Quantum Advantage by Relational Queries About Equivalence Classes

Karl Svozil(✉)

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

Abstract. Relational quantum queries are sometimes capable to effectively decide between collections of mutually exclusive elementary cases without completely resolving and determining those individual instances. Thereby the set of mutually exclusive elementary cases is effectively partitioned into equivalence classes pertinent to the respective query. In the second part of the paper, we review recent progress in theoretical certifications (relative to the assumptions made) of quantum value indeterminacy as a means to build quantum oracles for randomness.

Keywords: Quantum computation · Partitioning of cases · Quantum parallelism · Hidden subgroup problem · Quantum random number generators

1 Quantum (Dis-)advantages

Genuine quantum computations will be with us for a long time to come, because the miniaturization of electronic circuits is pushing the processor physics into the coherent superposition/complementarity/entanglement/value-indefinite regime (which has no sharp boundary just as the quantum–classical separation is fuzzy and means dependent). Moore's law, insofar as it relates to classical "paper and pencil" [45, p. 34] computation, has reached its effective bottom ceiling approximately ten to five years ago; this is due to exhaustion of minimization with respect to reasonably cooling, as well as by approaching the atomic scale. Most recent performance increases are due to parallelization (if possible).

Alas, this upcoming kind of "enforced" quantum domain computing, imagined by Manin, Feynman, and others, still poses conceptual, theoretical and technological challenges. Indeed, contemporary quantum information theory appears to be far from being fully comprehended, worked out and mature. It is based on quantum mechanics, a theory whose semantics has been notoriously debated almost from its inception, while its syntax – its formalism, and, in particular, the rules of deriving predictions – are highly successful, accepted and relied upon. Depending on temperament and metaphysical inclination, its proponents admit that nobody understands quantum mechanics [13,21], maintain that there is

L. Grandinetti et al. (Eds.): TopHPC 2019, CCIS 891, pp. 504–512, 2019.
https://doi.org/10.1007/978-3-030-33495-6_39

no issue whatsoever [18,22], one should not bother too much [10,14] about its meaning and foundations, and rather shut up and calculate [30,31].

By transitivity or rather a reduction, quantum information theory inherits its quantum mechanics' apparent lack of consensus, as well as a certain degree of cognitive dissonance between applying the formalism while suffering from an absence of conceptual clarity [33], Strong hopes, claims and promises [1–3,16,17,41] of quantum "supremacy" [46] are accompanied by the pertinent question of what exactly, if at all, could make quantum information and computation outperform classical physical resources. Surely many nonclassical quantum features present themselves as being useful or decisive in this respect; among them complementarity, coherence (aka parallelism), entanglement, or value indeterminacy (aka contextuality). But if and how exactly those features will contribute or enable future algorithmic advances still remains to be seen.

The situation is aggravated by the fact that, although the quantum formalism amounts to linear algebra and functional analysis, some of its most important theorems are merely superficially absorbed by the community at large: take, for example, Gleason's theorem [23], and extensions thereof [8,36]. Another example is Shor's factoring algorithm [35, Chapter 5] whose presentations often suffer from the fact that its full comprehension requires a nonsuperficial understanding of number theory, analysis, as well as quantum mechanics; a condition seldom encountered in a single (wo)man. Moreover, often one is confronted with confusing opinions: for instance, the claim that quantum computation is universal with respect to either unitary transformations or first-order predicate calculus is sometimes confused with full Turing universality. And the plethora of algorithms collected into a quantum algorithm zoo [25] is compounded by the quest of exactly why and how quantum algorithms may outperform classical ones.

Quantum advantages may be enumerated in four principal groups, reflecting potential non-classical quantum features:

- quantum parallelism – aka *coherent superposition* of classically mutually exclusive bit states, associated with their simultaneous co-representation;
- quantum collectivism – aka entanglement (involving possibly nonlocal correlations) in a multi-particle situation: information is encoded only in *relational properties* among particles; individual particles have no definite property;
- quantum probabilities are vector-based (orthogonal projection operators), resulting in non-classical expectation values rendering different (from classical value assignments) predictions;
- quantum complementarity: in general quantized systems forbid measurements of certain pairs of observables with arbitrary precision: "you cannot eat a piece of the quantum cake & have another one too;"
- quantum value indefiniteness: there cannot exist classical (true/false) value assignments on certain collections of (intertwining) quantum observables.

In what follows the first and the last feature – parallelism and value indefiniteness – will be discussed in more detail.

2 Suitable Partitioning of Cases

One quantum feature called "quantum parallelism," which is often presented as a possible quantum resource not available classically, is the capacity of n quantum bits to encode 2^n classically mutually exclusive distinct classical bit states at once, that is, simultaneously: $|\Psi\rangle = \sum_{i=0}^{2^n-1} \psi_i |i\rangle$, where the index i runs through all 2^n possible combinations of n classically mutually exclusive bit states $\{0, 1\}$, $|i\rangle$ are elements of an orthonormal basis in 2^n-dimensional Hilbert space, and ψ_i represent probability amplitudes whose absolute squares sum up to 1.

Quantum parallelism, often presented rather mystically, may formally come about rather trivially: the alleged simultaneous quantum co-existence of classically mutually exclusive states is like pretending that a vector in the plane may simultaneously point in both directions of the plane [17]; a sort of confusion between a vector and its components. This seemingly absurd co-representability of contradicting classical states was the motivation for Schrödinger's cat paradox [37]. Note also that, in order to maintain coherence throughout a quantum computation, a *de facto* exponential overhead of "physical stuff" might be required. This could well compensate or even outweigh the advantage; that is, the exponential simultaneous co-representability of (coherent superpositions of) classical mutually exclusive cases of a computation.

The state $|\Psi\rangle$ "carrying" all these classical cases in parallel is not directly accessible or "readable" by any physical operational means. And yet, it can be argued that its simultaneous representation of classically exclusive cases can be put to practical use indirectly if certain criteria are met:

- first of all, there needs to be a quantum physical realizable grouping or partitioning of the classical cases, associated with a particular query of interest; and
- second, this aforementioned query needs to be realizable by a quantum observable.

In that way, one may attain knowledge of a particular feature one is interested in; but, unlike classical computation, (all) other features remain totally unspecified and unknown. There is no "free quantum lunch" here, as a total specification of all observables would require the same amount of quantum queries as with classical resources. And yet, through coherent superposition (aka interference) one might be able to "scramble" or re-encode the signal in such a way that some features can be read off of it very efficiently – indeed, with an exponential (in the number of bits) advantage over classical computations which lack this form of rescrambling and re-encoding (through coherent superpositions). However, it remains to be seen whether, say, classical analog computation with waveforms, can produce similar advantages.

For the sake of a demonstration, the Deutsch algorithm [32, Chapter 2] serves as a Rosetta stone of sorts for a better understanding of the formalism and respective machinery at work in such cases. It is based on the four possible binary functions $f_0, \ldots, f_3$ of a single bit $x \in \{0, 1\}$: the two constant functions

$f_0(x) = 1 - f_3(x) = 0$, as well as the two nonconstant functions: the identity $f_1(x) = x$ and the not $f_3(x) = (x + 1) \bmod 2$, respectively. Suppose that one is presented with a black box including in- and output interfaces, realizing one of these classical functional cases, but it is unknown which one. Suppose further that one is only interested in their parity; that is, whether or not the encoded black box function is a constant function of the argument. Thereby, with respect to the corresponding equivalence relation of being "(not) constant in the arguement" the set of functions $\{f_0, \ldots, f_3\}$ is partitioned into $\{\{f_0, f_3\}, \{f_1, f_2\}\}$.

A different way of looking at this relational encoding is in terms of zero-knowledge proofs: thereby nature is in the role of an agent which is queried about a property/proposition, and issues a correct answer without disclosing all the details and the fine structure of the way this result is obtained.

Classically the only way of figuring this ("constant or not") out is to input the two bit-state cases, corresponding to two separate queries. If the black box admits quantum states, then the Deutsch algorithm presents a way to obtain the answer ("constant or not") directly in one query. In order to do this one has to perform three successive steps [40,44]:

- first one needs to scramble the classical bits into a coherent superposition of the two classical bit states. This can be done by a Hadamard transformation, or a quantum Fourier transformation;
- second, one has to transform the coherent superposition according to the binary function which is encoded in the box. This has to be done while maintaining reversibility; that is, by taking "enough" auxiliary bits to maintain bijectivity/permutation; even if the encoding function is many-to-one (eg, constant).
- third, one needs to unscramble this resulting state to produce a classical output signal which indicates the result of the query. As all involved transformations need to be unitary and thus reversible the latter task can again be achieved by an (inverse) Hadamard transformation, or an (inverse) quantum Fourier transformation.

This structural pattern repeats itself in many quantum algorithms suggested so far. It can be subsumed into the three- or rather fivefold framework: "prepare a classical state; then spread (the classical state into a coherent superposition of classical states) — transform (according to some functional form pertinent to the problem or query considered) — fold (into partitions of classical states which can be accessed via quantum queries and yield classical signals); then detect that classical signal."

Besides the (classical) pre- and post-processing of the data, Shor's algorithm [35, Chapter 5] has a very similar structure in its quantum (order-finding) core: It creates a superposition of classically mutually exclusive states i *via* a generalized Hadamard transformation. It then processes this coherent superposition of all i by computing $x^i \bmod n$, for some (externally given) x and n, the number to be factored. And it finally "folds back" the expanded, processed state by applying an inverse quantum Fourier transform, which then (with high probability) conveniently yields a piece of classical information (in one register) about

the period or order; that is, the least positive integer k such that $x^k = 1(\mathrm{mod}\ n)$ holds. As far as Shor's factoring algorithm is concerned, everything else is computed classically.

Partitioning of states may be related to the hidden subgroup problem [35, Section 5.4.3]: thereby, a function maps from some group to a finite set and is promised to be constant on cosets of the hidden subgroup. If those cosets are identified with the transformations "filtering" and "singling out" [15,38–40] the elements of a partition of states associated with the particular problem, finding the hidden subgroup may yield an effective way of solving this problem (encoded by the state partition).

Whether or not this strategy to find "quantum oracles" corresponding to arbitrary partitions of classical cases is quantum feasible remains to be seen. There appears to be an *ad hoc* counterexample, as there is no speedup for generalized parity [20]; at least with the means considered.

3 Quantum Oracles for Random Numbers

Let me, for the sake of presenting another quantum resource mentioned in the beginning, contemplate one example for which, relative to the assumptions made, quantum "computation" outperforms classical recursion theory: the generation of (allegedly) irreducibly indeterministic numbers; or sequences thereof [7]. A recent extension of the Kochen-Specker theorem [4,6,8] allowing partial value assignments suggests the following algorithm: Suppose one prepares a quantized system capable of three or more mutually exclusive outcomes, formalized by Hilbert spaces of dimension three and higher, in an arbitrary pure state. Then, relative to certain reasonable assumptions (for value assignments and noncontextuality), this system cannot be in any defined, determined property in any other direction of Hilbert state not collinear or orthogonal to the vector associated with the prepared state [24,36]: the associated classical truth assignment cannot be a total function. The proof by contradiction is constructive and involves a configuration of intertwining quantum contexts (aka orthonormal bases). Figure 1 depicts a particular configuration of quantum observables, as well as a particular one of their faithful orthogonal representations [28] in which the prepared and measured states are an angle $\arccos \langle \mathbf{a}|\mathbf{b}\rangle = \arccos \left[(1,0,0)\, \frac{1}{2}\, \left(\sqrt{2},1,1\right)^{\intercal}\right] = \frac{\pi}{4}$ apart [8, Table 1].

Whenever one approaches quantum indeterminacy from the empirical, inductive side, one has to recognize that, without *a priori* assumptions, formal proofs of (in)computability, and more so algorithmic incompressibility (aka randomness [29]) are blocked by reduction to the halting problems and similar [43]. The best one can do is to run tests, such as Borel normality and other criteria, on finite sequences of random number generators [5,12] which turn out to be consistent with the aforementioned value indefiniteness and quantum indeterminacy.

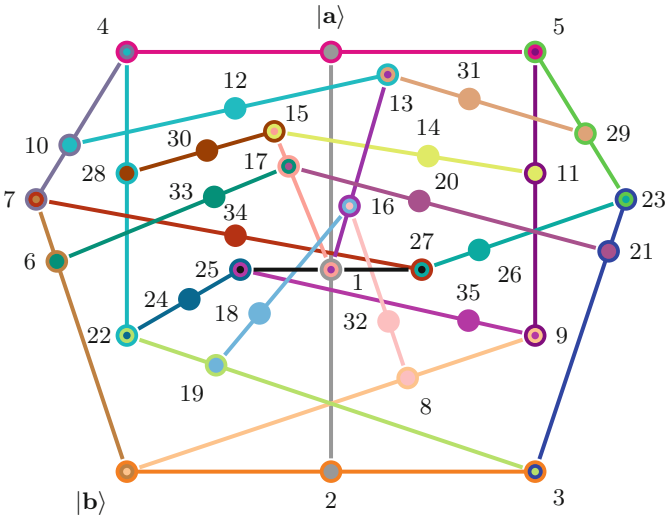

Fig. 1. Greechie orthogonality diagram of a logic [8, Fig. 2, p. 102201-8] realizable in $\mathbb{R}^3$ with the true–implies–value indefiniteness (neither true nor false) property on the atoms $|\mathbf{a}\rangle$ and $|\mathbf{b}\rangle$, respectively. The 8 classical value assignments require $|\mathbf{a}\rangle$ to be false. Therefore, if one prepares the quantized system in state $|\mathbf{a}\rangle$, the second state $|\mathbf{b}\rangle$ cannot have any consistent classical value assignment – it must be value indeterminate/indefinite.

4 Afterthoughts on Assumptions

Let me, as a substitute for a final discussion, mention a *caveat*: as all results and certifications hold true relative to the assumptions made, different assumptions and axioms may change the perceptual framework and results entirely. One might, for instance, disapprove of the physical existence of states and observables beyond a single vector or context [9,42]. Thereby, the problem of measuring other contexts would be relegated to the general measurement problem of coherent superpositions [27]. In this case, as von Neumann, Wigner and Everett have pointed out, by "nesting" the measurement objects and the measurement apparatus in larger and larger systems [19], the assumption of the universal validity of the quantum state evolution would result in mere epistemic randomness; very much like the randomness encountered in, and the second law of [34], classical statistical physics. From that perspective, quantum randomness might turn out to be valid "for all practical purposes" [10] through interaction with a huge number of (uncontrollable) degrees of freedom in the environment of a quantized system in a coherent state, "squeezing" out this coherence very much like a balloon losing gas [11].

Acknowledgments. I kindly acknowledge enlightening discussions with Cristian Calude about many of the subjects mentioned. All misconceptions and errors are mine. I declare that I have no conflict of interest.

References

1. Aaronson, S.: Happy new year! My response to M. I. Dyakonov (1999). http://www.scottaaronson.com/writings/bignumbers.html. Accessed 16 Mar 2017
2. Aaronson, S.: Quantum Computing Since Democritus. Cambridge University Press, New York (2013). https://doi.org/10.1017/CBO9780511979309
3. Abbott, A.A., Calude, C.S.: Limits of quantum computing: a sceptic's view. http://www.quantumforquants.org/quantum-computing/limits-of-quantum-computing/. Accessed 19 June 2016
4. Abbott, A.A., Calude, C.S., Conder, J., Svozil, K.: Strong Kochen-Specker theorem and incomputability of quantum randomness. Phys. Rev. A **86**, 062109 (2012). https://doi.org/10.1103/PhysRevA.86.062109
5. Abbott, A.A., Calude, C.S., Dinneen, M.J., Huang, N.: Experimentally probing the algorithmic randomness and incomputability of quantum randomness. Physica Scripta **94**(4), 045103 (2019). https://doi.org/10.1088/1402-4896/aaf36a
6. Abbott, A.A., Calude, C.S., Svozil, K.: Value-indefinite observables are almost everywhere. Phys. Rev. A **89**, 032109 (2014). https://doi.org/10.1103/PhysRevA.89.032109
7. Abbott, A.A., Calude, C.S., Svozil, K.: On the unpredictability of individual quantum measurement outcomes. In: Beklemishev, L.D., Blass, A., Dershowitz, N., Finkbeiner, B., Schulte, W. (eds.) Fields of Logic and Computation II. LNCS, vol. 9300, pp. 69–86. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-23534-9_4
8. Abbott, A.A., Calude, C.S., Svozil, K.: A variant of the Kochen-Specker theorem localising value indefiniteness. J. Math. Phys. **56**(10), 102201 (2015). https://doi.org/10.1063/1.4931658
9. Aufféves, A., Grangier, P.: Extracontextuality and extravalence in quantum mechanics. Philos. Trans. R. So. A: Math. Phys. Eng. Sci. **376**(2123), 20170311 (2018). https://doi.org/10.1098/rsta.2017.0311
10. Bell, J.S.: Against 'measurement'. Phys. World **3**, 33–41 (1990). https://doi.org/10.1088/2058-7058/3/8/26
11. Bengtsson, I., Zyczkowski, K.: Geometry of quantum states - addendum (2018). http://chaos.if.uj.edu.pl/~karol/decoh18.pdf. Accessed 24 Mar 2019
12. Calude, C.S., Dinneen, M.J., Dumitrescu, M., Svozil, K.: Experimental evidence of quantum randomness incomputability. Phys. Rev. A **82**(2), 022102 (2010). https://doi.org/10.1103/PhysRevA.82.022102
13. Clauser, J.: Early history of Bell's theorem. In: Bertlmann, R., Zeilinger, A. (eds.) Quantum (Un)speakables: From Bell to Quantum Information, pp. 61–96. Springer, Berlin (2002). https://doi.org/10.1007/978-3-662-05032-3_6
14. Dirac, P.A.M.: The Principles of Quantum Mechanics, 4th edn. Oxford University Press, Oxford (1930, 1958)
15. Donath, N., Svozil, K.: Finding a state among a complete set of orthogonal ones. Phys. Rev. A **65**, 044302 (2002). https://doi.org/10.1103/PhysRevA.65.044302
16. Dyakonov, M.I.: State of the Art and Prospects for Quantum Computing, chap. 20, pp. 266–285. Wiley (2013). https://doi.org/10.1002/9781118678107.ch20

17. Dyakonov, M.I.: When will we have a quantum computer? (2019). https://arxiv.org/abs/1903.10760, talk at the conference "Future trends in microelectronics", Sardinia (2018). To be published in a special issue of Solid State Electronics
18. Englert, B.G.: On quantum theory. Eur. Phys. J. D **67**(11), 1–16 (2013). https://doi.org/10.1140/epjd/e2013-40486-5
19. Everett III, H.: The Everett Interpretation of Quantum Mechanics: Collected Works 1955–1980 with Commentary. Princeton University Press, Princeton (2012). http://press.princeton.edu/titles/9770.html
20. Farhi, E., Goldstone, J., Gutmann, S., Sipser, M.: Limit on the speed of quantum computation in determining parity. Phys. Rev. Lett. **81**, 5442–5444 (1998). https://doi.org/10.1103/PhysRevLett.81.5442
21. Feynman, R.P.: The Character of Physical Law. MIT Press, Cambridge (1965)
22. Fuchs, C.A., Peres, A.: Quantum theory needs no 'interpretation'. Phys. Today **53**(4), 70–71 (2000). https://doi.org/10.1063/1.883004, further discussions of and reactions to the article can be found in the September issue of Physics Today, 53, 11–14 (2000)
23. Gleason, A.M.: Measures on the closed subspaces of a Hilbert space. J. Math. Mech. (now Indiana Univ. Math. J.) **6**(4), 885–893 (1957). https://doi.org/10.1512/iumj.1957.6.56050
24. Hrushovski, E., Pitowsky, I.: Generalizations of Kochen and Specker's theorem and the effectiveness of Gleason's theorem. Stud. Hist. Philos. Sci. Part B: Stud. Hist. Philos. Mod. Phys. **35**(2), 177–194 (2004). https://doi.org/10.1016/j.shpsb.2003.10.002
25. Jordan, S.: Quantum Algorithm Zoo (2011–2019). http://quantumalgorithmzoo.org/. Accessed 26 Mar 2019
26. London, F., Bauer, E.: La theorie de l'observation en mécanique quantique; No. 775 of Actualités scientifiques et industrielles: Exposés de physique générale, publiés sous la direction de Paul Langevin. Hermann, Paris (1939). English translation in [27]
27. London, F., Bauer, E.: The theory of observation in quantum mechanics. In: Quantum Theory and Measurement, pp. 217–259. Princeton University Press, Princeton (1983). Consolidated Translation of French Original [26]
28. Lovász, L.: On the Shannon capacity of a graph. IEEE Trans. Inf. Theory **25**(1), 1–7 (1979). https://doi.org/10.1109/TIT.1979.1055985
29. Martin-Löf, P.: On the notion of randomness. In: Kino, A., Myhill, J., Vesley, R.E. (eds.) Intuitionism and Proof Theory, p. 73. North-Holland, Amsterdam and London (1970)
30. Mermin, D.N.: Could Feynman have said this? Phys. Today **57**, 10–11 (1989). https://doi.org/10.1063/1.1768652
31. Mermin, D.N.: What's wrong with this pillow? Phys. Today **42**, 9–11 (1989). https://doi.org/10.1063/1.2810963
32. Mermin, D.N.: Quantum Computer Science. Cambridge University Press, Cambridge (2007). https://doi.org/10.1017/CBO9780511813870
33. Mermin, D.N.: Making better sense of quantum mechanics (2019). https://arxiv.org/abs/1809.01639
34. Myrvold, W.C.: Statistical mechanics and thermodynamics: a Maxwellian view. Stud. Hist. Philos. Sci. Part B: Stud. Hist. Philos. Mod. Phys. **42**(4), 237–243 (2011). https://doi.org/10.1016/j.shpsb.2011.07.001
35. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2010). https://doi.org/10.1017/CBO9780511976667, 10th Anniversary Edition

36. Pitowsky, I.: Infinite and finite Gleason's theorems and the logic of indeterminacy. J. Math. Phys. **39**(1), 218–228 (1998). https://doi.org/10.1063/1.532334
37. Schrödinger, E.: Die gegenwärtige Situation in der Quantenmechanik. Naturwissenschaften **23**, 807–812, 823–828, 844–849 (1935). https://doi.org/10.1007/BF01491891. https://doi.org/10.1007/BF01491914. https://doi.org/10.1007/BF01491987
38. Svozil, K.: Quantum information in base n defined by state partitions. Phys. Rev. A **66**, 044306 (2002). https://doi.org/10.1103/PhysRevA.66.044306
39. Svozil, K.: Quantum information via state partitions and the context translation principle. J. Mod. Opt. **51**, 811–819 (2004). https://doi.org/10.1080/09500340410001664179
40. Svozil, K.: Characterization of quantum computable decision problems by state discrimination. In: Adenier, G., Khrennikov, A., Nieuwenhuizen, T.M. (eds.) Quantum Theory: Reconsideration of Foundations–3, vol. 810, pp. 271–279. American Institute of Physics (2006). https://doi.org/10.1063/1.2158729
41. Svozil, K.: Quantum hocus-pocus. Ethics Sci. Environ. Politics (ESEP) **16**(1), 25–30 (2016). https://doi.org/10.3354/esep00171
42. Svozil, K.: New forms of quantum value indefiniteness suggest that incompatible views on contexts are epistemic. Entropy **20**(6), 406(22) (2018). https://doi.org/10.3390/e20060406
43. Svozil, K.: Physical (A)Causality. Determinism, Randomness and Uncaused Events. FTP, vol. 192. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-70815-7
44. Svozil, K., Tkadlec, J.: On the solution of trivalent decision problems by quantum state identification. Natural Computing (2009, in print). https://doi.org/10.1007/s11047-009-9112-5
45. Turing, A.M.: Intelligent machinery. In: Evans, C.R., Robertson, A.D.J. (eds.) Cybernetics. Key Papers, pp. 27–52. Butterworths, London (1968)
46. Wiesner, K.: The careless use of language in quantum information. https://arxiv.org/abs/1705.06768