On quantum hypercomputation

Tien D. Kieu*
Centre for Atom Optics and Ultrafast Spectroscopy,
ARC Centre of Excellence for Quantum-Atom Optics,
Swinburne University of Technology, Hawthorn 3122, Australia
(Dated: August 21, 2006)

Quantum computation has attracted much attention and investment lately through its theoretical potential to speed up some important computations as compared to classical Turing computation. The most well-known and widely-studied form of quantum computation is the (standard) model of quantum circuits [1] which comprise several unitary quantum gates (belonging to a set of universal gates), arranged in a prescribed sequence to implement a quantum algorithm. Each quantum gate only needs to act singly on one qubit (quantum bit), a quantum generalisation of the classical bit, or on a pair of qubits.

In view of this promising potential of quantum computation, another question then inevitably arises is whether the class of Turing computable functions can be extended by applying quantum principles. This kind of computation beyond the Turing barrier is also known as hypercomputation [2]. Initial efforts [3] have indicated that quantum computability is the same as classical computability. However, this negative conclusion is only valid for the standard quantum computation; but the standard model is not the only model of quantum computation. Nor does it necessarily exploit fully the principles of quantum mechanics.

As an illustration of the ability of quantum mechanics, a truly random sequence of bits could be easily generated from a qubit initially prepared in a certain state, while Turing machines have to be content with only pseudo-random generators (see, for example, [4]). (Thus, it seems from the view point of Algorithmic Information Theory [5] that a finitely prepared qubit can have an infinite algorithmic informational theoretic complexity as compared to any finite Turing machine!) This ability to generate random numbers could thus be seen as a form of hypercomputation – albeit of some very limited application and of a nature which is non-harnessible or non-exploitable for universal computation.

Also not being restricted by the standard model of quantum computation, we have claimed [6, 7, 8, 9, 10] to have a quantum algorithm for Hilbert's tenth problem [11] despite the fact that the problem has been shown to be recursively noncomputable. The algorithm makes essential use of the Quantum Adiabatic Theorem (QAT) [12] and other results in the framework of Quantum Adiabatic Computation (QAC) [13], subject to some predetermined and arbitrarily small probability of error. We name this kind of algorithms *Probabilistically Correct Algorithms* to emphasise the fact that the end results from such algorithms are subject to some *probabilities of being incorrect.* Such error probabilities are necessary when there is, in principle, no other way to verify all the outcomes of the algorithms.

We should note here that there is a whole hierarchy of the noncomputables [14]; that is, some are more 'noncomputable' than others. Computability of certain noncomputable, if could be ascertained, does not mean that *all* the noncomputables are then computable. Our claim of (quantum) computability is restricted in that sense, it is only applied to Hilbert's tenth problem, or equivalently the Turing halting problem, or any equivalent problem.

What constitutes, in particular, the noncomputability of Hilbert's tenth problem? For each Diophantine equation without any parameter, there is nothing noncomputable about whether that particular equation has any integer solution or not. If we have not yet had a (recursive) procedure to obtain that answer then it does not mean that such a procedure is ever out of reach.

Nor there is anything noncomputable about a collection of *finitely* many Diophantine equations, because we can always concatenate all the procedures for all the equations (as there is always a procedure in principle to determine the existence of solution for each equation) into a *finitely* collective procedure that can be applied to the whole collection.

What constitutes the noncomputability of Hilbert's tenth problem is the fact that we ask for

*Electronic address: kieu@swin.edu.au

a *single* finite procedure which can be applied to all the elements of sets of *countably* many Diophantine equations. The application of Cantor's diagonal arguments to the Turing hating problem, see for example [15], has established that were there a finite and recursive Turing machine that can be applied to determine the halting of, or lack of, any Turing machine then contradiction and inconsistency would have to follow. What that means for Hilbert's tenth problem is that there is *no* single finite recursive algorithm for *all* Diophantine equations, but for each given equation we have to find a recursive algorithm *anew* each time.

In those regards, noncomputability is similar to the concept of randomness; there is nothing random about a *single* bit or number by itself. (The notion of randomness only applies to a series of such bits or numbers which does not have any statistical pattern or, if we appeal to algorithmic information theory, does not have a pattern which can be encoded more effectively and economically than the length of the series.)

To illustrate that Cantor's arguments cannot rule out hypercomputation (for a general discussion on this issue, see [15]), we have pointed out that the probabilistic arguments of our algorithm can avoid the usual Cantor's arguments and thus leads to no contradiction. Nor there would be any contradiction if our quantum algorithm cannot be encoded with a Gödel integer. And this is how we could reconcile the quantum adiabatic algorithm with Cantor's diagonal arguments in a consistent manner. Certainly the probabilistic nature of the algorithm is not sufficient to imply that it is hypercomputational. For that, we have had to construct and show explicitly that it could, as a single algorithm, resolve any instance of Hilbert's tenth problem.

Since our first proposal in 2001 of an algorithm employing quantum adiabatic processes to render the classically noncomputable Hilbert's tenth problem into that of a quantum mechanically computable [6, 8, 9, 10], there have been a lot of interests as well as criticisms. That situation is inevitable for such seemingly radical a claim against the accepted and accustomed wisdom. It is also a natural and healthy state of scientific research wherein all new proposals must be subjected to rigorous examination against what is currently known. In our case, however, most of the criticisms are not in the formal literature but only in informal discussions in private or on internet forum and at the many seminars and conference presentations that we have given. We have tried to collect all the criticisms known to us and evaluate them one by one, for instance, in one of our recent postings [16], see also [17, 18] in response to [19], and [20] in response to [21].

We make the distinction between the algorithm itself and its physical implementation. Against the algorithm, most of the criticisms are just misunderstandings. We have also discussed the question of physical implementation of the algorithmin in more details in [16].

People often are puzzled by the apparent ability of the quantum algorithm to *explore an infinite space in a finite time*. That puzzlement comes from a simplistic expectation that in order to determine whether a Diophantine equation has any solution or not one would have to explore the *whole* integer space. Such an exploring task apparently could not be accomplished in a finite time in the case the equation has no solution at all. As a matter of fact, the expectation is too simplistic and not quite correct. Were it correct then we would easily be able to, and certainly not need the sophisticated Davis-Putnam-Robinson-Matiyasevich theorem [11] and then Cantor's diagonal arguments, to establish the noncomputability of Hilbert's tenth problem. The fact of the matter is for each Diophantine equation we only need to explore a *finite* domain in the space of appropriate tuples of integers; the equation has a solution *if and only if* the solution resides in that finite domain (bounded by the so-called test function, see Davis [22]). This property is quite remarkable and is applicable to a wider class of so-called *finitely refutable* problems, see a theorem in [23]. Once such a finite domain is known for a Diophantine equation, it is just a matter of substitution of a finite number of integers to determine if the equation has any solution at all. The noncomputability of Hilbert's tenth problem comes from the fact that there can be no *single* finite recursive procedure to determine such a finite domain for each and every Diophantine equation. There must be, in other words, at least one Diophantine equation that is not susceptible to the treatment of any given recursive procedure.

On the other hand, we claim that a single quantum adiabatic procedure, as described by the quantum algorithm, can be applied to each and every equation. Surely, in a finite time the quantum mechanical (normalisable) wave function can only spread out from its initial wave form to explore an effectively finite domain of the underlying Hilbert space. But the domain so explored is the relevant domain sufficient for the purpose of finitely refuting or confirming the existence of solution for the equation. The finitely refutable character of Hilbert's tenth problem manifests itself in the quantum algorithm as the finiteness in the energy of the final ground state and in the time that this ground state can be obtained and identified (by our identification criterion via a probability measure [18]).

One should not and cannot use Grover's search algorithm [24] in an unstructured database to erroneously imply that quantum adiabatic computation cannot search more efficiently than the time complexity offered by Grover's algorithm (which is of the order of the square root of the database size) and thus cannot compute Hilbert's tenth problem. Such a comparison is misleading and incorrect in at least three aspects. Firstly, quantum adiabatic computation could accomplish the search in a time *independent* of the size of the database, provided sufficient energy must be supplied, see the references [25, 26, 27, 28]. The energy, secondly, need not be proportional to the square root of the database size, quantum entanglement can reduce substantially the required energy, as demonstrated in a quantum adiabatic algorithm for the NP-complete travelling salesman problem [28]. And thirdly, for any instance of Hilbert's tenth problem, as we only need to search in a finite domain appropriate for the specific parameter-free equation under consideration thanks to the finitely refutable property, both the energy required and the time taken are *finite* for a successful execution of the quantum algorithm in the infinite underlying Hilbert space. Some finite information about the final ground state is that all we could have, there is no infinite amount of information here.

In short, one should not think that Hilbert's tenth problem is the same as a search problem in an unstructured and infinite database. While the latter unstructured search problem is quite general and difficult, each parameter-free Diophantine instance of Hilbert's tenth problem *does* provide some structure, which is the information mathematically encoded in the equation itself. Furthermore, the search space for such a minimum is always finite. To highlight possible pitfalls of a simplistic comparison with unstructured search, let us consider the counterpart of Hilbert's tenth problem over the real numbers, that is, the question of a single universal procedure to determine the existence or lack of *real* solution for any given multivariate polynomial with *real* coefficients. Were the brute-force approach of unstructured search in the real numbers the only one available, one would have concluded that this would be another noncomputable problem because such a search in an infinite space of the reals, which is even 'larger' in cardinality than that of the integers, could have never been completed in a finite time. On the contrary, and perhaps fortunately, such a conclusion is wrong: Tarski showed that [29], unlike Hilbert's tenth problem, this counterpart problem is classical *computable* – thanks to the mathematical structures encoded in the polynomials themselves.

Metaphorically speaking, the initial ground state of the quantum algorithm provides one end of a *finite* string along which we can trace to the final ground state at the other end. This can be done quantum mechanically because of the quantum adiabatic theorem, which asserts that a particular eigenstate of a final-time Hamiltonian, even in dimensionally *infinite* spaces, could be found mathematically and/or physically *in a finite time*. This is a remarkable property, which is enabled by quantum interference and quantum tunneling with complex-valued probability amplitudes, and in principle allows us to find a needle in a particular infinite haystack! Such a property is clearly *not* available for classical recursive search in an unstructured infinite space. Being built on these principles, our algorithm is far from being a simple brute-force search.

The central issue here is the physical implementations of the algorithm. To argue that the assumption that the Hamiltonians of the quantum algorithm cannot be effectively constructed due to a lack of infinite precision may not be a forgone conclusion, we emphasise the virtually unknown fact that, on the contrary, simple instances of Diophantine equations with apparently *infinitely precisely* integer coefficients have *already* been realised in certain experiments known as quantum phase transitions (in the so-called Bose-Hubbard model)! We have also speculated on how central limit theorem might be of some help in the effective implementation of the required Hamiltonians.

Our ultimate objective is to obtain the ground state of a desired Hamiltonian, and the algorithm is 'just' a means to that end, but a universal means nevertheless. In saying that the negative resolution of Hilbert's tenth problem of the (platonic) mathematical world also carries over to the physical world in such a way that we could never achieve the above objective is equivalently to saying that we would never be able either to identify some ground states, or to construct some suitable Hamiltonians, or both. That would be a very powerful and stringent constraint on the physical world and would have resulted in an entirely new physical principle – but we do not have any reason or anything to support this negative conclusion.

We, as yet, have absolutely no 'no-go' physical principles which dictate that there must exist a physical system which we cannot cool down to the ground state, or in which there must exist a physical limit of a distinctively non-zero temperature beyond which we cannot proceed any further. The third law of thermodynamics, and its generalisation to the quantum domain, only states that we should not be able to obtain exact absolute zero temperature, or equivalently, that we should not be able to obtain a ground state with total certainty, but that is fine as we do not need to obtain a ground state with unity probability in order to identify it. But the third law does not demand that there must be a non-zero lower bound on achievable temperature, or equally, that there must be an upper bound of obtainable probability for a ground state. (If anything, the postulate of projective measurement in standard quantum mechanics may contradict some classical statement of the third law.)

Computability should constitute of both consistency and also implementability. However, the issue of implementability can only be settled either in the negative by citing prohibiting physical principles, of which there is none known at present, or in the positive by actual and general demonstrations, of which there are so far only special cases connected to certain quantum phase transitions. The awaited final outcome must and can only be bounded by physical laws. Until it is settled one way or another, it should be remembered that premature and prejudiced judgement has never served us well.

Acknowledgments

I wish to thank Peter Hannaford and Toby Ord for support and discussions. This work has also been supported by the Swinburne University Strategic Initiatives.

[1] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, Cambridge, 2000.
[2] J. Copeland. Hypercomputation. *Minds and Machines*, 12:461–502, 2002.
[3] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM J. Comp.*, 26:1411, 1997.
[4] M. Stannett. Hypercomputation is experimentally irrefutable. Sheffield University Department of Computer Science Report TR CS-01-04, 2001.
[5] G.J. Chaitin. *Algorithmic Information Theory.* Cambridge University Press, Cambridge, 1987.
[6] T.D. Kieu. Computing the non-computable. *Contemporary Physics*, 44:51–77, 2003.
[7] T.D. Kieu. Numerical simulations of a quantum algorithm for Hilbert's tenth problem. In Eric Donkor, Andrew R. Pirich, and Howard E. Brandt, editors, *Proceedings of SPIE Vol. 5105 Quantum Information and Computation*, pages 89–95. SPIE, Bellingham, WA, 2003.
[8] T.D. Kieu. Quantum adiabatic algorithm for Hilbert's tenth problem: I. The algorithm. `ArXiv:quant-ph/0310052`, 2003.
[9] T.D. Kieu. Quantum algorithms for Hilbert's tenth problem. *Int. J. Theor. Phys.*, 42:1451–1468, 2003.
[10] T.D. Kieu. A reformulation of Hilbert's tenth problem through quantum mechanics. *Proc. Roy. Soc.*, A 460:1535–1545, 2004.
[11] Y.V. Matiyasevich. *Hilbert's Tenth Problem.* MIT Press, Cambridge, Massachussetts, 1993.
[12] A. Messiah. *Quantum Mechanics.* Dover, New York, 1999.
[13] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser. Quantum computation by adiabatic evolution. `ArXiv:quant-ph/0001106`, 2000.
[14] Hartley Rogers. *Theory of Recursive Functions and Effective Computability.* McGraw-Hill, New York, 1967.
[15] T. Ord and T.D. Kieu. The diagonal method and hypercomputation. *Brit. J. Phil. Sci.*, 56:147–156, 2005.
[16] T.D. Kieu. Mathematical computability questions for some classes of linear and non-linear differential equations originated from Hilbert's tenth problem. `arXiv:math.GM/0507109`, 2005.
[17] T.D. Kieu. On the identification of the ground state based on occupation probabilities: An investigation of Smith's apparent counterexample. `arXiv:quant-ph/0602145`, 2006.
[18] T.D. Kieu. A mathematical proof for a ground-state identification criterion. `arXiv:quant-ph/0602146`, 2006.
[19] Warren D. Smith. Three counterexamples refuting Kieu's plan for "quantum adiabatic hypercomputation"; and some uncomputable quantum mechanical tasks. http://math.temple.edu/w̃ds/homepage/works.html, #85, 2005.

[20] T.D. Kieu. Reply to Andrew Hodges. `arXiv:quant-ph/0602214v2`, 2006.
[21] Andrew Hodges. Can quantum computing solve classically unsolvable problems? `arXiv:quant-ph/0512248`, 2005.
[22] Martin Davis, Yuri Matiyasevich, and Julia Robinson. Hilbert's tenth problem. Diophantine equations: Positive aspects of a negative solution. *Proceedings of Symposia in Pure Mathematics*, 28:323–378, 1976.
[23] C.S. Calude. *Information and Randomness: An Algorithmic Perspective*. Springer-Verlag, Berlin Heidelberg, 2nd edition, 2002.
[24] L.K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 79:325–328, 1997.
[25] Recep Eryigit, Yigit Gunduc, and Resul Eryigit. Local adiabatic quantum search with different paths. `arXiv:quant-ph/0309201`, 2003.
[26] Saurya Das, Randy Kobes, and Gabor Kunstatter. Energy and efficiency of adiabatic quantum search algorithms. *J. Phys. A: Math. Gen.*, 36:1–7, 2003.
[27] Zhaohui Wei and Mingsheng Ying. Quantum search algorithm by adiabatic evolution under a priori probability. `arXiv:quant-ph/0412117`, 2004.
[28] T.D. Kieu. Quantum adiabatic computation and the travelling salesman problem. `arXiv:quant-ph/0601151`, 2006.
[29] Alfred Tarski. *A Decision Method for elementary Algebra and Geometry*. University of California Press, Berkeley Los Angeles, second edition, 1951.