Some Quantum advantages

http://tph.tuwien.ac.at/~svozil/publ/2019-Svozil-TopHPC2019-pres.pdf

https://arxiv.org/abs/1904.08307

Karl Svozil

ITP/Vienna University of Technology, Austria
svozil@tuwien.ac.at

TopHPC2019, Tehran, Iran, April 22-25, 2019

Possible quantum advantages: features not present in classical "paper machines"

- Quantum parallelism – aka *coherent superposition* – of classically mutually exclusive bit states (Schrödinger DOI: 10.1007/BF01491891 (§5, cat paradox), 10.1007/BF01491914, 10.1007/BF01491987);
- Quantum collectivism – aka (possibly nonlocal correlations DOI: 10.1103/PhysRev.47.777) entanglement – in a multi-particle situation: information encoded only in *relational properties* among particles; individual particles have no definite property; exploitable for quantum cryptography & communication & authentification (Schrödinger DOI: 10.1007/BF01491891, 10.1007/BF01491914 (§10), 10.1007/BF01491987);

Possible quantum advantages: features not present in classical "paper machines" cntd.

- Quantum probabilities based on vectors (orthogonal projection operators) rather than on sets: non-classical expectation values rendering different (from classical value assignments) predictions; in particular, violations of Boole-Bell type inequalities; exploitable for quantum cryptography & communication & authentification (Boole DOI: 10.1098/rstl.1862.0015, Bell DOI: 10.1103/RevModPhys.38.447);
- 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;" exploitable for quantum cryptography & communication (Pauli DOI: 10.1007/978-3-642-61287-9, Moore DOI: 10.1515/9781400882618-006);

Possible quantum advantages: features not present in classical "paper machines" cntd.

- Quantum value indefiniteness: no classical (true/false) value assignments on certain collections of (intertwining) quantum observables; exploitable for quantum oracles of randomness (Gleason DOI: 10.1512/iumj.1957.6.56050, Kochen & Specker DOI: 10.1512/iumj.1957.6.56050, Abbott, Calude, Svozil DOI: 10.1017/S0960129512000692, 10.1063/1.4931658).

"Babylonian" example collection: Stephen Jordan's *quantum algorithm zoo* @ url `http://quantumalgorithmzoo.org/`

Scheme to exploit quantum parallelism supporting/rendering equivalence classes (partitions) of classically distict cases

- prepare a classical state;
- spread the classical state into a coherent superposition of classical states by a Hadamard or quantum Fourier transformation;
- 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; and, finally,
- detect that classical signal.

"Babylonian" example 1: Deutsch algorithm (eg, Mermin DOI: 10.1017/CBO9780511813870) – "parity" [aka (non)constancy] of a Boolean function of a single bit

Suppose you are given a black box implementing one of the four functions – but you don't know which one:

The task is to find out (not which function but) whether or not this function is constant. This induces a partition

$$\{\{f_0, f_3\}, \{f_1, f_2\}\}$$

$f_i(x)$	$x = 0$	$x = 1$
f_0	0	0
f_1	0	1
f_2	1	0
f_3	1	1

of the set $\{f_0, f_1, f_2, f_3\}$ of all such functions, which can be realized by one quantum query.

However: No generalization exist, as there is no exponential quantum speedup for parity (Farhi, Goldstone, Gutmann & Sipser DOI: 10.1103/PhysRevLett.81.5442).

“Babylonian” example 2: Shor’s algorithm (eg, Nielsen & Chuang DOI: 10.1017/CBO9780511976667)

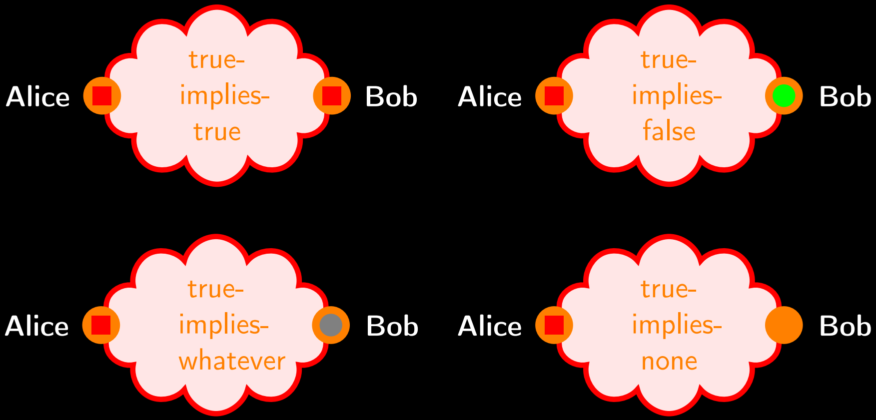
- It creates a superposition of classically mutually exclusive states i *via* a generalized Hadamard transformation;
- It processes this coherent superposition of all i by computing $x^i \bmod n$, for some (externally given) x and n, the number to be factored.
- And it finally “folds back” the expanded, processed state by applying an inverse quantum Fourier transform, which then (with high probability) conveniently yields a classical information (in one register) about the period or order; that is, the least positive integer k such that $x^k = 1 (\bmod\ n)$ holds.

As far as Shor’s factoring algorithm is concerned, everything else is computed classically.

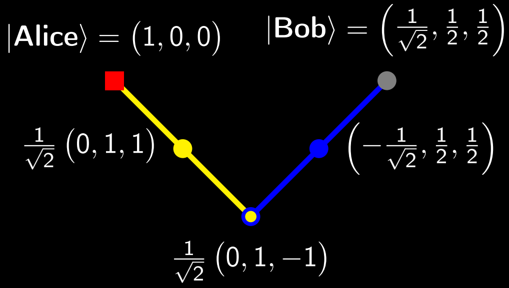
Scheme to exploit quantum value indefiniteness supporting/rendering quantum (oracles for) random number generators

- Alice prepares a pure state, representable by a vector (in a context);
- Bob measures an observable proposition, representable by another vector (in a context) which is neither collinear nor orthogonal to Alice's preparation.
- Alice's and Bob's preparation & measurement are then connected by a quantum cloud – that is, by a collection of intertwining counterfactual quantum contexts (and observables).
- These clouds are then interpreted classically; in particular, and in its strongest form, it is shown that these clouds – or at least the outcome of Bob's measurement – do not have any classical representation.

How is $|\textbf{Bob}\rangle$ given $|\textbf{Alice}\rangle$? True? False? Whatever? None?

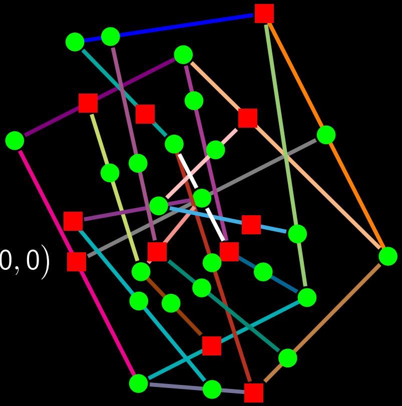


True (1) implies whatever (quantum 50:50)



True (1) implies false (0) (Svozil DOI: 10.3390/e20060406, based on Abbott, Calude & Svozil DOI: 10.1017/S0960129512000692)

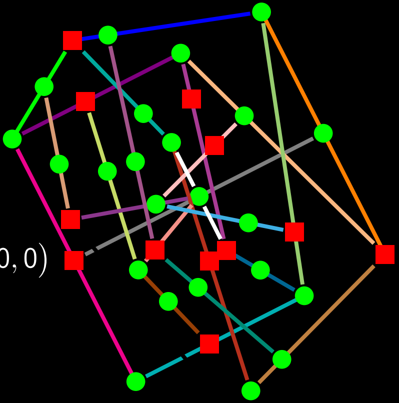
$|\textbf{Alice}\rangle = (1, 0, 0)$



$|\textbf{Bob}\rangle = \left(\frac{1}{\sqrt{2}}, \frac{1}{2}, \frac{1}{2}\right)$

True (1) implies true (1) (Svozil DOI: 10.3390/e20060406, based on Abbott, Calude & Svozil DOI: 10.1017/S0960129512000692)

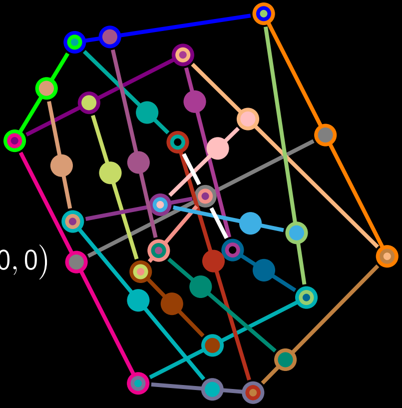
$|\textbf{Alice}\rangle = \left(1, 0, 0\right)$



$|\textbf{Bob}\rangle = \left(\frac{1}{\sqrt{2}}, \frac{1}{2}, \frac{1}{2}\right)$

True (1) implies value indefinite (Abbott, Calude & Svozil DOI: 10.1017/S0960129512000692)

$|\textbf{Alice}\rangle = (1, 0, 0)$



$|\textbf{Bob}\rangle = \left(\frac{1}{\sqrt{2}}, \frac{1}{2}, \frac{1}{2}\right)$

Strategies to obtain value indefiniteness/partiality

The scheme of the construction & proof of partiality of value assignments is as follows:

(i) Find a logic (collection of intertwined contexts of observables) exhibiting a true-implies-false property on the two atoms **a** and **b**.

(ii) Find another logic exhibiting a true-implies-true property on the same two atoms **a** and **b**.

(iii) Then join (paste) these logics into a larger logic, which, given **a**, neither allows **b** to be true nor to be false. Consequently **b** must be value indefinite.

Extensions of value indefiniteness/partiality

Partiality/value indefiniteness can be extended to any vector **b** non-collinear and non-orthogonal to **a** (Abbott, Calude & Svozil DOI: 10.1017/S0960129512000692)

For a (in some respects weaker because it is based on stronger assumptions) proof relative to global truth assignments, see Pitowsky DOI: 10.1063/1.532334

History of contextual sets & elational properties realizable by two-point quantum clouds

if a is true classical value assignments	anectodal, historic quantum realisation	reference to utility or relational properties
imply **b** is independent (arbitrary)	firefly logic L_{12} eg, Cohen, 1989[pp. 21, 22]	
imply **b** false (TIFS)	Specker bug logic S, 1965 [Fig. 1, p. 182]	Stairs, 1983 [p. 588-589], Cabello et al, 1995 . . . 2018
imply **b** true (TITS)	extended Specker bug logic	KS, 1967 [Γ_1, p. 68], Clifton, 1993 [Sects. II,III, Fig. 1], Belinfante, 73 [Fig. C.l. p. 67], Pitowsky, 1982 [p. 394], Hardy, 1992, 1993, 1997, Cabello et al, 1995 . . . 2018
iff **b** true (nonseparability)	combo of intertwined Specker bugs	KS, 1967 [Γ_3, p. 70]
imply value indefiniteness of **b**	depending on types of value assignments	Pitowsky, 1998, Abbott et al, 2012 . . . 2015

BUT: Epistemology/ontology of clouds of intertwined contexts/cliques/maximal observables/Boolean subalgebras

Summary

- Quantum parallelism exploitable sometimes (similar to zero knowledge proofs) but not always; that is, for all equivalence classes (partitions).
- Quantum random number generators (oracles) are "theoretically certified" relative to the assumptions made, and the quantum means employed.

For some critical thoughts on the prospects of quantum computation, please see quantum hocus-pocus DOI: 10.3354/esep00171.

Thank you for your attention!