

Hypercomputation and the Grand Challenge in Non-Classical Computation

Susan Stepney

Department of Computer Science, University of York, UK

Abstract

The UK Computing Research Committee has initiated the Grand Challenges in Computing Research exercise. One of the Grand Challenges constituted as a result of this call is “Journeys in Non-Classical Computation”. Its goal is to create a fully mature science of *all* forms of computation, that unifies the classical and non-classical paradigms. Along the way, it seeks to challenge many classical computational paradigms, including the Turing paradigm. This position paper outlines the role that hypercomputation research could play in support of the Challenge.

Overview

Today’s computing, *classical* computing, is an extraordinary success story. However, there is a growing appreciation that it encompasses an extremely small subset of all computational possibilities. There are several standard paradigms that seem to define classical computing, but these may not necessarily be true in *all* computing paradigms. As these paradigms are challenged, the subject area is widened, and enriched. The UKCRC’s Grand Challenge exercise [1] includes the Grand Challenge of Non-Classical Computation (GC-7) [1][2][3][4], which is nothing less than a complete reconceptualisation of computation itself.

GC-7 challenges any classical paradigm that its participants can think of, including ones related to approximate computing, bio-inspired computing, complex dynamical systems, parallel computing, and others[3]. The one of most relevance to hypercomputation is to challenge the Turing paradigm, which treats computation as a purely mathematico-logical construct, independent of the implementing substrate, and independent of the laws of physics. As Deutsch [5] neatly sums it up:

Turing hoped that his abstracted-paper-tape model was so simple, so transparent and well defined, that it would not depend on any assumptions about physics that could conceivably be falsified, and therefore that it could become the basis of an abstract theory of computation that was independent of the underlying physics. ‘He thought,’ as Feynman once put it, ‘that he understood paper.’ But he was mistaken. Real, quantum-mechanical paper is wildly different from the abstract stuff that the Turing machine uses. The Turing machine is entirely classical

The Turing machine is based on concepts consistent with Newtonian physical laws, and on “disembodied” mathematical abstractions that, for example, require unbounded memory resources and ignore power consumption. But the world is not Newtonian, and all computation is physically embodied in devices whose behaviour cannot be completely captured by a closed mathematical model. The mathematical model of the Turing Machine is not an adequate model for all notions of computation.

Laws of physics

We know that exploitation of *quantum superposition* makes a difference to computational efficiency. Certain quantum random walk algorithms are exponentially faster than their classical counterparts; see [6] for an overview. (Shor’s quantum factorisation algorithm is

polynomial time complexity [7], whereas the best known classical one is exponential, but it is not known if there is a polynomial time classical algorithm.) Other quantum effects can lead to results simply not possible classically. For example “wavefunction collapse” makes genuine random number generation possible [8], and *quantum entanglement* can be exploited to achieve untappable communication channels, dense coding, and information teleportation [9]. It is not all gain, however: quantum information cannot be cloned [10], leading to interesting problems in developing quantum error-correcting codes [11], among other things.

To emphasize further the critical importance of the underlying physical laws, it has been shown that the deep unsolved conundrum of whether $P = NP$ is answerable, in the affirmative, *if the laws of quantum mechanics are non-linear* [12]. The fact that the precise form of the laws of physics have an impact on what is classically thought to be a purely *mathematical* question is considerable food for thought.

We know some of the consequences of considering computation in a world that includes quantum mechanics? What are the consequences of considering it in a world that includes special and general relativity? And these theories of non-classical physics are by now a century old. What will be the computational consequences of, say, string theory or loop quantum gravity?

What about the “non-elementary” laws of physics? Solid-state physics teaches us that *more is different* [13], and that new higher-level laws of physics “emerge” from large collections of particles. How might these ideas and results give new higher-level concepts of computation and information?

Physical embodiment

Even in the everyday classical physical world, the importance of embodiment can turn up in strange places. For example, a computation, being embodied, takes time to execute, and consumes power as it executes, usually in a data-dependent manner. These time and power consumption *side-channels* can be measured and analysed. (Such analyses have been used to attack the security mechanisms of certain smart cards, for example [14][15].) Side channels are outside the classical mathematical model of computation. Even if these channels are explicitly modelled, the world is open, and further side channels always exist: no mathematical model of the world is complete. As we broaden the base of physical laws on which we base our computations, such side-channels may themselves become rich computational resources.

The role of hypercomputation

The study of hypercomputation seeks to discover computational devices that somehow break the Turing paradigm. Quantum computers have already shown that algorithm *feasibility* depends on the laws of physics. Does what is *computable* similarly depend on them?

Attempts to use relativistic devices to solve the Halting Problem all seem to run into some form of “ultraviolet catastrophe”. As the program runs ever faster (to perform infinite Turing computation in finite elapsed time [16]), the outputs get closer together and more energetic in the observer’s reference frame, until the observer is fried! (Does Shor’s algorithm suffer an “infra-red catastrophe”? When do the exponentially decreasing magnitude rotations become too small to physically implement?)

When we move from the mathematical to the physical domain to analyse our computations, we need to take into account much more infrastructure: the self-same laws of physics that

provide more computational power also constrain our ability to measure the outputs of our new exotic devices. So, even if we develop theoretical hypercomputers, we may not be able to build them. But this should not worry us, for we can't build a Turing machine either. Unbounded memory is unphysical. Even if hypercomputers don't, or can't exist, their study will help enrich our understanding of what computation is, and what its limits are, and why.

Enriching computation

Classical physics did not disappear when modern physics came along: rather its restrictions and domains of applicability were made explicit, and it was reconceptualised. Similarly, these various forms of *non-classical computation* – embodied computation, bio-inspired algorithms, open complex adaptive systems, and more – will not supersede classical computation: they will augment and enrich it. In the process, classical computation will inevitably be reconceptualised. The Grand Challenge in Non-Classical Computation seeks to explore, generalise, and unify all these many diverse non-classical computational paradigms, to produce **a fully mature and rich science of all forms of computation, that unifies the classical and non-classical computational paradigms.**

Such a mature computational science will allow us to design and build robust, adaptable, powerful, safe, complex computational systems. It will help researchers to uncover deep physical truths: what is the relationship between logical information (bits) and physical reality?

References

- [1] UKCRC Grand Challenge website: http://www.ukcrc.org.uk/grand_challenges/index.cfm
- [2] GC in Non-Classical Computation website: <http://www.cs.york.ac.uk/nature/gc7/>
- [3] S. Stepney, S. L. Braunstein, J. A. Clark, A. Tyrrell, A. Adamatzky, R. E. Smith, T. Addis, C. Johnson, J. Timmis, P. Welch, R. Milner, D. Partridge. Journeys in Non-Classical Computation I: A Grand Challenge for computing research. *Int. J. Parallel, Emergent and Distributed Systems* **20**(1):5–19, 2005
- [4] S. Stepney, S. L. Braunstein, J. A. Clark, A. Tyrrell, A. Adamatzky, R. E. Smith, T. Addis, C. Johnson, J. Timmis, P. Welch, R. Milner, D. Partridge. Journeys in Non-Classical Computation II: Initial journeys and waypoints. *Int. J. Parallel, Emergent and Distributed Systems*. **21**(2):97–125, 2006
- [5] David Deutsch. *The Fabric of Reality*. Penguin. 1997
- [6] J. Kempe. Quantum random walks: an introductory overview. *Contemporary Physics* **44**(4):307–327, 2003
- [7] P. W. Shor. Polynomial-time algorithms for prime number factorization and discrete logarithms on a quantum computer. *SIAM J. Comp.* **26**(5):1484–1509, 1997
- [8] Quantum random number download website: <http://www.randomnumbers.info/>
- [9] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70**:1895–1899, 1993
- [10] W. K. Wootters, W. H. Zurek. A Single Quantum Cannot be Cloned. *Nature* **299**:802–803, 1982
- [11] A. R. Calderbank, P. W. Shor. Good quantum error-correcting codes exist. *Phys Rev A*. **54**(2):1098–1105, 1996
- [12] D. S. Abrams, S. Lloyd. Nonlinear quantum mechanics implies polynomial-time solution for NP-complete and #P problems. *Phys. Rev. Lett.* **81**:3992–3995, 1998
- [13] P. W. Anderson. More is different. *Science* **177**:293–296, 1972
- [14] P. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. *Crypto '96*, LNCS 1109, Springer, 1996
- [15] P. Kocher, J. Jaffe, B. Jun. Differential Power Analysis. *Crypto '99*, LNCS 1666, Springer, 1999
- [16] M. Hogarth. Does General Relativity allow an observer to view an eternity in a finite time. *Foundations of Physics Letters* **5**:73–81, 1992