born’s indeterminism by its strongest formal expression (i.e., in terms of algorithmic randomness).

Quantum randomness produced by quantum systems which have no classical interpretation can be proven [4] Turing incomputable. More precisely, if the experiment would run under ideal conditions “to infinity,” the resulting infinite sequence of bits would be Turing incomputable; that is, no Turing machine (or algorithm) could reproduce exactly this infinite sequence of digits. This result has many consequences. Here is one example: The experiment could produce a billion 0’s, but not all bits produced will be 0. A stronger form of incomputability holds true: Every Turing machine (or algorithm) can reproduce exactly only finitely many scattered digits of that infinite sequence. Yet this proof stops short of showing that the sequence produced by such a quantum experiment is algorithmically random; that is, it is unknown whether or not such a sequence is or is not algorithmically random. One of the strategies toward answering this question is to empirically perform tests “against” the algorithmic randomness hypothesis.

Our (more modest) aim is to present tests capable of distinguishing computable from incomputable sources of “randomness” by examining (long, but) finite prefixes of infinite sequences. Such differences are guaranteed to exist by [4], but, because computability is an asymptotic property, there was no guarantee that finite tests can “pick” differences in the prefixes that we have analyzed.

^{*}cristian@cs.auckland.ac.nz; <http://www.cs.auckland.ac.nz/~cristian>[†]mjd@cs.auckland.ac.nz; <http://www.cs.auckland.ac.nz/~mjd>[‡]mdumi@fmi.unibuc.ro; http://fmi.unibuc.ro/ro/dumitrescu_monica[§]svozil@tuwien.ac.at; <http://tph.tuwien.ac.at/~svozil>

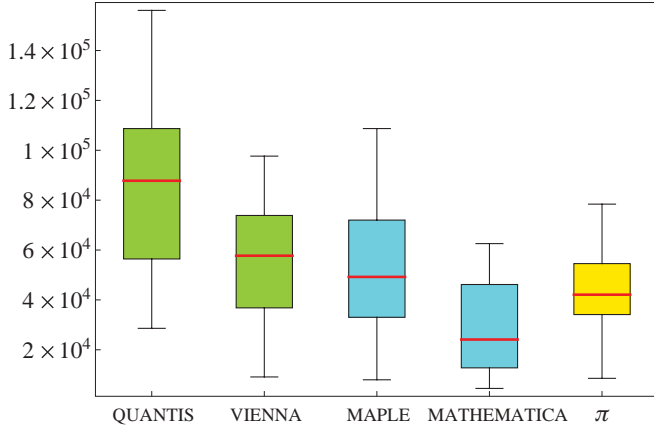


FIG. 1. (Color online) Box-and-whisker plot for the results of the “book stack” randomness test.

II. TESTS OF EXPERIMENTAL QUANTUM INDETERMINACY

Based on Born’s postulate, several quantum random number generators employing beam splitters have recently been proposed and realized [8–15]. In what follows a detailed analysis of bit strings of length 2^{32} obtained by two such quantum random number generators will be presented. (The size correlates well with the square root of the cycle length used by cyclic pseudo-random generators; randomness properties of longer strings generated in this way are impaired.) We will compare the performance of quantum random number generators with software-generated number generators on randomness inspired by algorithmic information theory (which complement some commonly used statistical tests implemented in “batteries” of test suites such as, for instance, DIEHARD [16], NIST [17], or TESTU01 [18]). The standard test suites are often based on tests which are not designed for physical random number generators, but rather to quantify the quality of the cyclic pseudo-random numbers generated by algorithms. As we would like to separate “truly” random sequences from software-generated random sequences, the emphasis is on the former type of tests.

The tests based on algorithmic information theory directly analyze randomness and thus the strongest possible form of incomputability. They differ from tests employed in the standard randomness batteries as they depend on irreducible algorithmic information content, which is constant for algorithmic pseudo-random sequences. Some tests are related to each other, as for instance sequences which are not Borel normal (cf. the following) could be algorithmically compressed; the analysis of results helps understand subtle differences at the edge of in-

computability or algorithmic randomness. All tests depend on the size of the analyzed strings; the legitimacy of our approach is given by the fact that algorithmic randomness of an infinite sequence can be “uniformly read” in its prefixes (cf. [7]).

III. DATA SOURCES

The analyzed quantum data consist of 10 quantum random strings generated with the commercially available QUANTIS device [19], based on research of a group in Geneva [11], as well as 10 quantum random strings generated by the Vienna Institute for Quantum Optics and Quantum Information (IQOQI) group [20]. The pseudo-random data consist of 10 pseudo-random strings produced by MATHEMATICA 6 [21], and 10 pseudo-random strings produced by MAPLE 11 [22], as well as 10 strings of 2^{32} bits from the binary expansion of π obtained from the University of Tokyo’s supercomputing center [23].

The signals of the QUANTIS device are generated by a light-emitting diode (LED) producing photons which are then transmitted toward a beam splitter (a semitransparent mirror) and two single-photon detectors (detectors with single-photon resolution) to record the outcomes associated with the symbols “0” and “1,” respectively [19]. Due to hardware imbalances which are difficult to overcome at this level, QUANTIS processes these raw data by unbiasing the sequence by a von Neumann-type normalization: The biased raw sequence of zeros and ones is partitioned into fixed subsequences of length two; then the even-parity sequences “00” and “11” are discarded, and only the odd parity ones “01” and “10” are kept. In a second step, the remaining sequences are mapped into the single symbols $01 \mapsto 0$ and $10 \mapsto 1$, thereby extracting a new unbiased sequence at the cost of a loss of original bits ([24], p. 768).

This normalization method requires that the events are (temporally) uncorrelated and thus independent. (For the sake of a simple counterexample, the von Neumann normalization of the sequences $010101 \dots$ or $1100110011 \dots$ are the constant-0 sequence $000 \dots$ and the empty sequence.) Under the independence hypothesis, the normalized sequences are Borel normal with probability one [25]; e.g., all finite subsequences of length n occur with their expected asymptotic frequencies 2^{-n} . (Alas, see [26] for some pitfalls when transforming such sequences.)

The signals of the Vienna IQOQI group were generated with photons from a weak blue LED light source, which impinged on a beam splitter without any polarization sensitivity with two output ports associated with the codes “0” and “1,” respectively [10]. There was *no* pre- or post-processing of the raw data stream, in particular no von Neumann normalization as discussed for the QUANTIS device; however, the output was

TABLE I. Statistics for the results of the “book stack” randomness test.

	Minimum	Q1	Median	Q3	Maximum	Mean	Standard deviation
MAPLE	796 4	344 90	492 20	696 30	108 700	534 10	330 68.58
MATHEMATICA	450 8	130 20	241 10	434 50	625 70	279 40	194 06.03
QUANTIS	286 00	604 80	877 80	106 700	156 100	899 90	415 45.76
VIENNA	911 0	384 20	577 20	732 20	976 60	538 60	279 38.92
π	855 1	354 80	421 00	528 70	784 10	412 80	207 58.46

TABLE II. Statistics for the results based on the Solovay-Strassen probabilistic primality test.

	Minimum	$Q1$	Median	$Q3$	Maximum	Mean	Standard deviation
MAPLE	93.0	96.0	101.0	113.5	120.0	104.9	10.577 23
MATHEMATICA	93.0	97.0	109.0	132.3	142.0	113.5	19.608 67
QUANTIS	99.0	103.3	113.0	121.3	130.0	112.6	10.668 75
VIENNA	82.0	100.3	104.5	109.0	119.0	103.5	11.037 81
π	84.0	91.8	106.0	110.8	128.0	104.7	10.668 75

constantly monitored (the exact method being subject to a pending patent). In very general terms, the setup needs to be running for at least one day to reach a stable operation. There is a regulation mechanism which keeps track of the bias between “0” and “1” and tunes the random generator for perfect symmetry. Each data file was created in one continuous run of the device lasting over hours.

We have employed the extended cellular automaton generator default of MATHEMATICA 6’s pseudo-random function. It is based on a particular five-neighbor rule, so each new cell depends on five nonadjacent cells from the previous step [21]. MAPLE 11 uses a Mersenne Twister algorithm to generate a random pseudo-random output [22].

IV. TESTING INCOMPUTABILITY AND RANDOMNESS

The tests we performed can be grouped into (i) two tests based on algorithmic information theory, (ii) statistical tests involving frequency counts (Borel normality test), (iii) a test based on Shannon’s information theory, and (iv) a test based on random walks.

In Figures 1–5 the graphical representation of the results is rendered in terms of box-and-whisker plots, which characterize groups of numerical data through five characteristic summaries: test minimum value, first quantile (representing one fourth of the test data), median or second quantile (representing half of the test data), third quantile (representing three fourths of the test data), and test maximum value. Mean and standard deviation of the data representing the results of the tests are calculated. Tables containing the experimental data

and the programs used to generate the data can be downloaded from our extended paper [27].

A. Book stack randomness test

The *book stack* (also known as “move to front”) test [28,29] is based on the fact that compressibility is a symptom of less randomness.

The results, presented in Fig. 1 and Table I, are derived from the original count, the count after the application of the transformation, and the difference. The key metric for this test is the count of ones after the transformation. The book stack encoder does not compress data but instead rewrites each byte with its index from the top (front) with respect to its input characters being stacked (moved to front). Thus, if a lot of repetitions occur (i.e., a symptom of nonrandomness), then the output contains more zeros than ones due to the sequence of indices generally being smaller numerically.

B. Solovay-Strassen probabilistic primality test

The second algorithmic test, based on the Solovay-Strassen probabilistic primality test, uses Carmichael (composite) numbers, which are “difficult” to factor, to determine the quality of randomness by computing how fast the probabilistic primality test reaches the verdict “composite” [30,31].

To test whether a positive integer n is prime, we take k natural numbers uniformly distributed between 1 and $n - 1$, inclusive, and, for each chosen i , check whether the predicate $W(i, n)$ holds. If this is the case we say that “ i is a witness of n ’s compositeness.” If $W(i, n)$ holds for at least one i then

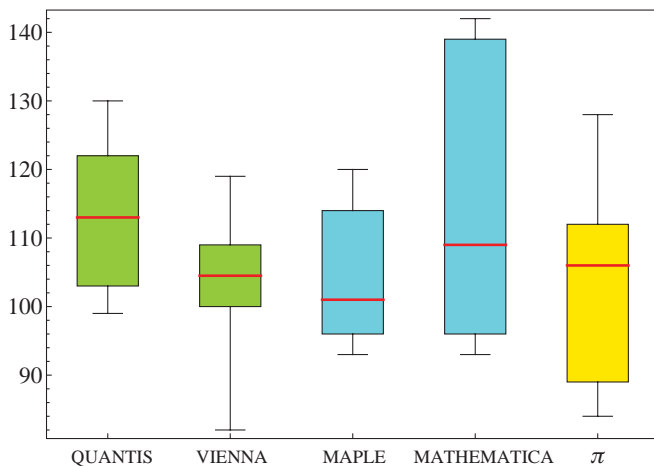


FIG. 2. (Color online) Box-and-whisker plot for the results based on the Solovay-Strassen probabilistic primality test.

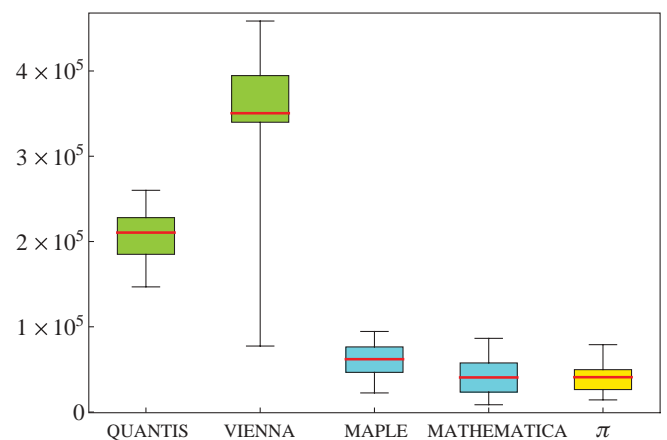


FIG. 3. (Color online) Box-and-whisker plot for the results for tests of the Borel normality property.

TABLE III. Statistics for the results for tests of the Borel normality property.

	Minimum	$Q1$	Median	$Q3$	Maximum	Mean	Standard deviation
MAPLE	224 30	471 70	619 90	761 30	945 10	602 10	219 33.52
MATHEMATICA	8572	255 00	405 90	556 50	864 30	418 70	232 29.77
QUANTIS	146 800	185 100	210 500	226 600	260 000	207 200	335 15.65
VIENNA	774 10	340 200	350 500	392 500	260 000	337 100	103 354.3
π	142 60	288 60	408 80	478 60	790 30	402 20	179 06.21

n is composite; otherwise, the test is inconclusive, but in this case if one declares n to be prime then the probability of being wrong is smaller than 2^{-k} .

This is because at least half the i values from 1 to $n - 1$ satisfy $W(i, n)$ if n is indeed composite, and *none* of them satisfy $W(i, n)$ if n is prime [30]. Selecting k natural numbers between 1 and $n - 1$ is the same as choosing a binary string s of length $n - 1$ with k 1's such that the i th bit is 1 if and only if i is selected. Reference [31] contains a proof that, if s is a long enough algorithmically random binary string, then n is prime if and only if $Z(s, n)$ is true, where Z is a predicate constructed directly from conjunctions of negations of W .¹

A Carmichael number is a composite positive integer k satisfying the congruence $b^{k-1} \equiv 1 \pmod{k}$ for all integers b relative prime to k . Carmichael numbers are composite, but they are difficult to factorize and thus are “very similar” to primes; they are sometimes called pseudo-primes. Fermat’s primality test declares significantly more Carmichael numbers as primes than the Solovay-Strassen test. With increasing values, Carmichael numbers become “rare.”²

We used the Solovay-Strassen test for all Carmichael numbers less than 10^{16} —computed in Refs. [32,33]—with

¹In fact, every “decent” Monte Carlo simulation algorithm in which tests are chosen according to an algorithmic random string produces a result which is not only true with high probability but *rigorously correct* [34].

²There are 1,401,644 Carmichael numbers in the interval $[1, 10^{18}]$.

numbers selected according to increasing prefixes of each sample string till the algorithm returns a nonprimality verdict. The metric is given by the length of the sample used to reach the correct verdict of nonprimality for all of the 246 683 Carmichael numbers less than 10^{16} . [We started with $k = 1$ tests (per each Carmichael number) and increase k until the metric goal is met; as k increases we always use new bits (never recycling) from the sample source strings.] The results are presented in Fig. 2 and Table II.

C. Borel normality test

Borel normality—requesting that every binary string appears in the sequence with the correct probability 2^{-n} for a string of length n —served as the first mathematical definition of randomness [25]. A sequence is (Borel) normal if every binary string appears in the sequence with the right probability (which is 2^{-n} for a string of length n). A sequence is normal if and only if it is incompressible by any information lossless finite-state compressor [35], so normal sequences are those sequences that appear random to any finite-state machine.

Every algorithmic random infinite sequence is Borel normal [36]. The converse implication is not true: There exist computable normal sequences (e.g., Champernowne’s constant).

Normality is invariant under finite variations: Adding, removing, or changing a finite number of bits in any normal sequence leaves it normal. Further, if a sequence satisfies the normality condition for strings of length $n + 1$, then it also satisfies normality for strings of length n , but the converse is not true.

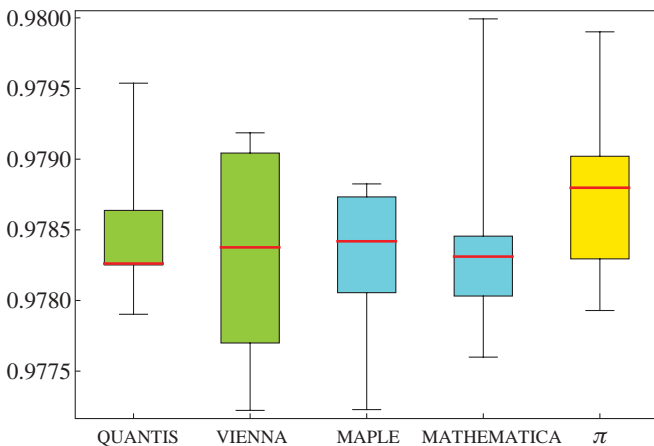


FIG. 4. (Color online) Box-and-whisker plot for average results in “sliding window” estimations of the Shannon entropy.

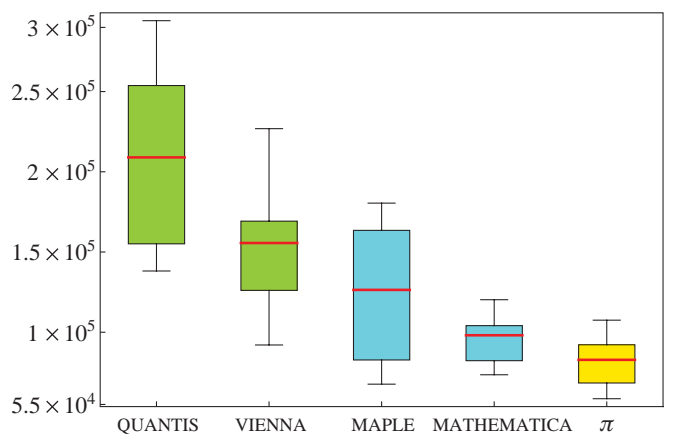


FIG. 5. (Color online) Box-and-whisker plot for the results of the random walk tests.

TABLE IV. Statistics for average results in “sliding window” estimations of the Shannon entropy.

	Minimum	$Q1$	Median	$Q3$	Maximum	Mean	Standard deviation
MAPLE	0.977 2	0.978 1	0.978 4	0.978 7	0.978 8	0.978 3	0.000 523 161 7
MATHEMATICA	0.977 6	0.978 1	0.978 3	0.978 5	0.980 0	0.978 3	0.000 665 493 6
QUANTIS	0.977 9	0.978 3	0.978 3	0.978 6	0.979 5	0.978 4	0.000 452 269 9
VIENNA	0.977 2	0.977 7	0.978 4	0.979 0	0.979 2	0.978 3	0.000 695 583 4
π	0.977 9	0.978 4	0.978 8	0.979 0	0.979 9	0.978 8	0.000 606 272 4

Normality was transposed to strings in Ref. [36]. In this process one has to replace limits with inequalities. As a consequence, these two properties, which are valid for sequences, are no longer true for strings.

For any fixed integer $m > 1$, consider the alphabet $B_m = \{0, 1\}^m$ consisting of all binary strings of length m , and for every $1 \leq i \leq 2^m$ denote by $N_i^m(x)$ the number of occurrences of the lexicographical i th binary string of length m in the string x (considered over the alphabet B_m). By $|x|_m$ we denote the length of x over B_m ; $|x|_1 = |x|$. A string x is Borel normal if for every natural $1 \leq m \leq \log_2 \log_2 |x|$,

$$\left| \frac{N_j^m(x)}{|x|_m} - 2^{-m} \right| \leq \sqrt{\frac{\log_2 |x|}{|x|}},$$

for every $1 \leq j \leq 2^m$. In Ref. [36] it is shown that almost all algorithmic random strings are Borel normal.

First we count the maximum, minimum, and difference of nonoverlapping occurrences of m -bit ($m = 1, \dots, 5$) strings in each sample string. Then we test the Borel normality property for each sample string and found that almost all strings pass the test, with some notable exceptions. We found that several of the Vienna sequences failed the expected count range for $m = 2$ and a few of the Vienna sequences were outside the expected range for $m = 3$ and $m = 4$ (with some less than the expected minimum count and some more than the expected maximum count). The only other bit sequence that was outside the expected range count was one of the MATHEMATICA sequences that had too big of a count for $k = 1$. Figure 3 depicts a box-and-whisker plot of the results. This is followed by statistical (numerical) details in Table III.

D. Test based on Shannon’s information theory

The next test computes “sliding window” estimations of the Shannon entropy L_n^1, \dots, L_n^t according to the method described in [37]: A smaller entropy is a symptom of less randomness. The results are presented in Fig. 4 and Table IV.

E. Test based on random walks

A symptom of nonrandomness of a string is detected when the plot generated by viewing a sample sequence as a 1D random walk meanders “less away” from the starting point (both ways); hence the maximum–minimum range is the metric.

The fifth test is thus based on viewing a random sequence as a one-dimensional *random walk*, whereby the successive bits, associated with an increase of one unit *per* bit of the x coordinate, are interpreted as follows: 1 = “move up” and 0 = “move down” on the y axis. In this way a measure is obtained for how far away one can reach from the starting point (either positive or negative) from the starting y value of 0 that one can reach using successive bits of the sample sequence. Figure 5 and Table V summarize the results.

V. STATISTICAL ANALYSIS OF RANDOMNESS TESTS RESULTS

In what follows the significance of results corresponding to each randomness test applied to all five sources are analyzed by means of some statistical comparison tests. The Kolmogorov-Smirnov test for two samples [38] determines whether two datasets differ significantly. This test has the advantage of making no prior assumption about the distribution of data (i.e., it is nonparametric and distribution free).

The Kolmogorov-Smirnov test returns a p value, and the decision “the difference between the two datasets is statistically significant” is accepted if the p value is *less than* 0.05, or, stated pointedly, if the probability of taking a wrong decision is less than 0.05. Exact p values are only available for the two-sided two-sample tests with no ties.

In some cases we have tried to double-check the decision “no significant differences between the datasets” at the price of a supplementary, plausible distribution assumption. Therefore, we have performed the Shapiro-Wilk test for normality [39] and, if normality is not rejected, we have assumed that the datasets have normal (Gaussian) distributions. In order to be able to compare the expected values (means) of the two

TABLE V. Statistics for the results of the random walk tests.

	Minimum	$Q1$	Median	$Q3$	Maximum	Mean	Standard deviation
MAPLE	676 40	887 30	126 400	162 500	180 500	125 300	429 95.59
MATHEMATICA	735 00	847 60	981 10	103 400	120 300	964 50	146 85.34
QUANTIS	138 200	161 600	209 000	250 200	294 200	211 300	559 60.23
VIENNA	920 70	130 200	155 600	167 600	226 900	152 900	367 17.55
π	585 70	704 20	828 00	919 20	107 500	821 20	148 33.75

TABLE VI. Kolmogorov-Smirnov test p values for the “book stack” tests.

	MATHEMATICA	QUANTIS	VIENNA	π
MAPLE	0.417 5	0.167 8	0.994 5	0.417 5
MATHEMATICA		0.002 1	0.167 8	0.417 5
QUANTIS			0.167 8	0.012 3
VIENNA				0.417 5

samples, the Welch t -test [40], which is a version of Student’s test, has been applied. In order to emphasize the relevance of p values less than 0.05 associated with Kolmogorov-Smirnov, Shapiro-Wilk, and Welch’s t -tests, they are printed in boldface and discussed in the text.

A. Book stack randomness test

The results of the Kolmogorov-Smirnov test associated with the “book-stack” tests are enumerated in Table VI. Statistically significant differences are identified for QUANTIS versus MATHEMATICA and π .

As more compression is a symptom of less randomness, the corresponding ranking of samples is as follows: $\langle \text{QUANTIS} \rangle = 899\,88.9 > \langle \text{VIENNA} \rangle = 538\,63.8 > \langle \text{MAPLE} \rangle = 534\,11.6 > \langle \pi \rangle = 412\,77.5 > \langle \text{MATHEMATICA} \rangle = 279\,38.3$. The Shapiro-Wilk tests results are presented in Table VII.

Since normality is not rejected for any string, we apply the Welch’s t -test for the comparison of means. The results are enumerated in Table VIII. Significant differences between the means are identified for the following sources: (i) QUANTIS versus all other sources (MAPLE, MATHEMATICA, VIENNA, π) and (ii) VIENNA versus MATHEMATICA and MAPLE (as already mentioned).

B. Solovay-Strassen probabilistic primality test

The Kolmogorov-Smirnov test results for this test are presented in Table IX, where no significant differences are detected.

The Shapiro-Wilk test results are presented in Table X. Since there is no clear pattern of normality for the data, the application of Welch’s t -test is not appropriate.

C. Borel test of normality

The results of the Kolmogorov-Smirnov test are presented in Table XI.

Statistically significant differences are identified for

- (i) QUANTIS versus MAPLE, MATHEMATICA, and π ;
- (ii) VIENNA versus MAPLE, MATHEMATICA, and π ; and
- (iii) QUANTIS versus VIENNA.

Note the following:

- (1) Pseudo-random strings pass the Borel normality test for comparable, relatively small (with respect to quantum strings;

TABLE VII. Shapiro-Wilk test p values for the “book stack” tests.

	MATHEMATICA	QUANTIS	VIENNA	π
MAPLE				
0.788 0	0.481 9	0.723 9	0.814 6	0.517 2

TABLE VIII. Welch’s t -test p values for the “book stack” tests.

	MATHEMATICA	QUANTIS	VIENNA	π
MAPLE	0.053 5	0.043 6	0.974	0.341 2
MATHEMATICA		0.000 9	0.028 3	0.155 1
QUANTIS			0.036 8	0.005 4
VIENNA				0.269 0

cf. the following) numbers of counts: If the angle brackets $\langle x \rangle$ stand for the statistical mean of tests on x , then $\langle \text{MAPLE} \rangle = 602\,10$, $\langle \text{MATHEMATICA} \rangle = 418\,70$, $\langle \pi \rangle = 402\,20$.

(2) Quantum strings pass the Borel normality test only for “much larger numbers” of counts ($\langle \text{QUANTIS} \rangle = 207\,200$, $\langle \text{VIENNA} \rangle = 337\,100$).

As a result, the Borel normality test detects and identifies statistically significant differences between all pairs of computable and incomputable sources of “randomness.”

D. Test based on Shannon’s information theory

The results of the Kolmogorov-Smirnov test are presented in Table XII. No significant differences are detected. The descriptive statistics data for the results of this test indicate almost identical distributions corresponding to the five sources.

The results of the Shapiro-Wilk test associated with a test based on Shannon’s information theory are presented in Table XIII. Since there is no clear pattern of normality for the data, the application of Welch’s t -test is not appropriate.

E. Test based on random walks

The Kolmogorov-Smirnov test results associated with test based on random walks are presented in Table XIV. Statistically significant differences are identified for (i) QUANTIS versus all other sources (MAPLE, MATHEMATICA, VIENNA, and π); (ii) VIENNA versus MATHEMATICA, VIENNA (as already mentioned), and π ; and (iii) MAPLE versus π .

Quantum strings move farther away from the starting point than the pseudo-random strings (i.e., $\langle \text{QUANTIS} \rangle > \langle \text{VIENNA} \rangle > \langle \text{MAPLE} \rangle > \langle \text{MATHEMATICA} \rangle > \langle \pi \rangle$).

It was quite natural to double-check the conclusion “QUANTIS and VIENNA do not exhibit significant differences.” Hence we run the Shapiro-Wilk test, which concludes that normality is not rejected (cf. Table XV).

Next, we apply the Welch’s t -test for the comparison of means. The results are given in Table XVI. Significant

TABLE IX. Kolmogorov-Smirnov test p values for the Solovay-Strassen tests.

	MATHEMATICA	QUANTIS	VIENNA	π
MAPLE	0.759 1	0.400 5	0.759 1	0.759 1
MATHEMATICA		0.759 1	0.759 1	0.759 1
QUANTIS			0.400 5	0.759 1
VIENNA				0.988 3

TABLE X. Shapiro-Wilk test p values for the Solovay-Strassen tests.

MAPLE	MATHEMATICA	QUANTIS	VIENNA	π
0.069 6	0.036 3	0.437 8	0.696 3	0.431 5

TABLE XI. Kolmogorov-Smirnov test p values for the Borel normality tests.

	MATHEMATICA	QUANTIS	VIENNA	π
MAPLE	0.417 5	$< 10^{-4}$	0.000 2	0.167 8
MATHEMATICA		$< 10^{-4}$	0.000 2	0.994 5
QUANTIS			0.000 2	$< 10^{-4}$
VIENNA				0.000 2

TABLE XII. Kolmogorov-Smirnov test p values for Shannon's information theory tests.

	MATHEMATICA	QUANTIS	VIENNA	π
MAPLE	0.787 0	0.787 0	0.787 0	0.167 8
MATHEMATICA		0.787 0	0.417 5	0.052 5
QUANTIS			0.417 5	0.167 8
VIENNA				0.417 5

TABLE XIII. Shapiro-Wilk test p values for Shannon's information theory tests.

MAPLE	MATHEMATICA	QUANTIS	VIENNA	π
0.196 2	0.018 9	0.034 5	0.379 0	0.877 4

TABLE XIV. Kolmogorov-Smirnov test p values for the random walk tests.

	MATHEMATICA	QUANTIS	VIENNA	π
MATHEMATICA	0.167 8	0.012 3	0.417 5	0.052 5
QUANTIS		$< 10^{-4}$	0.002 1	0.167 8
VIENNA			0.052 5	$< 10^{-4}$
π				0.000 2

TABLE XV. Shapiro-Wilk test p values for the random walk tests.

MAPLE	MATHEMATICA	QUANTIS	VIENNA	π
0.200 6	0.926 8	0.546 4	0.888 8	0.957 7

TABLE XVI. Welch's t -test p values for the random walk tests.

	MATHEMATICA	QUANTIS	VIENNA	π
MAPLE	0.069 61	0.001 3	0.140 9	0.011 9
MATHEMATICA		$< 10^{-4}$	0.000 7	0.043 5
QUANTIS			0.014 3	$< 10^{-4}$
VIENNA				0.000 1

differences between the means are identified for the following sources: (i) QUANTIS versus all other sources (MAPLE, QUANTIS, VIENNA, and π); (ii) VIENNA versus MATHEMATICA, QUANTIS (as already mentioned), and π ; (iii) MAPLE versus π .

VI. SUMMARY

Tests based on algorithmic information theory analyze algorithmic randomness, the strongest possible form of incomputability. In this respect they differ from tests employed in the standard test batteries, as the former depend on irreducible algorithmic information content, which is constant for algorithmic pseudo-random generators. Thus the set of randomness tests performed for our analysis could in principle be expected to be "more sensitive" with respect to differentiating between quantum randomness and algorithmic types of "quasi-randomness" than statistical tests alone.

All tests have produced evidence—with different degrees of statistical significance—of differences between quantum and nonquantum sources:

(a) For the test for Borel normality—the strongest discriminator test—statistically significant differences between the distributions of datasets are identified for (i) QUANTIS versus MAPLE, MATHEMATICA, and π ; (ii) VIENNA versus MAPLE, MATHEMATICA, and π ; and (iii) QUANTIS versus VIENNA. Not only is the average number of counts larger for quantum sources, but the increase is quite significant: QUANTIS is 3.5–5 times larger than the corresponding average number of counts for software-generated sources, and VIENNA is 5–8 times larger than those values.

(b) For the test based on random walks, statistically significant differences between the distributions of datasets are identified for (i) QUANTIS versus all other sources (MAPLE, MATHEMATICA, VIENNA, and π) and (ii) VIENNA versus MATHEMATICA, VIENNA, and π . Quantum strings move farther away from the starting point than the pseudo-random strings (i.e., $\langle \text{QUANTIS} \rangle > \langle \text{VIENNA} \rangle > \langle \text{MAPLE} \rangle > \langle \text{MATHEMATICA} \rangle > \langle \pi \rangle$).

(c) For the "book-stack" test, significant differences between the means are identified for the following sources: (i) QUANTIS versus all other sources (MAPLE, MATHEMATICA, VIENNA, and π) and (ii) VIENNA versus MATHEMATICA and MAPLE.

(d) For the test based on Shannon's information theory, as well as for the Solovay-Strassen test, *no significant differences* among the five chosen sources are detected. In the first case the reason may come from the fact that averages are the same for all samples. In the second case the reason may be because the test is based solely on the behavior of algorithmic random strings and not on a specific property of randomness.

We close with a cautious remark about the impossibility to formally or experimentally "prove absolute randomness." Any claim of randomness can only be secured *relative* to, and *with respect* to, a more or less large class of laws or behaviors, as it is impossible to inspect the hypothesis against an infinity of—and even less so all—conceivable laws. To rephrase a statement about computability ([41], p. 11), "How can we ever exclude the possibility of our presented, some day (perhaps by some extraterrestrial visitors), with a (perhaps extremely

complex) device that ‘computes’ and ‘predicts’ a certain type of hitherto ‘random’ physical behavior?”

ACKNOWLEDGMENTS

We are grateful to Thomas Jennewein and Anton Zeilinger for providing us with the quantum random bits produced at the University of Vienna by the Vienna IQOQI group, for the description of their method, critical comments, and interest in this research. We thank Alastair Abbott, Hector

Zenil, and Boris Ryabko for interesting comments; Ulrich Speidel for his tests for which some partial results have been reported in our extended paper [27]; Stefan Wegenkittl for critical comments of various drafts of this paper and his suggestions to exclude some tests; and the anonymous referees for constructive suggestions. CSC gratefully acknowledges the support of the Hood Foundation and the Vienna University of Technology. KS gratefully acknowledges support of the CDMTCS at the University of Auckland, as well as of the Ausseninstitut of the Vienna University of Technology.

-
- [1] M. Born, *Z. Phys.* **37**, 863 (1926).
 - [2] M. Born, *Z. Phys.* **38**, 803 (1926).
 - [3] A. Zeilinger, *Nature (London)* **438**, 743 (2005).
 - [4] C. S. Calude and K. Svozil, *Adv. Sci. Lett.* **1**, 165 (2008).
 - [5] P. Martin-Löf, *Inform. Control* **9**, 602 (1966).
 - [6] G. J. Chaitin, *Exploring Randomness* (Springer Verlag, London, 2001).
 - [7] C. Calude, *Information and Randomness—An Algorithmic Perspective*, 2nd ed. (Springer, Berlin, 2002).
 - [8] K. Svozil, *Phys. Lett. A* **143**, 433 (1990).
 - [9] J. G. Rarity, M. P. C. Owens, and P. R. Tapster, *J. Mod. Opt.* **41**, 2435 (1994).
 - [10] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, *Rev. Sci. Instrum.* **71**, 1675 (2000).
 - [11] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, *J. Mod. Opt.* **47**, 595 (2000).
 - [12] M. Hai-Qiang, W. Su-Mei, Z. Da, C. Jun-Tao, J. Ling-Ling, H. Yan-Xue, and W. Ling-An, *Chin. Phys. Lett.* **21**, 1961 (2004).
 - [13] P. X. Wang, G. L. Long, and Y. S. Li, *J. Appl. Phys.* **100**, 056107 (2006).
 - [14] M. Fiorentino, C. Santori, S. M. Spillane, R. G. Beausoleil, and W. J. Munro, *Phys. Rev. A* **75**, 032334 (2007).
 - [15] K. Svozil, *Phys. Rev. A* **79**, 054306 (2009).
 - [16] G. Marsaglia [<http://www.stat.fsu.edu/pub/diehard/>].
 - [17] A. Rukhin *et al.*, NIST Special Publ. 800-22 (National Institute of Standards and Technology, Washington DC, 2001) [<http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22b.pdf>].
 - [18] P. L’Ecuyer and R. Simard, *ACM Trans. Math. Software (TOMS)* **33**, 22 (2007).
 - [19] ID Quantique SA, QUANTIS (idQuantique, Geneva, Switzerland, 2001–2010) [<http://www.idquantique.com/images/stories/PDF/quantis-random-generator/quantis-whitepaper.pdf>].
 - [20] T. Jennewein, Institut für Quantenoptik und Quanteninformatik, Quantum random number generator (private communication).
 - [21] Wolfram Research, Inc., MATHEMATICA Version 6.0 (Wolfram Research, Waterloo, Ontario, 2007) [<http://reference.wolfram.com/mathematica/tutorial/RandomNumberGeneration.html>].
 - [22] Maplesoft, MAPLE Version 11 (Maplesoft, Champaign, IL, 2007) [<http://www.maplesoft.com/support/help/Maple/view.aspx?path=rand>].
 - [23] Y. Kanada and D. Takahashi, Calculation of π up to 4 294 960 000 decimal digits, University of Tokyo (1995), [<ftp://pi.super-computing.org>].
 - [24] J. von Neumann, National Bureau of Standards Applied Math Series **12**, 36 (1951), reprinted in *John von Neumann, Collected Works*, Vol. V, edited by A. H. Traub (MacMillan, New York, 1963), pp. 768–770.
 - [25] É. Borel, *Rendiconti del Circolo Matematico di Palermo* **27**, 247 (1909).
 - [26] P. Hertling, *J. Universal Comput. Sci.* **8**, 235 (2002).
 - [27] C. S. Calude, M. J. Dinneen, M. Dumitrescu, and K. Svozil, Report CDMTCS-372 (Centre for Discrete Mathematics and Theoretical Computer Science, University of Auckland, Auckland, New Zealand, 2009), e-print [arXiv:0912.4379](http://arxiv.org/abs/0912.4379).
 - [28] B. Y. Ryabko and A. I. Pestunov, *Prob. Peredachi Inf.* **40**, 73 (2004).
 - [29] B. Y. Ryabko and V. A. Monarev, *J. Statist. Plan. Inference* **133**, 95 (2005).
 - [30] R. Solovay and V. Strassen, *SIAM J. Comput.* **6**, 84 (1977). Corrigendum in [42].
 - [31] G. J. Chaitin and J. T. Schwartz, *Commun. Pure Appl. Math.* **31**, 521 (1978).
 - [32] R. G. Pinch, e-print [arXiv:math.NT/9803082](http://arxiv.org/abs/math.NT/9803082).
 - [33] R. G. Pinch, in *Proceedings of Conference on Algorithmic Number Theory 2007. TUCS General Publication No. 46*, edited by A.-M. Ernvall-Hytönen, M. Jutila, J. Karhumäki, and A. Lepistö (Turku Centre for Computer Science, Turku, Finland, 2007), pp. 129–131.
 - [34] C. Calude and M. Zimand, *Int. J. Comput. Math.* **16**, 47 (1984).
 - [35] J. Ziv and A. Lempel, *IEEE Trans. Inf. Theory* **24**, 530 (1978).
 - [36] C. Calude, in *Developments in Language Theory*, edited by G. Rozenberg and A. Salomaa (World Scientific, Singapore, 1994), pp. 113–129.
 - [37] A. D. Wyner, IEEE Information Theory Society (1994).
 - [38] W. J. Conover, *Practical Nonparametric Statistics* (Wiley, New York, 1999), p. 584.
 - [39] S. S. Shapiro and M. B. Wilk, *Biometrika* **52**, 591 (2005).
 - [40] B. L. Welch, *Biometrika* **34**, 28 (1947).
 - [41] M. Davis, *Computability and Unsolvability* (McGraw-Hill, New York, 1958).
 - [42] R. Solovay and V. Strassen, *SIAM J. Comput.* **7**, 118 (1978).

The diagonalization method in quantum recursion theory

Karl Svozil

Published online: 16 May 2009
© Springer Science+Business Media, LLC 2009

Abstract As quantum parallelism allows the effective co-representation of classical mutually exclusive states, the diagonalization method of classical recursion theory has to be modified. Quantum diagonalization involves unitary operators whose eigenvalues are different from one.

Keywords Quantum information · Quantum recursion theory · Halting problem

PACS 03.67.Hk · 03.65.Ud

1 Introduction

The reasoning in formal logic and the theory of recursive functions and effective computability [1–6], at least insofar as their applicability to worldly things is concerned [7], makes implicit assumptions about the physical meaningfulness of the entities of discourse; e.g., their actual physical representability and operationalizability [8]. It is this isomorphism or correspondence between the phenomena and theory and vice versa—postulated by the Church-Turing thesis [9]—which confers power to the formal methods. Therefore, any finding in physics presents a challenge to the formal sciences; at least insofar as they claim to be relevant to the physical universe, although history shows that the basic postulates have to be re-considered very rarely.

For example, the fundamental atom of classical information, the bit, is usually assumed to be in one of two possible mutually exclusive states, which can be represented

K. Svozil (✉)
Institute for Theoretical Physics, Vienna University of Technology,
Wiedner Hauptstraße 8-10/136, 1040 Vienna, Austria
e-mail: svozil@tuwien.ac.at
URL: <http://tph.tuwien.ac.at/~svozil>

by two distinct states of a classical physical system. These issues have been extensively discussed in the context of energy dissipation associated with certain logical operations and universal (ir)reversible computation [10–13].

In general, all varieties of physical states, as well as their evolution and transformations, are relevant for propositional logic as well as for a generalized theory of information. Quantum logic [14], partial algebras [15, 16], empirical logic [17, 18] and continuous time computations [19] are endeavors in this direction. These states need not necessarily be mapped into or bounded by classical information. Likewise, physical transformations and manipulations available, for instance, in quantum information and classical continuum theory, may differ from the classical paper-and-pencil operations modeled by universal Turing machines. Hence, the computational methods available as “elementary operations” have to be adapted to cope with the additional physical capabilities [20].

Indeed, in what follows it is argued that, as quantum theory offers nonclassical states and operators available in quantum information theory, several long-held assumptions on the character and transformation of classical information have to be adapted. As a consequence, the formal techniques in manipulating information in the theory of recursive functions and effective computability have to be revised. Particular emphasis is given to undecidability and the diagonalization method.

2 Quantum information theory

As several fine presentations of quantum information and computation theory exist (cf. Refs. [21–29] for a few of them), there is no need of an extended exposition. In what follows, we shall mainly follow Mermin’s notation [29, 30]. For the representation of both a single classical and quantum bit, suppose a two-dimensional Hilbert space. (For physical purposes a linear vector space endowed with a scalar product will be sufficient.) Let the superscript T indicate transposition, and let $|0\rangle \equiv (1, 0)^T$ and $|1\rangle \equiv (0, 1)^T$ be the orthogonal vector representations of the classical states associated with “falsity” and “truth,” or “0” and “1,” respectively.

From the varieties of properties featured by quantum information, one is of particular importance for quantum recursion theory: the ability to co-represent classically distinct, contradictory states of information via the generalized quantum bit state

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle \equiv \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}, \quad (1)$$

with the normalization $|\alpha_0|^2 + |\alpha_1|^2 = 1$. This feature is also known as *quantum parallelism*, alluding to the fact that n quantum bits can co-represent 2^n classical mutually exclusive states $\{|i_1 i_2 \cdots i_n\rangle \mid i_j \in \{0, 1\}, j = 1, \dots, n\}$ of n classical bits.

As will be argued below, recursion theoretic diagonalization can be symbolized by the diagonalization or “not” operator $\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, transforming $|0\rangle$ into $|1\rangle$, and vice versa. The eigensystem of the diagonalization operator \mathbf{X} is given by the two 50:50 mixtures of $|0\rangle$ and $|1\rangle$ with the two eigenvalues 1 and -1 ; i.e.,

$$\mathbf{X} \frac{1}{\sqrt{2}} (|0\rangle \pm |1\rangle) = \pm \frac{1}{\sqrt{2}} (|0\rangle \pm |1\rangle) = \pm |\psi_{\pm}\rangle. \quad (2)$$

In particular, the state $|\psi_{+}\rangle$ associated with the eigenvalue $+1$ is a *fixed point* of the operator \mathbf{X} .

Note that, provided that $|\psi\rangle \notin \{|0\rangle, |1\rangle\}$, a quantum bit is not in a pure classical state “relative to” the propositions corresponding to the projectors $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$. Any practical determination of the quantum bit amounts to a measurement of the state “along” one context [31] or base, such as the base “spanned” by $\{|0\rangle, |1\rangle\}$. Any such *single* measurement will be indeterministic (provided that the basis does not coincide with $\{|\psi_{+}\rangle, |\psi_{-}\rangle\}$); in particular, $|\langle\psi_{\pm}|0\rangle|^2 = |\langle\psi_{\pm}|1\rangle|^2 = 1/2$. That is, if the fixed point state and the measurement context mismatch, by Born’s postulate [32,33], the outcome of a *single* measurement occurs indeterministically, unpredictably and at random. Hence, in terms of the quantum states $|0\rangle$ and $|1\rangle$ corresponding to the classical states, the fixed point remains indeterminate.

In what follows it is argued that, due to the superposition principle, the quantum recursion theoretic diagonalization method has to be reformulated as a fixed point argument. Application of the diagonal operator \mathbf{X} yields no *reductio ad absurdum*. Instead, undecidability is recovered as a natural consequence of quantum coherence and of the unpredictability of certain quantum events.

3 Diagonalization

For comprehensive reviews of recursion theory and the diagonalization method the reader is referred to Refs. [1–6]. Therefore, only a few hallmarks will be stated. As already pointed out by Gödel in his classical paper on the incompleteness of arithmetic [34], the undecidability theorems of formal logic [2] are based on semantical paradoxes such as the liar [35] or Richard’s paradox. A proper translation of the semantic paradoxes into formal proofs results in the diagonalization method. Diagonalization has apparently first been applied by Cantor to demonstrate the undenumerability of real numbers [36]. It has also been used by Turing for a proof of the recursive undecidability of the halting problem [37].

A brief review of the classical algorithmic argument will be given first. Consider a universal computer C . For the sake of contradiction, consider an arbitrary algorithm $B(X)$ whose input is a string of symbols X . Assume that there exists a “halting algorithm” HALT which is able to decide whether B terminates on X or not. The domain of HALT is the set of legal programs. The range of HALT are classical bits (classical case) and quantum bits (quantum mechanical case).

Using $\text{HALT}(B(X))$ we shall construct another deterministic computing agent A , which has as input any effective program B and which proceeds as follows: Upon reading the program B as input, A makes a copy of it. This can be readily achieved, since the program B is presented to A in some encoded form $\ulcorner B \urcorner$, i.e., as a string of symbols. In the next step, the agent uses the code $\ulcorner B \urcorner$ as input string for B itself; i.e., A forms $B(\ulcorner B \urcorner)$, henceforth denoted by $B(B)$. The agent now hands $B(B)$ over to its subroutine HALT . Then, A proceeds as follows: if $\text{HALT}(B(B))$ decides that $B(B)$

halts, then the agent A does not halt; this can for instance be realized by an infinite DO-loop; if $\text{HALT}(B(B))$ decides that $B(B)$ does *not* halt, then A halts.

The agent A will now be confronted with the following paradoxical task: take the own code as input and proceed.

3.1 Classical case

Assume that A is restricted to classical bits of information. To be more specific, assume that HALT outputs the code of a classical bit as follows (\uparrow and \downarrow stands for divergence and convergence, respectively):

$$\text{HALT}(B(X)) = \begin{cases} |0\rangle & \text{if } B(X) \uparrow \\ |1\rangle & \text{if } B(X) \downarrow \end{cases}. \quad (3)$$

Then, whenever $A(A)$ halts, $\text{HALT}(A(A))$ outputs $|1\rangle$ and forces $A(A)$ not to halt. Conversely, whenever $A(A)$ does not halt, then $\text{HALT}(A(A))$ outputs $|0\rangle$ and steers $A(A)$ into the halting mode. In both cases one arrives at a complete contradiction. Classically, this contradiction can only be consistently avoided by assuming the non-existence of A and, since the only nontrivial feature of A is the use of the peculiar halting algorithm HALT , the impossibility of any such halting algorithm.

3.2 Quantum mechanical case

As has been argued above, in quantum information theory a quantum bit may be in a linear coherent superposition of the two classical states $|0\rangle$ and $|1\rangle$. Due to the superposition of classical bit states, the usual *reductio ad absurdum* argument breaks down. Instead, diagonalization procedures in quantum information theory yield quantum bit solutions which are fixed points of the associated unitary operators.

In what follows it will be demonstrated how the task of the agent A can be performed consistently if A is allowed to process quantum information. To be more specific, assume that the output of the hypothetical “halting algorithm” is a quantum bit

$$\text{HALT}(B(X)) = |\psi\rangle. \quad (4)$$

We may think of $\text{HALT}(B(X))$ as a universal computer C' simulating C' and containing a dedicated *halting bit*, which is the output of C' at every (discrete) time cycle. Initially (at time zero), this halting bit is prepared to be a 50:50 mixture of the classical halting and non-halting states $|0\rangle$ and $|1\rangle$ with equal phase; i.e., $|\psi_+\rangle$. If later C' finds that C converges (diverges) on $B(X)$, then the halting bit of C' is set to the “classical” values $|1\rangle$ or $|0\rangle$.

The emergence of fixed points can be demonstrated by a simple example. Agent A 's diagonalization task can be formalized as follows. Consider for the moment the action of diagonalization on the classical bit states. (Since the quantum bit states are merely a linear coherent superposition thereof, the action of diagonalization on quantum bits is straightforward.) Diagonalization effectively transforms the classical bit value $|0\rangle$

into $|1\rangle$ and *vice versa*. Recall that in equation (3), the state $|1\rangle$ has been identified with the halting state and the state $|0\rangle$ with the non-halting state.

The evolution representing diagonalization (effectively, agent A 's task) can be expressed by the unitary operator \mathbf{D} as

$$\mathbf{D}|0\rangle = |1\rangle \quad \text{and} \quad \mathbf{D}|1\rangle = |0\rangle. \quad (5)$$

Thus, \mathbf{D} acts essentially as a NOT-gate corresponding to the operator \mathbf{X} . In the above state basis, \mathbf{D} can be represented by

$$\mathbf{D} = \mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \quad (6)$$

\mathbf{D} will be called *diagonalization* operator, despite the fact that the only nonvanishing components are off-diagonal.

As has been pointed out earlier, quantum information theory allows a linear coherent superposition $|\psi\rangle$ of the “classical” bit states $|0\rangle$ and $|1\rangle$. \mathbf{D} has a fixed point at the quantum bit state

$$|\psi_+\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}. \quad (7)$$

$|\psi_+\rangle$ does not give rise to inconsistencies [38]. If agent A hands over the fixed point state $|\psi_+\rangle$ to the diagonalization operator \mathbf{D} , the same state $|\psi_+\rangle$ is recovered. Stated differently, as long as the output of the “halting algorithm” to input $A(A)$ is $|\psi_+\rangle$, i.e., $\text{HALT}(A(A)) = |\psi_+\rangle$, diagonalization does not change it. Hence, even if the (classically) “paradoxical” construction of diagonalization is maintained, quantum theory does not give rise to a paradox, because the quantum range of solutions is larger than the classical one. Therefore, standard proofs of the recursive unsolvability of the halting problem do not apply if agent A is allowed a quantum bit. The consequences for quantum recursion theory are discussed below.

4 Consequences for quantum recursion theory

Several critical remarks are in order. It should be noted that the fixed point quantum bit “solution” of the above halting problem is of not much practical help. In particular, if one is interested in the “classical” answer whether or not $A(A)$ halts, then one ultimately has to perform an irreversible measurement on the fixed point state. This causes a state reduction into the classical states corresponding to $|0\rangle$ and $|1\rangle$. Any single measurement will yield an indeterministic result. There is a 50:50 chance that the fixed point state will be either in $|0\rangle$ or $|1\rangle$, since as has been argued before, $|\langle\psi_+|0\rangle|^2 = |\langle\psi_+|1\rangle|^2 = 1/2$. Thereby, classical undecidability is recovered.

Thus, as far as problem solving is concerned, classical bits are not much of an advance. If a classical information is required, then quantum bits are not better than probabilistic knowledge. With regards to the question of whether or not a computer halts, the “solution” is effectively equivalent to the throwing of a fair coin [39]. Therefore, the advance of quantum recursion theory over classical recursion theory is not so much classical problem solving but *the consistent representation of statements* which would give rise to classical paradoxes.

The above argument used the continuity of quantum bit states as compared to the two discrete classical bit states for a construction of fixed points of the diagonalization operator. One could proceed a step further and allow *nonclassical diagonalization procedures*. Thereby, one could extend diagonalization to the entire range of two-dimensional unitary transformations [40], which need not have fixed points corresponding to eigenvalues of exactly one. Note that the general diagonal form of finite-dimensional unitary transformations in matrix notation is $\text{diag}(e^{i\varphi_1}, e^{i\varphi_2}, \dots, e^{i\varphi_n})$; i.e., the eigenvalues of a unitary operator are complex numbers of unit modulus (e.g., Ref. [41, p. 39], or Ref. [42, p. 161]). Fixed points only occur if at least one of the phases φ_i , $i \in \{1, 2, \dots, n\}$ is a multiple of 2π . In what follows, we shall study the physical realizability of general unitary operators associated with generalized beam splitters [43–46]. We will be particularly interested in those transformations whose spectra do not contain the eigenvalue one and thus do not allow a fixed point eigenvector.

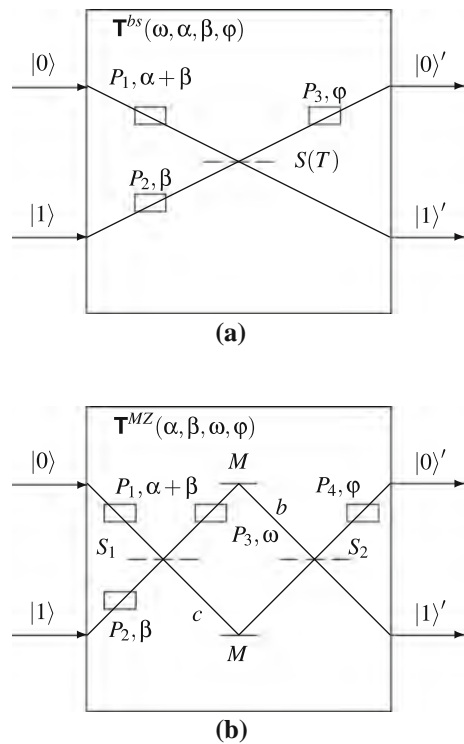
In what follows, lossless devices will be considered. In order to be able to realize a universal unitary transformation in two-dimensional Hilbert space, one needs to consider gates with two input and two output ports representing beam splitters and Mach-Zehnder interferometers equipped with an appropriate number of phase shifters. For the sake of demonstration, consider the two realizations depicted in Fig. 1. The elementary quantum interference device \mathbf{T}^{bs} in Fig. 1a is a unit consisting of two phase shifters P_1 and P_2 in the input ports, followed by a beam splitter S , which is followed by a phase shifter P_3 in one of the output ports. The device can be quantum mechanically represented by [47]

$$\begin{aligned} P_1 : |0\rangle &\rightarrow |0\rangle e^{i(\alpha+\beta)}, \\ P_2 : |1\rangle &\rightarrow |1\rangle e^{i\beta}, \\ S : |0\rangle &\rightarrow \sqrt{T}|1'\rangle + i\sqrt{R}|0'\rangle, \\ S : |1\rangle &\rightarrow \sqrt{T}|0'\rangle + i\sqrt{R}|1'\rangle, \\ P_3 : |0'\rangle &\rightarrow |0'\rangle e^{i\varphi}, \end{aligned} \quad (8)$$

where every reflection by a beam splitter S contributes a phase $\pi/2$ and thus a factor of $e^{i\pi/2} = i$ to the state evolution. Transmitted beams remain unchanged; i.e., there are no phase changes. Global phase shifts from mirror reflections are omitted. With $\sqrt{T(\omega)} = \cos \omega$ and $\sqrt{R(\omega)} = \sin \omega$, the corresponding unitary evolution matrix is given by

$$\mathbf{T}^{bs}(\omega, \alpha, \beta, \varphi) = \begin{pmatrix} ie^{i(\alpha+\beta+\varphi)} \sin \omega & e^{i(\beta+\varphi)} \cos \omega \\ e^{i(\alpha+\beta)} \cos \omega & ie^{i\beta} \sin \omega \end{pmatrix}. \quad (9)$$

Fig. 1 A universal quantum interference device operating on a qubit can be realized by a 4-port interferometer with two input ports $|0\rangle, |1\rangle$ and two output ports $|0'\rangle, |1'\rangle$; **a** realization by a single beam splitter $S(T)$ with variable transmission T and three phase shifters P_1, P_2, P_3 ; **b** realization by two 50:50 beam splitters S_1 and S_2 and four phase shifters P_1, P_2, P_3, P_4



Alternatively, the action of a lossless beam splitter may be described by the matrix¹

$$\begin{pmatrix} i\sqrt{R(\omega)} & \sqrt{T(\omega)} \\ \sqrt{T(\omega)} & i\sqrt{R(\omega)} \end{pmatrix} = \begin{pmatrix} i \sin \omega & \cos \omega \\ \cos \omega & i \sin \omega \end{pmatrix}.$$

A phase shifter in two-dimensional Hilbert space is represented by either $\text{diag}(e^{i\varphi}, 1)$ or $\text{diag}(1, e^{i\varphi})$. The action of the entire device consisting of such elements is calculated by multiplying the matrices in reverse order in which the quanta pass these elements [48,49]; i.e.,

$$\mathbf{T}^{bs}(\omega, \alpha, \beta, \varphi) = \begin{pmatrix} e^{i\varphi} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} i \sin \omega & \cos \omega \\ \cos \omega & i \sin \omega \end{pmatrix} \begin{pmatrix} e^{i(\alpha+\beta)} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\beta} \end{pmatrix}. \quad (10)$$

The elementary quantum interference device \mathbf{T}^{MZ} depicted in Fig. 1b is a Mach-Zehnder interferometer with two input and output ports and four phase shifters. The process can be quantum mechanically described by

¹ The standard labeling of the input and output ports are interchanged, therefore sine and cosine are exchanged in the transition matrix.

$$\begin{aligned}
P_1 : |0\rangle &\rightarrow |0\rangle e^{i(\alpha+\beta)}, \\
P_2 : |1\rangle &\rightarrow |1\rangle e^{i\beta}, \\
S_1 : |1\rangle &\rightarrow (|b\rangle + i|c\rangle)/\sqrt{2}, \\
S_1 : |0\rangle &\rightarrow (|c\rangle + i|b\rangle)/\sqrt{2}, \\
P_3 : |b\rangle &\rightarrow |b\rangle e^{i\omega}, \\
S_2 : |b\rangle &\rightarrow (|1'\rangle + i|0'\rangle)/\sqrt{2}, \\
S_2 : |c\rangle &\rightarrow (|0'\rangle + i|1'\rangle)/\sqrt{2}, \\
P_4 : |0'\rangle &\rightarrow |0'\rangle e^{i\varphi}.
\end{aligned} \tag{11}$$

The corresponding unitary evolution matrix is given by

$$\mathbf{T}^{MZ}(\alpha, \beta, \omega, \varphi) = i e^{i(\beta+\frac{\omega}{2})} \begin{pmatrix} -e^{i(\alpha+\varphi)} \sin \frac{\omega}{2} & e^{i\varphi} \cos \frac{\omega}{2} \\ e^{i\alpha} \cos \frac{\omega}{2} & \sin \frac{\omega}{2} \end{pmatrix}. \tag{12}$$

Alternatively, \mathbf{T}^{MZ} can be computed by matrix multiplication; i.e.,

$$\begin{aligned}
\mathbf{T}^{MZ}(\alpha, \beta, \omega, \varphi) &= i e^{i(\beta+\frac{\omega}{2})} \begin{pmatrix} e^{i\varphi} & 0 \\ 0 & 1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix} \begin{pmatrix} e^{i\omega} & 0 \\ 0 & 1 \end{pmatrix} \\
&\times \frac{1}{\sqrt{2}} \begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix} \begin{pmatrix} e^{i(\alpha+\beta)} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\beta} \end{pmatrix}.
\end{aligned} \tag{13}$$

Both elementary quantum interference devices \mathbf{T}^{bs} and \mathbf{T}^{MZ} are universal in the sense that every unitary quantum evolution operator in two-dimensional Hilbert space

$$\mathbf{U}_2(\omega, \alpha, \beta, \varphi) = e^{-i\beta} \begin{pmatrix} e^{i\alpha} \cos \omega & -e^{-i\varphi} \sin \omega \\ e^{i\varphi} \sin \omega & e^{-i\alpha} \cos \omega \end{pmatrix}, \tag{14}$$

where $-\pi \leq \beta, \omega \leq \pi$, $-\frac{\pi}{2} \leq \alpha, \varphi \leq \frac{\pi}{2}$ [40] corresponds to $\mathbf{T}^{bs}(\omega', \alpha', \beta', \varphi')$ and $\mathbf{T}^{MZ}(\omega'', \alpha'', \beta'', \varphi'')$, where $\omega, \alpha, \beta, \varphi$ are arguments of the (double) primed parameters [46].

A typical example of a nonclassical operation on a quantum bit is the “square root of not” gate ($\sqrt{\text{not}}\sqrt{\text{not}} = \mathbf{X}$)

$$\sqrt{\text{not}} = \frac{1}{2} \begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}. \tag{15}$$

Although $\sqrt{\text{not}}$ still has a eigenstate associated with a fixed point of unit eigenvalue, not all of these unitary transformations have eigenvectors associated with eigenvalues one that can be identified with fixed points. Indeed, only unitary transformations of the form

$$\begin{aligned}
&[\mathbf{U}_2(\omega, \alpha, \beta, \varphi)]^{-1} \text{diag}(1, e^{i\lambda}) \mathbf{U}_2(\omega, \alpha, \beta, \varphi) \\
&= \begin{pmatrix} \cos \omega^2 + e^{i\lambda} \sin \omega^2 & \frac{-1+e^{i\lambda}}{2} e^{-i(\alpha+\varphi)} \sin(2\omega) \\ \frac{-1+e^{i\lambda}}{2} e^{i(\alpha+\varphi)} \sin(2\omega) & e^{i\lambda} \cos \omega^2 + \sin \omega^2 \end{pmatrix}
\end{aligned} \tag{16}$$

have fixed points.

Applying nonclassical operations on quantum bits with no fixed points

$$\begin{aligned} \mathbf{D}^* &= [\mathbf{U}_2(\omega, \alpha, \beta, \varphi)]^{-1} \text{diag}(e^{i\mu}, e^{i\lambda}) \mathbf{U}_2(\omega, \alpha, \beta, \varphi) \\ &= \begin{pmatrix} e^{i\mu} \cos(\omega)^2 + e^{i\lambda} \sin(\omega)^2 & \frac{e^{-i(\alpha+p)}}{2} (e^{i\lambda} - e^{i\mu}) \sin(2\omega) \\ \frac{e^{i(\alpha+p)}}{2} (e^{i\lambda} - e^{i\mu}) \sin(2\omega) & e^{i\lambda} \cos(\omega)^2 + e^{i\mu} \sin(\omega)^2 \end{pmatrix}, \end{aligned} \quad (17)$$

with $\mu, \lambda \neq 2n\pi$, $n \in \mathbb{N}_0$ gives rise to eigenvectors which are not fixed points, but which acquire nonvanishing phases μ, λ in the generalized diagonalization process.

5 Summary

It has been argued that, because of quantum parallelism, i.e., the effective co-representation of classical mutually exclusive states, the diagonalization method of classical recursion theory has to be modified. Quantum diagonalization involves unitary operators whose eigenvalues carry phases strictly different from multiples of 2π . The quantum fixed point “solutions” of halting problems can be 50:50 mixtures of the classical halting and nonhalting states, and therefore do not contribute to classical deterministic solutions of the associated decision problems.

Another, less abstract, application for quantum information theory is the handling of inconsistent information in databases. Thereby, two contradicting classical bits of information $|0\rangle$ and $|1\rangle$ are resolved, i.e., co-represented, by the quantum bit $|\psi_+\rangle$. Throughout the rest of the computation the coherence is maintained. After the processing, the result is obtained by an irreversible measurement. The processing of quantum bits, however, would require an exponential space overhead on classical computers in classical bit base [10]. Thus, in order to remain tractable, the corresponding quantum bits should be implemented on truly quantum universal computers.

References

1. Rogers, H. Jr.: Theory of Recursive Functions and Effective Computability. MacGraw-Hill, New York (1967)
2. Davis, M.: The Undecidable. Basic Papers on Undecidable, Unsolvable Problems and Computable Functions. Raven Press, Hewlett (1965)
3. Barwise, J.: Handbook of Mathematical Logic. North-Holland, Amsterdam (1978)
4. Enderton, H.: A Mathematical Introduction to Logic, 2nd edn. Academic Press, San Diego (2001)
5. Odifreddi, P.: Classical Recursion Theory, vol 1. North-Holland, Amsterdam (1989)
6. Boolos, G.S., Burgess, J.P., Jeffrey, R.C.: Computability and Logic, 5th edn. Cambridge University Press, Cambridge (2007)
7. Landauer, R.: Information is physical. Phys. Today **44**, 23–29. <http://dx.doi.org/10.1063/1.881299> (1991)
8. Bridgman, P.W.: A physicist's second reaction to Mengenlehre. Scripta Mathematica **2**, 101–117, 224–234, cf. R. Landauer [50] (1934)
9. Olszewski, A., Woleński, J., Janusz, R.: Church's Thesis After 70 Years. Ontos, Berlin (2006)
10. Feynman, R.P.: Simulating physics with computers. Int. J. Theo. Phys. **21**, 467–488 (1982)
11. Fredkin, E., Toffoli, T.: Conservative logic. Int. J. Theo. Phys. **21**, 219–253, reprinted in [51, part I, Chap. 3]. <http://dx.doi.org/10.1007/BF01857727> (1982)
12. Leff, H.S., Rex, A.F.: Maxwells Demon. Princeton University Press, Princeton (1990)

13. Feynman, R.P.: The Feynman lectures on computation. In: Hey, A.J.G., Allen, R.W. (eds.) Addison-Wesley Publishing Company, Reading (1996)
14. Birkhoff, G., von Neumann, J.: The logic of quantum mechanics. *Ann. Math.* **37**, 823–843 (1936)
15. Kochen, S., Specker, E.P.: Logical structures arising in quantum theory. In: Symposium on the Theory of Models. Proceedings of the 1963 International Symposium at Berkeley, pp. 177–189, reprinted in [52, pp. 209–221] (1965)
16. Kochen, S., Specker, E.P.: The calculus of partial propositional functions. In: Proceedings of the 1964 International Congress for Logic, Methodology and Philosophy of Science, Jerusalem, pp. 45–57, reprinted in [52, pp. 222–234] (1965)
17. Foulis, D.J., Piron, C., Randall, C.H.: Realism, operationalism, and quantum mechanics. *Found. Phys.* **13**, 813–841, invited papers dedicated to Günther Ludwig. <http://dx.doi.org/10.1007/BF01906271> (1983)
18. Randall, C.H., Foulis, D.J.: Properties and operational propositions in quantum mechanics. *Found. Phys.* **13**, 843–857, invited papers dedicated to Günther Ludwig. <http://dx.doi.org/10.1007/BF01906272> (1983)
19. Bournez, O., Campagnolo, M.L.: A survey on continuous time computations. In: Cooper, S., Löwe, B., Sorbi, A. (eds.) *New Computational Paradigms. Changing Conceptions of What is Computable*. Springer, New York, pp. 383–423. <http://www.lix.polytechnique.fr/~bournez/pmwiki/uploads/Main/SurveyContinuousTime.pdf> (2008)
20. Deutsch, D.: Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer. Proceedings of the royal society of London. *Math. Phys. Sci. A (1934–1990)* **400**, 97–117. <http://dx.doi.org/10.1098/rspa.1985.0070> (1985)
21. Gruska, J.: *Quantum Computing*. McGraw-Hill, London (1999)
22. Nielsen, M.A., Chuang, I.L.: *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge (2000)
23. Lo, H.-K., Popescu, S., Spiller, T.: *Introduction to Quantum Computation and Information*. World Scientific Publishing Company, Singapore (2001)
24. Brylinski, R.K., Chen, G., Brylinski, B.K.: *Mathematics of Quantum Computation*. Chapman & Hall/CRC Press, London (2002)
25. Hayashi, M.: *Quantum Information. An Introduction*. Springer, Berlin (2006)
26. Imai, H., Hayashi, M.: *Quantum Computation and Information. From Theory to Experiment*. Springer, Berlin (2006)
27. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dusek, M., Lütkenhaus, N., Peev, M.: The security of practical quantum key distribution. <http://arxiv.org/abs/0802.4155> (2008)
28. Jaeger, G.: *Quantum Information an Overview*. Springer, New York (2007)
29. Mermin, N.D.: *Quantum Computer Science*. Cambridge University Press, Cambridge <http://people.ccmr.cornell.edu/~mermin/qcomp/CS483.html> (2007)
30. Mermin, N.D.: From Cbits to Qbits: Teaching computer scientists quantum mechanics. *Am. J. Phys.* **71**, 23–30. <http://dx.doi.org/10.1119/1.1522741> (2003)
31. Svozil, K.: Contexts in quantum, classical and partition logic. In: Engesser, K., Gabbay, D.M., Lehmann, D. (eds.) *Handbook of Quantum Logic and Quantum Structures*, pp. 551–586. Elsevier, Amsterdam. <http://arxiv.org/abs/quant-ph/0609209> (2008)
32. Born, M.: Zur Quantenmechanik der Stoßvorgänge. *Zeitschrift für Physik* **37**, 863–867. <http://dx.doi.org/10.1007/BF01397477> (1926)
33. Zeilinger, A.: The message of the quantum. *Nature* **438**, 743. <http://dx.doi.org/10.1038/438743a> (2005)
34. Gödel, K.: Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme. *Monatshefte für Mathematik und Physik* **38**, 173–198, English translation in [53], and in [2] (1931)
35. Anderson A.R.: St. Paul's epistle to Titus. In: Martin, R.L. (ed.) *The Paradox of the Liar*. Yale University Press, New Haven. The Bible contains a passage which refers to Epimenides, a Crete living in the capital city of Cnossus: "One of themselves, a prophet of their own, said, 'Cretans are always liars, evil beasts, lazy gluttons.'",—St. Paul, Epistle to Titus I (12–13) (1970)
36. Cantor, G.: *Abhandlungen*. Springer, Berlin (1932)
37. Turing, A.M.: On computable numbers, with an application to the Entscheidungsproblem. Proceedings of the London mathematical society, series 2. **42** and **43**, 230–265 and 544–546, reprinted in [2] (1936)
38. Svozil, K.: Consistent use of paradoxes in deriving constraints on the dynamics of physical systems and of no-go-theorems. *Found. Phys. Lett.* **8**, 523–535 (1995)

39. Diaconis, P., Holmes, S., Montgomery, R.: Dynamical bias in the coin toss. *SIAM Rev.* **49**, 211–235. <http://dx.doi.org/10.1137/S0036144504446436> (2007)
40. Murnaghan, F.D.: *The Unitary and Rotation Groups*. Spartan Books, Washington, DC (1962)
41. Shankar R.: *Principles of Quantum Mechanics*, 2nd edn. Kluwer Academic/Plenum Publishers, New York (1994)
42. Halmos, P.R.: *Finite-dimensional Vector Spaces*. Springer, New York (1974)
43. Reck M., Zeilinger A., Bernstein H.J., Bertani P.: Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.* **73**, 58–61. <http://dx.doi.org/10.1103/PhysRevLett.73.58> (1994)
44. Reck, M., Zeilinger, A.: Quantum phase tracing of correlated photons in optical multiports. In: Martini, F.D., Denardo, G., Zeilinger, A., (eds.) *Quantum Interferometry*, pp. 170–177 (1994)
45. Zukowski, M., Zeilinger, A., Horne, M.A.: Realizable higher-dimensional two-particle entanglements via multiport beam splitters. *Phys. Rev. A* **55**, 2564–2579. <http://dx.doi.org/10.1103/PhysRevA.55.2564> (1997)
46. Svozil, K. Noncontextuality in multipartite entanglement. *J. Phys. A Math. Gen.* **38**, 5781–5798. <http://dx.doi.org/10.1088/0305-4470/38/25/013> (2005)
47. Greenberger, D.M., Horne, M.A., Zeilinger, A.: Multiparticle interferometry and the superposition principle. *Phys. Today* **46**, 22–29 (1993)
48. Yurke, B., McCall, S.L., Klauder, J.R.: SU(2) and SU(1,1) interferometers. *Phys. Rev. A* **33**, 4033–4054. <http://dx.doi.org/10.1103/PhysRevA.33.4033> (1986)
49. Campos, R.A., Saleh, B.E.A., Teich, M.C.: Fourth-order interference of joint single-photon wave packets in lossless optical systems. *Phys. Rev. A* **42**, 4127–4137. <http://dx.doi.org/10.1103/PhysRevA.42.4127> (1990)
50. Landauer, R.: Advertisement for a paper I like. In: Casti, J.L., Traub, J.F. (eds.) *On limits*. Santa Fe Institute Report 94-10-056, Santa Fe, NM, p. 39. <http://www.santafe.edu/research/publications/workingpapers/94-10-056.pdf> (1994)
51. Adamatzky, A.: *Collision-based Computing*. Springer, London (2002)
52. Specker, E.: *Selecta*. Birkhäuser Verlag, Basel (1990)
53. Gödel, K. In: Feferman, S., Dawson, J.W., Kleene, S.C., Moore, G.H., Solovay, R.M., van Heijenoort, J. (eds.). *Collected Works*. Publications 1929–1936, vol I. Oxford University Press, Oxford (1986)

Three criteria for quantum random-number generators based on beam splitters

Karl Svozil*

Institute for Theoretical Physics, Vienna University of Technology, Wiedner Hauptstraße 8-10/136, A-1040 Vienna, Austria

(Received 16 March 2009; published 15 May 2009)

We propose three criteria for the generation of random digital strings from quantum beam splitters: (i) three or more mutually exclusive outcomes corresponding to the invocation of three- and higher-dimensional Hilbert spaces, (ii) the mandatory use of pure states in conjugated bases for preparation and detection, and (iii) the use of entangled singlet (unique) states for elimination of bias.

DOI: [10.1103/PhysRevA.79.054306](https://doi.org/10.1103/PhysRevA.79.054306)

PACS number(s): 03.67.Hk, 03.65.Ud, 05.40.—a

Quantum random-number generators are important for quantum-information processing as they are likely to be one of the first technologies applied for various physical and commercial applications. They also serve as components of other quantum devices for quantum key distribution and experiments testing and utilizing quantum nonlocality.

Randomness is a notorious property, both from theoretical and practical points of view. It is commonly accepted that there is a satisfactory definition [1] of *infinite* random sequences in terms of algorithmic incompressibility [2] as well as of the equivalent statistical tests [3]. Besides the obvious fact that all computable and physically operational entities are limited to *finite* objects and methods, algorithmic pseudorandom generators suffer from von Neumann's verdict that [4] "*anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin.*" The halting probability Ω [5] shares three perplexing properties: it is computably enumerable (computable in a weak sense), provable random (which implies that Ω is noncomputable), as well as infinitely knowledgeable in its role as a "rosetta stone" for all decision problems encodable as halting problems [1]. A few of its starting bits have been computed [6], yet due to its randomness only finitely many bits of this number can ever be computed.

From the numerous random-number generators based on physical processes (cf. Refs. [7–12] to name a few), the use of single photons (or other quanta such as neutrons) subjected to beam splitters appears particularly promising [13–16] for the following reasons: (i) due to (ideally) single-photon events, the physical systems are "elementary;" (ii) they can be controlled to a great degree; and (iii) they can be certified to be random relative to the postulates of quantum theory [17].

Three features of quantum theory directly relate to random sequences generated from beam splitter experiments: (i) the randomness of individual events (cf. Ref. [18], p. 866 and Ref. [19], p. 804); (ii) complementarity ([20], p. 7); and (iii) value indefiniteness, i.e., the absence of two-valued states interpretable as "global" (i.e., valid on all observables) truth functions [21]. In order to fully implement these quantum features, we propose three improvements to existing protocols [13–16, 22–24].

The first criterion ensures that the quantum random-

number generators can be certified to be subjected to quantum value indefiniteness. A necessary condition for this to apply is the possibility of *three or more mutually exclusive outcomes* in measurements of single quanta. Formally, this is due to the fact that violations of Bell-type inequalities, as well as proofs of Gleason's and Kochen-Specker-type theorems are only realizable [25] in three- and higher-dimensional Hilbert spaces. Only from three-dimensional vector space onward it is possible to nontrivially interconnect bases through one (or up to $n-2$ for n -dimensional Hilbert space) common base element(s). This can be explicitly demonstrated by certain, even dense [26–28], "dilutions" of bases, which break up the possibility to interconnect, thus allowing value definiteness. In more operational terms, if some "exotic" scenarios (e.g., Refs. [29,30]) are excluded, the violation of Bell-type inequalities for two two-state particles (corresponding to two outcomes on each side) is a sufficient criterion for quantum value indefiniteness.

Of course, one could argue that protocols based on two outcomes are still protected by quantum complementarity, and the full range of quantum indeterminism, in particular quantum value indefiniteness, is not needed. There is also the possibility that the Born rule might be derived through some other argument (possibly from another set of axioms) than Gleason's theorem [31–34]. However, there exist sufficiently many two-valued states on propositional structures with two outcomes to allow for a homeomorphic embedding of this structure into a classical Boolean algebra. In any case, it appears prudent to use all the "mind-boggling" features of quantum mechanics against cryptanalytic attacks on some quantum-generated sequence.

The resulting trivalent or multivalued sequence can be easily "downgraded" or "translated" to binary sequences through elimination or identification without loss of randomness: systematically eliminating $n-2$ symbol(s) will transform a random sequence on an alphabet with $n \geq 3$ symbols into a random sequence on an alphabet with two symbols [1].

The second criterion proposes the mandatory use of *pure* states from maximally conjugated bases for preparation and detection. This requirement deals with the *single-particle source* of quantum random-number generators. Indeed, many two-particle experiments have been using this criterion already, as full tomography is performed to characterize the state as completely as possible. These experiments use a (Bell) state which is as pure and maximally entangled as operationally feasible; quite often they produce the singlet Bell state (which, due to technical issues related to other

*svozil@tuwien.ac.at; <http://tph.tuwien.ac.at/~svozil>

degrees of freedom, can never be ideally pure). Tomography is used to characterize the state and hence certify the randomness of outcomes. Hence in this sense and in these experiments, the criterion is already implicitly implemented.

Although it is generally believed that mixed (nonpure) quantum states can be “produced” and operationalized “for all practical purposes,” one might cautiously argue that this may actually be a subjective statement on behalf of the observer: whereas the experimenter might “pretend” that the exact state leaving the particle source is unknown, it might still be possible to conceive of the state to be in some, albeit unknown but not principally unknowable, unique pure state. This is related to the question of whether or not mixed states should be thought of as merely subjective constructions which even in the epistemic view—as the wave function (the quantum state) representing a catalog of expectations [35]—represent only certain partial incomplete representations of systems which might be completely defined by a single unique context.

Even if one is unwilling to accept these principal concerns, it remains prudent not to expose the protocols for generating quantum randomness to the possibility of hidden regularities of the source. After all, beam splitters are just one-to-one bijective devices representable by reversible unitary operators [36–38]—a fact which can be seen by recombining the two paths by a second beam splitter in a Mach-Zender interferometer, thereby recovering the original signal. Thus, in order to assure quantum randomness, the beam splitter should not be considered as an isolated element but has to be examined in combination with the source. In accordance with this principle, a *mismatch* between state preparation and measurement guarantees that quantum complementarity ensures the indeterministic outcome. This can, for instance, be implemented by preparing the single particle in a pure state which corresponds to an element of a certain basis and then measuring it in a different basis, in which the original state is in a coherent superposition of more than one states (cf. Ref. [13] and the first protocol using beam splitting polarizers in Ref. [15]).

Third and finally, in order to eliminate any possible bias (for some “classical” methods to eliminate bias, we refer to Refs. [39–42]), we propose to utilize Einstein-Podolsky-Rosen-type measurements of two quanta in a unique entangled state. Any state satisfying the uniqueness property [43] in at least two directions, such as the singlet states $\frac{1}{\sqrt{2}}(|\frac{1}{2}, -\frac{1}{2}\rangle - |-\frac{1}{2}, \frac{1}{2}\rangle)$, $\frac{1}{\sqrt{3}}(-|0, 0\rangle + |-1, 1\rangle + |1, -1\rangle)$, or $\frac{1}{2}(|\frac{3}{2}, -\frac{3}{2}\rangle - |\frac{3}{2}, \frac{3}{2}\rangle - |\frac{1}{2}, -\frac{1}{2}\rangle + |-\frac{1}{2}, \frac{1}{2}\rangle)$ of two spin- $\frac{1}{2}$, -1, or $-\frac{3}{2}$ particles could be used for this purpose. In that way, the outcome of

one particle can be combined with the outcome of the other particle to eliminate bias. Again, it should be kept in mind that physical realizations of this protocol can never be made ideal and necessarily suffer from, for instance, the nonideal behavior of the beam splitters.

For the sake of demonstration, suppose Alice and Bob share successive pairs of quanta in the singlet Bell state $\frac{1}{\sqrt{2}}(|\frac{1}{2}, -\frac{1}{2}\rangle - |-\frac{1}{2}, \frac{1}{2}\rangle)$. Denote Alice’s and Bob’s outcomes in the j th measurement by a_j and b_j , with the coding $a_j, b_j \in \{0, 1\}$, respectively. Using XOR operations on their combined results by a product mod 2 of a_j and b_j , i.e., by defining $s_j = a_j \oplus b_j = a_j b_j \bmod 2$, yields a totally unbiased sequence s_j of bits. Remarkably, as the state guarantees a 50:50 occurrence of 0’s and 1’s on either side, the associated bases of Alice and Bob need not even be maximally “apart:” one outcome on Alice’s side can be thought of as serving as “one-time pad” in encrypting the other outcome on Bob’s side, and vice versa. Again, this method will be as good as the entangled particle source. In order to eliminate causal influences, the events recorded by Alice and Bob should be separated by strict Einstein locality conditions [44,45], although separating the particles will be experimentally challenging.

Alternatively, in an adaptive “delayed choice” experiment the outcome on Alice’s side could be transferred to Bob, who adjusts his experiment (e.g., by changing the direction of spin-state measurements) according to Alice’s input [46]. This method resembles the previously implemented self-calibration techniques utilizing coincidence measurements [22], entropy measures [24], and iterative sampling [23]. Whether or not it could also be used for classical angular-momentum zero states “exploding” into two parts [47] remains unknown.

In summary we have argued that the present protocols for generating quantum random sequences with beam splitters should be improved to be certifiable against value definiteness and hidden bias of the source. We have also proposed a procedure to eliminate bias by using one particle of a singlet in an Einstein-Podolsky-Rosen configuration as a one-time pad for the other particle.

The author gratefully acknowledges discussions with and suggestions by Cristian Calude, as well as the kind hospitality of the Centre for Discrete Mathematics and Theoretical Computer Science (CDMTCS) of the Department of Computer Science at The University of Auckland. This work was also supported by The Department for International Relations of the Vienna University of Technology.

-
- [1] C. Calude, *Information and Randomness—An Algorithmic Perspective*, 2nd ed. (Springer, Berlin, 2002).
 [2] G. J. Chaitin, IBM J. Res. Dev. **21**, 350 (1977); *Information, Randomness and Incompleteness*, 2nd ed. (World Scientific, Singapore, 1990).
 [3] P. Martin-Löf, Inf. Control. **9**, 602 (1966).

- [4] J. von Neumann, in *John von Neumann, Collected Works*, edited by A. H. Traub (MacMillan, New York, 1963), Vol. V, p. 768.
 [5] G. J. Chaitin, *Exploring Randomness* (Springer Verlag, London, 2001).
 [6] C. S. Calude and M. J. Dinneen, Int. J. Bifurcation Chaos **17**,

- 1937 (2007).
- [7] The RAND Corporation, Knolls Atomic Power Laboratory Report No. KAPL-3147, 1955 (unpublished). The data digits are obtainable via http://www.rand.org/pubs/monograph_reports/2005/digits.txt.zip, the introduction via http://www.rand.org/pubs/monograph_reports/MR1418/index2.html, http://www.rand.org/pubs/monograph_reports/MR1418/.
 - [8] C. H. Vincent, J. Phys. E **3**, 594 (1970).
 - [9] T. Erber and S. Putterman, Nature (London) **318**, 41 (1985).
 - [10] H. Schmidt, J. Appl. Phys. **41**, 462 (1970).
 - [11] A. J. Martino and G. M. Morris, Appl. Opt. **30**, 981 (1991).
 - [12] J. Walker, *Hotbits Hardware* (1986–2009), <http://www.fourmilab.ch/hotbits/hardware3.html>
 - [13] K. Svozil, Phys. Lett. A **143**, 433 (1990).
 - [14] J. G. Rarity, M. P. C. Owens, and P. R. Tapster, J. Mod. Opt. **41**, 2435 (1994).
 - [15] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, Rev. Sci. Instrum. **71**, 1675 (2000).
 - [16] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, J. Mod. Opt. **47**, 595 (2000).
 - [17] A. Zeilinger, Nature (London) **438**, 743 (2005).
 - [18] M. Born, Z. Phys. **37**, 863 (1926).
 - [19] M. Born, Z. Phys. **38**, 803 (1926).
 - [20] W. Pauli, in *Handbuch der Physik, Band V, Teil I, Prinzipien der Quantentheorie I*, edited by S. Flügge (Springer, Berlin, 1958), pp. 1–168.
 - [21] S. Kochen and E. P. Specker, J. Math. Mech. **17**, 59 (1967); reprinted in works of E. Specker, *Selecta* (Birkhäuser Verlag, Basel, 1990), pp. 235–263.
 - [22] M. Hai-Qiang, W. Su-Mei, Z. Da, C. Jun-Tao, J. Ling-Ling, H. Yan-Xue, and W. Ling-An, Chin. Phys. Lett. **21**, 1961 (2004).
 - [23] P. X. Wang, G. L. Long, and Y. S. Li, J. Appl. Phys. **100**, 056107 (2006).
 - [24] M. Fiorentino, C. Santori, S. M. Spillane, R. G. Beausoleil, and W. J. Munro, Phys. Rev. A **75**, 032334 (2007).
 - [25] K. Svozil and J. Tkadlec, J. Math. Phys. **37**, 5380 (1996).
 - [26] C. D. Godsil and J. Zaks, University of Waterloo Research Report No. CORR 88-12, 1988 (unpublished).
 - [27] D. A. Meyer, Phys. Rev. Lett. **83**, 3751 (1999).
 - [28] H. Havlicek, G. Krenn, J. Summhammer, and K. Svozil, J. Phys. A **34**, 3071 (2001).
 - [29] I. Pitowsky, Phys. Rev. Lett. **48**, 1299 (1982).
 - [30] I. Pitowsky, Phys. Rev. D **27**, 2316 (1983).
 - [31] A. M. Gleason, J. Math. Mech. **6**, 885 (1957).
 - [32] I. Pitowsky, J. Math. Phys. **39**, 218 (1998).
 - [33] F. Richman and D. Bridges, J. Funct. Anal. **162**, 287 (1999).
 - [34] A. Dvurečenskij, *Gleason's Theorem and Its Applications* (Kluwer Academic Publishers, Dordrecht, 1993).
 - [35] E. Schrödinger, Naturwiss. **23**, 807 (1935); translated in English by J. D. Trimmer, Proc. Am. Philos. Soc. **124**, 323 (1980); <http://www.tu-harburg.de/rzt/rzt/it/QM/cat.html>; reprinted in works of J. A. Wheeler and W. H. Zurek, *Quantum Theory and Measurement* (Princeton University Press, Princeton, NJ, 1983), pp. 152–167.
 - [36] Z. Ou, C. Hong, and L. Mandel, Opt. Commun. **63**, 118 (1987).
 - [37] D. M. Greenberger, M. A. Horne, and A. Zeilinger, Phys. Today **46**(8), 22 (1993).
 - [38] A. Zeilinger, Am. J. Phys. **49**, 882 (1981).
 - [39] P. Elias, Ann. Math. Stat. **43**, 865 (1972).
 - [40] Y. Peres, Ann. Stat. **20**, 590 (1992); <http://www.jstor.org/stable/2242181>
 - [41] M. Dichtl, in *Fast Software Encryption*, Lecture Notes in Computer Science Vol. 4593, edited by A. Biryukov (Springer, Berlin, 2007), pp. 137–152.
 - [42] P. Lacharme, in *Fast Software Encryption*, Lecture Notes in Computer Science Vol. 5086, edited by K. Nyberg (Springer, Berlin, 2008), pp. 334–342.
 - [43] K. Svozil, New J. Phys. **8**, 39 (2006); J. Phys. A **38**, 5781 (2005).
 - [44] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **81**, 5039 (1998).
 - [45] T. Scheidl, R. Ursin, J. Kofler, S. Ramelow, X. Ma, T. Herbst, L. Ratschbacher, A. Fedrizzi, N. Langford, T. Jennewein, and A. Zeilinger, e-print arXiv:0811.3129.
 - [46] V. Jacques, E. Wu, F. Grosshans, F. Treussart, P. Grangier, A. Aspect, and J.-F. Roch, Science **315**, 966 (2007).
 - [47] A. Peres, Am. J. Phys. **46**, 745 (1978).



Quantum Randomness and Value Indefiniteness

Cristian S. Calude^{1,*†} and Karl Svozil²

¹Department of Computer Science, The University of Auckland, Private Bag 92019, Auckland, New Zealand

²Institute for Theoretical Physics, University of Technology Vienna, Wiedner Hauptstraße 8-10/136, A-1040 Vienna, Austria

As computability implies value definiteness, certain sequences of quantum outcomes cannot be computable.

Delivered by Ingenta to:
Vienna University of Technology
IP: 128.131.48.164
Wed, 29 Apr 2009 11:43:05

1. CONCEPTUALISATION

It certainly would be fascinating to pinpoint the time of the emergence of the notion that certain quantum processes, such as the decay of an excited quantum state, occurs principally and irreducibly at random; and how long it took to become the dominant way of thinking about them after almost two centuries of quasi-rationalistic dominance. Bohr's and Heisenberg's influence has been highly recognised and has prevailed, even against the strong rationalistic and philosophic objections raised by, for instance, by Einstein and Schrödinger.^{1,2} Of course, one of the strongest reasons for this growing acceptance of quantum randomness has been the factual inability to go "beyond" the quantum in any manner which would encourage new phenomenology and might result in any hope for a progressive quasi-classical research program.³

Here we intend to discuss quantum randomness and its connection with quantum value indefiniteness. Bell,⁴⁻⁷ Kochen and Specker (KS),⁸ as well as Greenberger, Horne and Zeilinger (GHZ)⁹⁻¹¹ contributed to the evidence that the mere concept of coexistence of certain elements of physical reality¹² results in a complete contradiction. In this view, speculations about the "reasons" for certain outcomes of experiments are necessarily doomed; just because of the simple fact that any such rational reason is provably (by contradiction) impossible.

An attempt is made here to clearly spell out the issues and problems involved in considering randomness, both with regard to the occurrence of single events, as well as their combination into time series. We wish to state from the beginning that we attempt to have no bias or preference for or against randomness. While to us it seems obvious that any claim of non-randomness has to be confronted with the factual inability to produce any satisfactory theory that goes beyond the quantum, especially in view of the known no-go theorems by Bell, KS and GHZ and others referred to above, it is also advisable to keep all options open and carefully study the types of randomness involved, and their possible "origins," if any.

Usually, the random outcome of certain quantum physical events seems to be axiomatically postulated from the onset; an assumption which can be also based on elementary principles.^{13,14} Here we argue that actually we can go further and infer some properties of quantum randomness—including the absence of effective global correlations—from the impossibility of value definiteness of certain quantum mechanical observables.

1.1. Difficulties

Consider, as two extreme cases, the binary expansion $\pi_1\pi_2\pi_3\dots\pi_i\pi_{i+1}\dots$ of pi, an ideal circle's ratio of the circumference to its diameter, starting from, say, the 571113th billion prime number place onwards, and compare it to a sequence generated by quantum coin tosses $x_1x_2x_3\dots x_ix_{i+1}\dots$.¹⁵⁻¹⁷ How could anyone possibly see a difference with respect to their (non-)stochasticity? For all practical purposes, the sequences will appear structurally identically from a stochastic point of view, and heuristically random. For example, both are unknown to be Borel normal; i.e., all finite sub-sequences $y_1y_2y_3\dots y_N$ might be contained in them with the expected frequencies. Indeed, it is not unreasonable to speculate that the pi sequence might be immune to all statistical and algorithmic tests of randomness but one: a test against the assumption that it is the binary expansion of pi, starting from the 571113th billion prime number place onwards.

Another obstacle for the physical conceptualisation of quantum randomness and its operationalisation in terms of physical entities originates in the formalism upon which such endeavours have to be based. The formal incompleteness and independence discovered by Gödel, Tarski, Turing, Chaitin and others essentially renders algorithmic proofs of randomness hopeless. We shall discuss these issues below, but we just note that, as an example, verification of any "law" describable by k symbols requires times exceeding any computable function of k [such as the Ackermann function $A(k)$] and could in general take also that long to be falsified. Thus, the proof of any absence of lawful behaviour seems provable impossible.

Randomness is an asymptotic property, that is, it is unaffected by finite variations. This makes testing randomness extremely

*Author to whom correspondence should be addressed.

[†]Work done at the University of Technology Vienna: The support of the Institute for Theoretical Physics is gratefully acknowledged.

On the solution of trivalent decision problems by quantum state identification

Karl Svozil · Josef Tkadlec

Published online: 4 February 2009
© Springer Science+Business Media B.V. 2009

Abstract The trivalent functions of a trit can be grouped into equipartitions of three elements. We discuss the separation of the corresponding functional classes by quantum state identifications.

Keywords Trivalent decision problems · Quantum computation · Quantum decision problems · Quantum state identification · Entanglement · Generalized Deutsch problem

1 Quantum computation by state identification

One of the advantages of quantum computation (Gruska 1999; Nielsen and Chuang 2000; Mermin 2007; Bennett et al. 1997; Ozhigov 1998; Beals et al. 2001; Cleve 2000; Fortnow 2003) over classical algorithms (Rogers 1967; Odifreddi 1989) is due to the fact that throughout a quantum computation, some classically useful information can be encoded by distributing it over different particles or quanta, such that (Mermin 2003; Svozil 2006)

- measurements of *single* quanta are irrelevant, yield “random” results, and even destroy the original information (by asking complementary questions);
- well defined correlations exist and can be defined among different particles or quanta—even to the extend that a state is solely defined by propositions about *collective* (or *relative*) properties of the particles or quanta involved; and
- identifying a given state of a quantized system can yield information about *collective* (or *relative*) properties of the particles or quanta involved.

K. Svozil (✉)

Institut für Theoretische Physik, Vienna University of Technology, Wiedner Hauptstraße 8-10/136,
1040 Vienna, Austria
e-mail: svozil@tuwien.ac.at

J. Tkadlec

Department of Mathematics, Faculty of Electrical Engineering, Czech Technical University,
166 27 Praha, Czech Republic
e-mail: tkadlec@fel.cvut.cz

How to Acknowledge Hypercomputation?

Alexander Leitsch*

Günter Schachner

*Institut für Computersprachen
Vienna University of Technology
Favoritenstr.9/185, 1040 Vienna, Austria
leitsch@logic.at

Karl Svozil†

*Institute for Theoretical Physics,
Vienna University of Technology,
Wiedner Hauptstraße 8-10/136, 1040 Vienna, Austria
†svozil@tuwien.ac.at*

We discuss the question of how to operationally validate whether or not a “hypercomputer” performs better than the known discrete computational models.

1. Introduction

It is widely acknowledged [1, 2], that every physical system corresponds to a computational process, and that every computational process, if applicable, has to be physically and operationally feasible in some concrete realization. In this sense, the physical and computational capacities should match, because if one is lagging behind the other, there is a lack in the formalism and its potential scientific (and ultimately, technological) applicability. Therefore, the exact correspondence of the mathematical formalism on the one hand, and the particular physical system that is represented by that formalism on the other hand, demand careful attention.

If one insists on operationalizability [3], one need not go very far in the history of mathematics to encounter suspicious mathematical objects. Surely enough, the number π can be defined and effectively computed as the ratio of the circumference to the diameter of a “perfect” (platonian) circle. Likewise, the numbers $\sqrt{2}$ and $\sqrt{3}$ can be interpreted as the ratio between the length of the diagonal to the side length of any square and cube, respectively. But it is not totally unjustified to ask whether or not these numbers have any operational meaning in a strict physical sense; that is, whether such numbers could, at least in principle, be constructed and measured with arbitrary, or even absolute, precision.

At the heart of most of the problems seems to lie the ancient issue of the “very large/small” or even potential infinite versus the actual

Communication cost of breaking the Bell barrier

Karl Svozil*

Institut für Theoretische Physik, University of Technology Vienna, Wiedner Hauptstraße 8-10/136, A-1040 Vienna, Austria

(Received 16 December 2004; published 14 November 2005)

Correlations in an Einstein-Podolsky-Rosen-Bohm experiment can be made stronger than quantum correlations by allowing a single bit of classical communication between the two sides of the experiment.

DOI: [10.1103/PhysRevA.72.050302](https://doi.org/10.1103/PhysRevA.72.050302)

PACS number(s): 03.67.Hk, 03.65.Ud, 03.65.Ta, 03.67.Mn

From an operational point of view, the nonlocal quantum correlations giving rise to violations of Bell-type inequalities amount to the fact that certain joint events at spacelike separated locations occur with greater or smaller frequencies than can possibly be expected from classical, local realistic models. Two detectors at different locations register pairs of particles or particle properties more frequently or infrequently as can be explained by the usual classical assumptions such as value definiteness.

With the rise of quantum algorithms and quantum-information theory [1], the emphasis shifted to the communication cost and to the quantum communication complexity related to those quantum correlations. The question of the expense of obtaining quantum-type correlations from classical systems was stimulated by quantum [2] and classical [3–6] teleportation. In a recent Letter [7], Toner and Bacon, based on Refs. [4,8], argue that classical systems could mimic quantum systems by reproducing the cosine law for correlation functions with the exchange of just one bit of classical information.

The formal coincidence of the quantum correlation function with classical correlations augmented with the exchange of a single classical bit might indicate a deep structure in quantum correlations. One could, for instance, speculate that two-partite quantum systems may be capable of conferring a single bit, a property which is reflected by the cosine form of the expectation function. In what follows it will be argued that, while this may still be the case for the Toner-Bacon protocol [7], in general the exchange of a single classical bit can give rise to stronger than quantum correlations.

Since the systems discussed are entirely planar, whenever possible, polar angles are used to represent the associated unit vectors. The same symbols denote polar angles (without hat) and the associated vectors (with hat). Consider two correlated and spatially separated classical subsystems sharing common directions λ_i , $i=1, \dots$ which are chosen independently of each other and are distributed uniformly. All parameters λ_i are assumed to be identical on each one of the two subsystems. There are two measurement directions a and b of two dichotomic observables with values “-1” and “1” at two spatially separated locations. The measurement direction a at “Alice’s location” is unknown to an observer “Bob”

measuring b and vice versa. A two-particle correlation function $E(\theta)$ with $\theta=|a-b|$ is defined by averaging the product of the outcomes $O(a)_i$, $O(b)_i \in -1, 1$ in the i th experiment, i.e., $E(\theta) = (1/N) \sum_{i=1}^N O(a)_i O(b)_i$.

The following nonadaptive, memoryless protocols could give rise to stronger-than-quantum correlations by allowing the exchange of a single bit per experiment. The protocols are similar to the one discussed by Toner and Bacon [7], but require only a single share λ , and an additional direction $\Delta(\delta)$, which is obtained by rotating $\hat{\lambda}$ clockwise around the origin by an angle δ which is a constant shift for all experiments. That is, $\Delta(\delta) = \lambda + \delta$. Alice’s observable is given by $\alpha = \text{sgn}(\hat{a} \cdot \hat{\lambda}) = \text{sgn}[\cos(a - \lambda)]$. The bit communicated by Alice is given by $c(\delta) = \text{sgn}(\hat{a} \cdot \hat{\lambda}) \text{sgn}[\hat{a} \cdot \hat{\Delta}(\delta)] = \text{sgn}[\cos(a - \lambda)] \text{sgn} \cos[a - \Delta(\delta)]$. Bob’s observable is defined by $\beta(\delta) = \text{sgn}[\hat{b} \cdot [\hat{\lambda} + c(\delta)\hat{\Delta}(\delta)]]$. This protocol becomes Toner and Bacon’s if δ is allowed to vary randomly, with uniform distribution.

The strongest correlations are obtained for $\delta = \pi/2$, i.e., in the case where the two directions associated with λ and $\Delta = \lambda + \pi/2$ are orthogonal and the information obtained by $c(\pi/2)$ is about the location of a within two opposite quadrants. Let $H(x)$ stand for the Heaviside step function of x . The effective shift in the parameter direction $\hat{\lambda} \rightarrow \hat{\lambda} \pm \hat{\lambda}^\perp$ yields a correlation function of the form

$$E\left(\theta, \delta = \frac{\pi}{2}\right) = H\left(\theta - \frac{3\pi}{4}\right) - H\left(\frac{\pi}{4} - \theta\right) - 2\left(1 - \frac{2}{\pi}\theta\right)H\left(\theta - \frac{\pi}{4}\right)H\left(\frac{3\pi}{4} - \theta\right). \quad (1)$$

To obtain a better understanding for the shift mechanism, in Fig. 1 a configuration is drawn which, without the shift $\hat{\lambda} \rightarrow \hat{\lambda} - \hat{\lambda}^\perp$, $\text{sgn}(\hat{b} \cdot \hat{\lambda}) = \text{sgn} \cos(b - \lambda)$ would have contributed the factor -1. The shift results in a positive contribution $\text{sgn}[\hat{b} \cdot (\hat{\lambda} - \hat{\lambda}^\perp)]$ to the expectation value. This shift mechanism always yields the strongest correlations ± 1 as long as the angle θ does not lie between $\pi/4$ and $3\pi/4$.

For general $0 \leq \delta \leq \pi/2$, Fig. 2 depicts numerical evaluations which fit the correlation function

*Electronic address: svozil@tuwien.ac.at

Are simultaneous Bell measurements possible?

Karl Svozil

Institute for Theoretical Physics, University of Technology Vienna,
Wiedner Hauptstrasse 8-10/136, A-1040 Vienna, Austria
E-mail: svozil@tuwien.ac.at

New Journal of Physics **8** (2006) 39

Received 2 February 2006

Published 10 March 2006

Online at <http://www.njp.org/>

doi:10.1088/1367-2630/8/3/039

Abstract. All experimental tests of Bell-type inequalities and Greenberger–Horne–Zeilinger setups rely on the separate and successive measurement of the terms involved. We discuss possibilities of experimental setups to measure all relevant terms simultaneously in a single experiment and find this to be impossible. One reason is the lack of multi-partite states which are unique in the sense that a measurement of some observable on one particle fixes the value of the corresponding observables of the other particles as well.

One motivation for the beautiful Bell-type experiment by Weihs *et al* [1] has been concerns [2] about the implicit coincidence between photon flight time and the specific switching frequency chosen in one of the first experiments [3] to test Bell-type inequalities. As pointed out by Gill *et al* [4]–[6] and by Larsson and Gill [7], any effectively computable synchronization strategy (e.g., [8]) fails for space-like separated observers who choose to switch the measurement directions at random [9, 10]. For Greenberger–Horne–Zeilinger (GHZ) measurements, the issue has already been discussed in the original paper by Pan *et al* [11]. Yet, there might remain reservations and uneasiness related to the fact that in all the experiments performed so far, different terms in the Bell-type inequalities have been measured consecutively, one after another, in different experiment setups.

In what follows we shall investigate, as a second and arguably conceptually more gratifying alternative, the feasibility to either measure or counterfactually infer all required entities simultaneously. By ‘simultaneous’ measurement we mean that all single measurements are pairwise spatially separated and temporally coincide in some reference frame (presumably in the centre-of-mass frame of the particles involved). Note also that, due to the apparent randomness and parameter independence of the single outcomes in the correlation experiment, relativistic locality is possible.

Eutactic quantum codes

Karl Svozil*

Institut für Theoretische Physik, University of Technology Vienna, Wiedner Hauptstraße 8-10/136, A-1040 Vienna, Austria

(Received 10 April 2003; revised manuscript received 3 November 2003; published 8 March 2004)

We consider sets of quantum observables corresponding to *eutactic stars*. Eutactic stars are systems of vectors which are the lower-dimensional “shadow” image, the orthogonal view, of higher-dimensional orthonormal bases. Although these vector systems are not comeasurable, they represent redundant coordinate bases with remarkable properties. One application is quantum secret sharing.

DOI: 10.1103/PhysRevA.69.034303

PACS number(s): 03.67.Hk, 03.65.Ta

The increased experimental feasibility to manipulate single or few particle quantum states, and the theoretical concentration on the algebraic properties of the mathematical models underlying quantum mechanics, have stimulated a wealth of applications in information and computation theory [1,2]. In this line of reasoning, we shall consider quantized systems which are in a coherent superposition of constituent states in such a way that only the coherent superposition of these pure states is in a predefined state; whereas one or all of the constituent states are not. Heuristically speaking, only the coherently combined states yield the “encoded message,” the constituents or “shares” do not.

This feature could be compared to “quantum secret sharing” schemes [3–7], as well as to “entangled entanglement” scenarios [8,9]. There, mostly entangled multipartite system are investigated. Thus, while the above cases concentrate mainly on quantum entanglement, in what follows quantum coherence will be utilized: in the secret-sharing scheme proposed here, one party receives part of a quantum state and the other party receives the other part. The parts are components of a vector lying in subspaces of a higher-dimensional Hilbert space. While the possible quantum states to be sent are orthogonal, the parts are not, so that the parties must put their parts together to decipher the message.

We shall deal with the general case first and consider examples later. Consider an orthonormal basis $\mathcal{E} = \{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ of the n -dimensional real Hilbert space \mathbb{R}^n [whose origin is at $(0, \dots, 0)$]. Every point \mathbf{x} in \mathbb{R}^n has a coordinate representation $x_i = \langle \mathbf{x} | \mathbf{e}_i \rangle$, $i = 1, \dots, n$ with respect to the basis \mathcal{E} . Hence, any vector from the origin $\mathbf{v} = \mathbf{x}$ has a representation in terms of the basis vectors given by $\mathbf{v} = \sum_{i=1}^n \langle \mathbf{v} | \mathbf{e}_i \rangle \mathbf{e}_i = \mathbf{v} \sum_{i=1}^n [\mathbf{e}_i^T \mathbf{e}_i]$, where the matrix notation has been used, in which \mathbf{e}_i and \mathbf{v} are row vectors and “ T ” indicates transposition. ($\langle \cdot | \cdot \rangle$ and the matrix $[\mathbf{e}_i^T \mathbf{e}_i]$ stand for the scalar product and the dyadic product of the vector \mathbf{e}_i with itself, respectively). Hence, $\sum_{i=1}^n [\mathbf{e}_i^T \mathbf{e}_i] = \mathbb{I}_n$, where \mathbb{I}_n is the n -dimensional identity matrix.

Next, consider more general, redundant, bases consisting of systems of “well-arranged” linear dependent vectors $\mathcal{F} = \{\mathbf{f}_1, \dots, \mathbf{f}_m\}$ with $m > n$, which are the orthogonal projections of orthonormal bases of m - (i.e., higher-than- n -) dimen-

sional Hilbert spaces. Such systems are often referred to as *eutactic stars* [10–14]. When properly normed, the sum of the dyadic products of their vectors yields unity, i.e., $\sum_{i=1}^m [\mathbf{f}_i^T \mathbf{f}_i] = \mathbb{I}_n$, giving raise to redundant eutactic coordinates $x'_i = \langle \mathbf{x} | \mathbf{f}_i \rangle$, $i = 1, \dots, m > n$. Indeed, many properties of operators and tensors defined with respect to standard orthonormal bases directly translate into eutactic coordinates [14].

In terms of m -ary (radix m) measures of quantum information based on state partitions [15], k elementary m -state systems can carry k nits [16–18]. A nit can be encoded by the one-dimensional subspaces of \mathbb{R}^m spanned by some orthonormal basis vectors $\mathcal{E}' = \{\mathbf{e}_1, \dots, \mathbf{e}_m\}$. In the quantum logic approach pioneered by Birkhoff and von Neumann (e.g., Refs. [19–22]), every such basis vector corresponds to the physical proposition that “the system is in a particular one of m different states.” All the propositions corresponding to orthogonal base vectors are comeasurable.

On the contrary, the propositions corresponding to the eutactic star

$$\mathcal{F} = \{P\mathbf{e}_1, \dots, P\mathbf{e}_m\}$$

formed by some orthogonal projection P of \mathcal{E}' is no longer comeasurable (or it just spans a one dimensional subspace). Neither is the eutactic star

$$\mathcal{F}^\perp = \{P^\perp \mathbf{e}_1, \dots, P^\perp \mathbf{e}_m\}$$

formed by the orthogonal projection P^\perp of \mathcal{E}' . Indeed, the elements of \mathcal{F} and \mathcal{F}^\perp may be considered as “shares” in the context of quantum secret sharing. Thereby, not all shares may be equally suitable for cryptographic purposes. This scenario can be generalized to multiple shares in a straightforward way.

Let us consider an example for a two-component two-share configuration, in which each party obtains one substate from two possible ones. In particular, consider the two shares $\{\mathbf{w}, \mathbf{x}\}$ and $\{\mathbf{y}, \mathbf{z}\}$ defined in four-dimensional complex Hilbert space by

$$\mathbf{w} = \left(0, 0, -\frac{1}{2\sqrt{2}}, \frac{1}{\sqrt{2}}\right), \quad \mathbf{x} = \frac{1}{2} \left(0, 0, -\frac{3}{2}, -1\right),$$

*Electronic address: svozil@tuwien.ac.at;

URL: <http://tph.tuwien.ac.at/~svozil>

Generalizing Tsirelson's Bound on Bell Inequalities Using a Min-Max Principle

Stefan Filipp*

Atominstytut der Österreichischen Universitäten, Stadionallee 2, A-1020 Vienna, Austria

Karl Svozil†

Institut für Theoretische Physik, University of Technology Vienna, Wiedner Hauptstraße 8-10/136, A-1040 Vienna, Austria

(Received 24 March 2004; published 23 September 2004)

Bounds on the norm of quantum operators associated with classical Bell-type inequalities can be derived from their maximal eigenvalues. This quantitative method enables detailed predictions of the maximal violations of Bell-type inequalities.

DOI: 10.1103/PhysRevLett.93.130407

PACS numbers: 03.65.Ud, 03.67.Mn

The violations of Bell-type inequalities represent a cornerstone of our present understanding of quantum probability theory [1]. Thereby, the usual procedure is as follows: First, the (in)equalities bounding the classical probabilities and expectations are derived systematically, e.g., by enumerating all conceivable classical possibilities and their associated two-valued measures. These form the extreme points which span the classical correlation polytopes [2–12], the faces of which are expressed by Bell-type inequalities which characterize the bounds of the classical probabilities and expectations—in Boole's term [13,14], the “conditions of possible experience.” (Generating functions is another method to find bounds on classical expectations [15,16].) The Bell-type inequalities contain sums of (joint) probabilities and expectations. In a second step, the classical probabilities and expectations in the Bell-type inequalities are substituted by quantum probabilities and expectations. The resulting operators violate the classical bounds. Until recently, little was known about the fine structure of the violations. Tsirelson (also written Cirel'son) published an absolute bound for the violation of a particular Bell-type inequality, the Clauser-Horne-Shimony-Holt (CHSH) inequality [2,3,17,18]. Cabello has investigated a violation of the CHSH inequality beyond the quantum mechanical bound by applying selection schemes to particles in a Greenberger-Horne-Zeilinger state [19,20]. Recently, detailed numerical [21] and analytical studies [22] stimulated experiments [23] to test the quantum bounds of certain Bell-type inequalities.

In what follows, a general method to compute quantum bounds on Bell-type inequalities is reviewed systematically. It makes use of the *min-max principle* for self-adjoint transformations (Ref. [24], Sec. 90 and Ref. [25], Sec. 75) stating that the operator norm is bounded by the minimal and maximal eigenvalues. These ideas are not entirely new and have been mentioned previously [15,21,22], yet to our knowledge no systematic investigation has been undertaken yet. It should also be kept in mind that this method *a priori* cannot produce quantum polytopes [21,26], but the quantum correspondents of

classical polytopes. Indeed, as we demonstrate explicitly, the resulting geometric forms are not convex. This, however, does not diminish the relevance of these quantum predictions to experiments testing the quantum violations of classical Bell-type inequalities.

As a starting point note that since $(A + B)^\dagger = A^\dagger + B^\dagger = (A + B)$ for arbitrary self-adjoint transformations A, B , the sum of self-adjoint transformations is again self-adjoint. That is, all self-adjoint transformations entering the quantum correspondent of any Bell-type inequality are again self-adjoint transformations. The sum does not preserve eigenvectors and eigenvalues; i.e., $A + B$ can have different eigenvectors and eigenvalues than A and B taken separately (i.e., A and B need not necessarily commute). The norm of the self-adjoint transformation resulting from summing the quantum counterparts of all the classical terms contributing to a particular Bell inequality obeys the min-max principle. Thus determining the maximal violations of classical Bell inequalities amounts to solving an eigenvalue problem. The associated eigenstates are the multipartite states which yield a maximum violation of the classical bounds under the given experimental (parameter) setup [27].

Let us demonstrate the method by considering two particles propagating in inverse directions, their polarization or spin being measured along two or more (m) distinct directions per particle perpendicular to their propagation directions. For these configurations, we enumerate analytical quantum bounds corresponding to the Clauser-Horne (CH) inequality, as well as of more general inequalities for $m > 2$ [10–12].

For $m = 2$, the CH inequalities restrict classical probabilities by $-1 \leq p_{13} + p_{14} + p_{23} - p_{24} - p_1 - p_3 \leq 0$, as well as permutations thereof. Here, p_1 and p_3 stand for the probabilities that the first particle is measured along the first direction and the second particle is measured along the third direction. p_{ij} stands for the joint probability to find the first particle along the direction i and the second particle along the direction j .

In order to evaluate the quantum counterpart of the CH inequalities, the classical probabilities have to be substi-