Vol. 16: 25–30, 2016
doi: 10.3354/esep00171

ETHICS IN SCIENCE AND ENVIRONMENTAL POLITICS
Ethics Sci Environ Polit

Published online November 28

Quantum hocus-pocus

Karl Svozil*

Institute for Theoretical Physics, Vienna University of Technology, Wiedner Hauptstraße 8-10/136, 1040 Vienna, Austria, and Department of Computer Science, University of Auckland, Private Bag 92019, Auckland 1142, New Zealand

ABSTRACT: The claims made in a manifesto resulting in the European quantum technologies flagship initiative in quantum technology and similar enterprises are taken as a starting point to critically review some potential quantum resources, such as coherent superposition and entanglement, and their dormant usefulness for parallelism and communication. Claims of absolute, irreducible (non-epistemic) randomness are argued to be metaphysical. Cryptanalytic man-in-the-middle attacks on quantum cryptography are well known to be feasible but hardly mentioned. If all of this is taken into account, a more sober perspective on quantum capacities emerges, but it may be ethically more justified than the 'hype and magic' that drives many current initiatives.

KEY WORDS: Quantum computation · Quantum information

INTRODUCTION

The European Quantum Manifesto (de Touzalin et al. 2016) contributed to the launch of a € 1 billion quantum technologies flagship initiative in quantum technology (European Commission 2016a). Thereby, quanta which "can be in different states at the same time ('superposition') and can be deeply connected without direct physical interaction ('entanglement')" are expected to create a 'second quantum revolution' by taking "quantum theory to its technological consequences" (European Commission 2016b).

This is in line with assurances by many proponents that 'quantum mechanics is magic' and, indeed, so irreducibly incomprehensible by rational human thought that anybody asking, "But how can it be like that?" will be dragged "'down the drain', into a blind alley from which nobody has yet escaped" (Feynman 1965, p. 129). From that perspective, it appears prudent to harvest these alleged capacities beyond classical algorithmics for technology and the economy at large, in particular if the experts proclaim such a program to be feasible.

I would like to state up front that I am not criticising this new initiative on the grounds that money will be wasted. On the contrary, it will be money wisely spent, and many new and interesting research and technological development will spin off from this initiative.

However, in what follows, I would like to point out that, at least in the way it is marketed, the quantum technologies flagship initiative in quantum technology is deceptive, if not dangerously misleading.

It is deceptive because while many of the Quantum Manifesto's short- and medium-term goals are reachable or have already been achieved, some of these goals strongly depend on the assumptions made.

It is dangerous because it pretends to deliver — for instance, with respect to quantum random number generators and quantum cryptography — what is provably impossible.

Moreover, it is highly unlikely that some of the long-term goals are achievable even in principle.

QUANTUM COMPUTATION

Let us first review quantum computation, in particular the Quantum Manifesto's long-term goal to

*Corresponding author: svozil@tuwien.ac.at

Publisher: Inter-Research · www.int-res.com

"build a universal quantum computer able to demonstrate the resolution of a problem that, with current techniques on a supercomputer, would take longer than the age of the universe" (de Touzalin et al. 2016, p. 18). I do not know what the authors had in mind by formulating this bold claim, but when it comes to quantum computation as compared to classical universal computation, there are at least 2 issues which have to be kept in mind: one is algorithmic in nature, and one is hardware related.

Quantum algorithm

As anecdotal as this may sound, one of the greatest former talents in quantum computation, and co-author of an authoritative volume on the subject (which, after publication in 2000, made it to the 10th anniversary edition in 2010), gave up his tenured academic position to work "as an advocate for open science" (Nielsen 2016).

Such brain drain is surprising, given the hype. Alas, it might not be too negative to state that, besides a growing zoo of quantum algorithms (Jordan 2011–2016) (and notwithstanding some progress in communication complexity [Raz 1999, Montanaro 2011, Gavinsky 2016], given unlimited computational power), quantum algorithms have not advanced much since the proposal of Grover's algorithm, for a period of 20 yr now. So, to call this field of research 'progressive' might be overly optimistic.

Moreover, while quantum factoring is often mentioned as a 'killer app' for quantum computation, classical prime factorization is neither in the class of NP-complete problems nor can it be excluded that classical algorithms solve this task in polynomial time, just like Shor's probabilistic quantum algorithm. The key issue, in my opinion, is a lack of knowledge of just what the quantum assets and capacities, capable of potentially trespassing classical computational means, really are.

Parallel processing by superpositions

Many researchers would be inclined to postulate quantum superpositions — the capacity to simultaneously co-represent classically distinct, even mutually contradictory, states — and the resulting sort of parallelism as one of the main quantum-over-classical advantages.

Unfortunately, all of our attempts to comprehend a widely cited paper on quantum complexity theory (Bernstein & Vazirani 1993) failed. In particular, their hint in Section 3.3, that superposition (and thus parallelism) requires a huge (exponential) computational capacity (one that could potentially be harvested) of the physical universe, is immediately questioned by mentioning restrictions because the quantum evolution is essentially a permutation of the quantum state.

A recent review (Montanaro 2016) also attempts to locate quantum capacities by emphasizing coherent superpositions (and thus parallelism). It is mentioned that a cynical reader might point out that, based on a result by Shi (2003), any quantum algorithm whatsoever can be expressed as the use of just 2 components: (1) gates producing coherent superpositions of a classical bit (such as the Hadamard gate or quantum Fourier transforms) interspersed with (2) classical processing.

Alas, all the parallel 'results' of a quantum computation encoded in a coherent superposition are not directly accessible; due to quantum complementarity and the no-cloning theorem, there is no way to access and measure complementary aspects of an arbitrary pure state comprehensively. In terms of the many-worlds interpretation, every one of the parallel results resides in one of those parallel worlds simultaneously, but any particular observer has direct access to only one such universe.

Indeed, relative to 'reasonable' assumptions, observables which are not identical to pure states (and their negation) cannot consistently (co-)exist with the latter (Pitowsky 1998, Abbott et al. 2015). From this point of view, 'coherent superpositions' just correspond to improper, misleading representations of non-existing aspects of physical reality. They are delusive because they confuse ontology with epistemology (Jaynes 1989, 1990) by suggesting the physical co-existence of counterfactuals, in particular classically inconsistent cases, in an exploitable classical manner. However, upon closer inspection, this alleged capacity might just be a consequence of a misconception, yielding an operational ill-representation of the quantum state (Svozil 2014).

'Forcing' a 'measurement' of such states in a coherent superposition of 'observables' results in a context translation (Svozil 2004). This may introduce stochasticity due to the many (for all practical purposes [Bell 1990]) uncontrollable degrees of freedom of the measurement device (Englert et al. 1988).

Nevertheless, with all these provisos, a potential quantum advantage resides in the possibility to encode certain suitable relational functional properties representable by (equi-)partitions of the image of

the function (Donath & Svozil 2002, Svozil 2002) into suitable orthogonal projections (Svozil 2016). Unfortunately, this is not ubiquitous, as for certain tasks such as parity, effective speedups are impossible (Farhi et al. 1998).

Multipartite communication by entanglement

Quantum mechanics denies the separate existence and apartness of certain entities (such as quanta of light) 'tightly bundled together' by entanglement. Indeed, the entire state of multiple quanta can be expressed completely, uniquely and solely in terms of correlations (joint probability distributions) (Bergia et al. 1980, Mermin 1998) or by another term, relational properties (Zeilinger 1999), among observables belonging to the subsystems irrespective of their relativistic spatio-temporal locations (Seevinck 2010). Consequently, one has "a complete knowledge of the whole, without knowing the state of any one part. That a thing can be in a definite state, even though its parts were not" (IBM 2016).

In more technical terms, this can be interpreted as just another consequence of quantum coherence, only that the co-represented classical cases refer to product states of multiple quanta, thereby effectively allowing 2 or more different quanta to be coherently connected over a large distance. Note also that if the 2 parties share correlated pairs of quanta, then (by quantum teleportation) the quantum communication and selection between those parties can be done by classical information.

While it may be too early for a definite answer, many (exponential) quantum speedups (Raz 1999, Montanaro 2011, Gavinsky 2016) might again, just as in the functional case, be due to the possibility to encode communication tasks into suitable orthogonal subspaces. Observe that every binary function $g\colon x \times x \to z$ can be converted into an equivalent unary function $f\colon x \to z^x$, such that $g(x_1, x_2) = [f(x_2)](x_1) \in z$. One may think of x_2 as some 'index' running over unary functions f. If this 'index' can be efficiently communicated, f and its equivalent representation g can be evaluated.

Quantum hardware

In the last 30 yr, single-quantum experiments, such as single quanta in a double slit, and all kinds of other interference and state (re-)construction experiments sharpened and enlightened our understanding of the quanta. One of the main features of the (unitary quantum) evolution is that it is a permutation of the state; therefore, at least in principle, information can be neither created (or copied) nor lost. Thus, designs of quantum computers have to answer the question of how to get rid of auxiliary qubits (they cannot).

Another formidable question is to maintain coherence over sufficient amounts of computation space and time, thereby keeping the system isolated, that is, by avoiding entanglement with the environment. It may well be that maintenance of coherence scales exponentially with both computation space and time, thereby rendering quantum computation non-scalable.

It should be kept in mind that while it may, in very special cases, be possible to obtain quantum coherence for more than a thousand qubits, those systems are non-universal and are specifically tailored for very particular tasks. And, of course, every system is a perfect simulation of itself; so as every system is quantized, it is also a perfect simulation of a multipartite quantum state; indeed, this could involve zillions of quanta.

HYPERCOMPUTATIONAL CAPACITIES THROUGH IRREDUCIBLE QUANTUM RANDOMNESS

Since 'true' sources of randomness are often required in quantum information theory such as in quantum cryptography, quantum random number generators will be shortly discussed next. While Born and others have expressed their personal inclinations about randomness in nature, and have explicitly stated their very subjective choices as such, this supposition has been canonized and postulated as an axiom. It is corroborated by our obvious inability to come up with theoretical predictions of certain quantum outcomes.

In practice, quantum random number generators are tested and certified by performing a battery of statistical criteria, such as diehard tests, on finite sequences of data. This is far from the claims of absolute, irreducible certification promised to customers.

Unfortunately, by merely studying the raw data without additional assumptions (such as the quantum axiom mentioned), and even if the supposedly random data sequences could be provided at arbitrary length, due to the recursive undecidability of the rule inference problem and other theorems of recursion theory, claims of absolute randomness are provably

unprovable and therefore are metaphysical, that is, beyond the reach of science. In other words, science can neither assert nor disprove quantum randomness and never will be able to do so: this method is (provably) blocked by limits due to consistency and, consequently, the avoidance of paradoxical self-reference (Yanofsky 2003).

Therefore, any claims that quantum random number generators are certified by the very laws of nature to behave indeterministically are incorrect. Certification resides in, and is relative to, the validity of canonical quantum theory, which in turn resides in our beliefs in it.

Another way of thinking about quantum randomness is in terms of the supposedly (that is, relative to the axioms) 'indeterministic' generation process. Particular single outcomes are thought of as occurring without deterministic cause, quasi *ex nihilo*. In theological terms, such outcomes are by *creatio continua*. Thereby, the 'measurement of the outcome' is postulated to come about in a quantum formalism based on an evolution that one-to-one permutes the state (which consequently has a unique history), an ambivalence (Everett 1957, p. 454) which is protected through orthodoxy.

Very often, it is also not explicitly disclosed how exactly such random sequences are generated and where the randomness resides — would, for instance, a source of photons impinging on 2 detectors qualify as a beam splitter? — not to mention the fact that lossless beam splitters are represented by one-to-one unitary transformations, that is, merely permuting the state, let alone the method of normalization of the unbiased raw signals.

QUANTUM CRYPTOGRAPHY

Regarding cryptography, the Quantum Manifesto mentions 2 goals. One is a medium-term goal: to "enable secure communication between distant cities via quantum networks, which enhance information security and make eavesdropping impossible" (de Touzalin et al. 2016, p. 17); and one is a long-term goal: to "create a secure and fast quantum internet connecting the major cities in Europe using quantum repeaters running quantum communication protocols" (de Touzalin et al. 2016, p. 18).

Contrary to publicized claims, quantum cryptography is insecure and can be successfully cryptanalyzed through man-in-the-middle attacks, that is, by compromising both quantum and (public) classical communication lines (cf. references in Svozil 2006 for a 'demonstration' using Viennese chocolate balls). This is a well-known fact which is already explicitly mentioned in the original paper by Bennett & Brassard (1984), as follows: "The need for the public (non-quantum) channel in this scheme to be immune to active eavesdropping can be relaxed if Alice and Bob have agreed beforehand on a small secret key, which they use to create Wegman-Carter authentication tags [WC] for their messages over the public channel."

Alas, the consequences of the cryptanalytic capacities that can be deployed through non-immune classical channels are more devastating than they first may appear because quantum cryptography is often seen as a remedy for non-immune, and thus compromised, public classical channels. However, to prove 'unconditional security' of quantum cryptography, it has to be assumed that the public classical channel is immune (thus the necessity of classical authentication). As a consequence, one is relegated to 'growing' an initial key at best; but key growing might be perceived as merely a gradual improvement over classical methods, since the identities of the communicating parties still need to be checked by classical authentication.

In short, if a classical channel is not compromised, no quantum cryptography is required. Since quantum cryptography protocols such as the one mentioned earlier presuppose an immune classical channel, they can be compromised if the classical channel is compromised.

This simple fact is often 'taken for granted' and not mentioned in proofs of 'unconditional security of quantum cryptography,' even in authoritative reviews of the subject. As a consequence, those proofs are correct relative to the absence of tampering with the classical channel.

One of the problems with claims of absolute security (certified by the quantum nature) is that, as in other domains, while ignorance favours the proponents of a technology, the real costs as well as the disadvantages have to be borne by others having their skin in the game. Ernst Specker called such particular instances of non-disclosure 'Jesuit lies' because the neglect to mention allegedly obvious but important and decisive unfavourable facts is different from stating false propositions; Jesuits have faced a not dissimilar problem (and solution) under torture or danger.

By the same rhetoric, fission reactors are 'unconditionally secure,' provided earthquakes and tsunamis are absent, as well as reckless misconduct and other problems that would make them insecure.

WHATEVER IT TAKES

As I have emphasized at the beginning, I have no intention to criticize the European flagship initiative in quantum technology on grounds that liquidity is poured into certain quantum laboratories and industries. What I criticize is the hubris in marketing it. Of course, one might say that at the end of the day, nobody will remember the claims that initiated the funding; all of its proponents and political supporters and enablers will be gone, and many valuable findings and technologies will spin off from it anyhow. After all, one has to exaggerate to motivate and account for resource allocation in societies like ours.

I believe that science will fare better if it goes for the (sometimes 'awful' or complicated) truth in the long run and not for marketable promises. It should be made clear to the public at large what the stakes and realistic prospects are, and what the risks of funding are, rather than trumpeting out vague claims which deceive and serve expectations rather than inform. In the public interest, as well as for scientific progress, funding agencies and scientific organizations need to allocate more space, time and resources to 'negative' contributions (Mueck 2013) which are critical about feasibility and status, in particular when it comes to conference contributions and publications.

Let me finally express one opinion about a research area that I find positively necessary to finance: nuclear fusion research. In view of the energy crisis that will affect and deeply transform our societies in the not-so-distant future, we need to make sure that we have sufficient electric energy deployable which could eventually substitute the depleting oil reserves. I believe it is not overstated that despite the tremendous challenges and obstacles in physics and material science of this prospective technology, thermonuclear fusion reactors could provide us with the energy our societies need, accompanied with sustainably bearable side effects. At the moment, the two formidable problems — creating an environment for fusion as well as being able to thermalize the energy released during fusion in a sustainable manner — might require a commitment that goes far beyond the € 1 billion input into the quantum technologies flagship initiative in quantum technology discussed here. But, as this might become a necessity rather than a convenience in the medium-term future, we should spend 'whatever it takes' to accomplish this energy goal, regardless of the price of energy today, thereby transforming the petrochemical industry, as well as our societies at large, into entities that could survive and prosper during and after the upcoming energy crisis.

Acknowledgements. This work was supported in part by the European Union, Research Executive Agency (REA), Marie Curie FP7-PEOPLE-2010-IRSES-269151-RANPHYS grant. Responsibility for the information and views expressed in this article lies entirely with the author. The content therein does not reflect the official opinion of the Vienna University of Technology or the University of Auckland. The author declares no conflict of interest and, in particular, no involvement in nuclear fusion research.

LITERATURE CITED

Abbott AA, Calude CS, Svozil K (2015) A variant of the Kochen-Specker theorem localising value indefiniteness. J Math Phys 56:102201

Bell J (1990) Against 'measurement'. Phys World 3:33–41

Bennett CH, Brassard G (1984) Quantum cryptography: public key distribution and coin tossing. In: Proc IEEE Int Conf Comput, Systems, and Signal Processing, Bangalore, India, 9–12 Dec 1984. IEEE Computer Society Press, p 175–179. http://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf

Bergia S, Cannata F, Cornia A, Livi R (1980). On the actual measurability of the density matrix of a decaying system by means of measurements on the decay products. Found Phys 10:723–730

Bernstein E, Vazirani U (1993). Quantum complexity theory. In: Proc 25th Annu ACM Symp Theory Computing, San Diego, CA, 16–18 May 1993. ACM, New York, NY, p 11–20

Born M (1926) Zur Quantenmechanik der Stoßvorgänge. Zeitschrift für Physik 37:863–867

de Touzalin A, Marcus C, Heijman F, Cirac I, Murray R, Calarco T (2016). Quantum manifesto. A new era of technology. http://qurope.eu/system/files/u7/93056_Quantum%20Manifesto_WEB.pdf (accessed on 23 May 2016)

Donath N, Svozil K (2002). Finding a state among a complete set of orthogonal ones. Phys Rev A 65:044302

Englert BG, Schwinger J, Scully MO (1988) Is spin coherence like Humpty-Dumpty? I. Simplified treatment. Found Phys 18:1045–1056

European Commission (2016a) European commission will launch € 1 billion quantum technologies flagship. https://ec.europa.eu/digital-single-market/en/news/european-commission-will-launch-eu1-billion-quantum-technologies-flagship

European Commission (2016b) Quantum technologies. https://ec.europa.eu/digital-single-market/en/quantum-technologies (accessed on 23 May 2016)

Everett H III (1957) 'Relative state' formulation of quantum mechanics. Rev Mod Phys 29:454–462

Farhi E, Goldstone J, Gutmann S, Sipser M (1998) Limit on the speed of quantum computation in determining parity. Phys Rev Lett 81:5442–5444

Feynman R (1965) The character of physical law. MIT Press, Cambridge, MA

Gavinsky D (2016) Entangled simultaneity versus classical interactivity in communication complexity. In: Proc 48th

Annu ACM SIGACT Symp Theory of Computing, STOC 2016, Cambridge, MA, 18–21 Jun 2016, p 877–884

IBM (International Business Machines Corporation) (2016) Charles Bennett — a founder of quantum information theory. https://www.youtube.com/watch?v=9q-qoeqVVD0 (accessed on 16 July 2016)

Jaynes ET (1989) Clearing up mysteries — the original goal. In: Skilling J (ed) Maximum-entropy and Bayesian methods. Proc 8th Max Entropy Workshop, 1–5 Aug 1988, Cambridge. Kluwer, Dordrecht, p 1–28. http://bayes.wustl.edu/etj/articles/cmystery.pdf

Jaynes ET (1990) Probability in quantum theory. In: Zurek WH (ed) Complexity, entropy, and the physics of information. Proc 1988 Workshop on Complexity, Entropy, and the Physics of Information, Santa Fe, NM, May–Jun 1989. Addison-Wesley, Reading, MA, p 381–404 http://bayes.wustl.edu/etj/articles/prob.in.qm.pdf

Jordan S (2011–2016) Quantum algorithm zoo. http://math.nist.gov/quantum/zoo/ (accessed on 16 July 2016)

Mermin DN (1998) What is quantum mechanics trying to tell us? Am Phys 66:753–767

Montanaro A (2011) A new exponential separation between quantum and classical one-way communication complexity. Quantum Inf Comput 11:574–591

Montanaro A (2016) Quantum algorithms: an overview. npj Quantum Inf 2:15023

Mueck L (2013) Report the awful truth! Nat Nanotechnol 8: 693–695

Nielsen MA (2016) Blog. http://michaelnielsen.org/blog/michael-a-nielsen/ (accessed on 23 May 2016)

Pitowsky I (1998) Infinite and finite Gleason's theorems and the logic of indeterminacy. J Math Phys 39:218–228

Raz R (1999) Exponential separation of quantum and classical communication complexity. In: Proc 31st Annu ACM Symp on Theory of Computing, STOC '99, New York, NY, p 358–367

Seevinck MP (2010) Can quantum theory and special relativity peacefully coexist? Technical report. http://arxiv.org/abs/1010.3714

Shi Y (2003) Both Toffoli and controlled-NOT need little help to do universal quantum computing. Quantum Inf Comput 3:84–92

Svozil K (2002) Quantum information in base *n* defined by state partitions. Phys Rev A 66:044306

Svozil K (2004) Quantum information via state partitions and the context translation principle. J Mod Opt 51:811–819

Svozil K (2006) Staging quantum cryptography with chocolate balls. Am J Phys 74:800–803

Svozil K (2014) Unscrambling the quantum omelette. Int J Theor Phys 53:3648–3657

Svozil K (2016) Orthogonal vector computations. Entropy 18: 156

Yanofsky NS (2003) A universal approach to self-referential paradoxes, incompleteness and fixed points. Bull Symbolic Logic 9:362–3867

Zeilinger A (1999) A foundational principle for quantum mechanics. Found Phys 29:631–643

Editorial responsibility: Michael C. Thorne, Halifax, UK

Submitted: July 6, 2016; Accepted: August 30, 2016
Proofs received from author(s): October 29, 2016