Quantum Hypercomputation

TIEN D. KIEU
Centre for Atom Optics and Ultrafast Spectroscopy, Swinburne University of Technology, Hawthorn, Victoria 3122, Australia; E-mail: kieu@swin.edu.au

Abstract. We explore the possibility of using quantum mechanical principles for hypercomputation through the consideration of a quantum algorithm for computing the Turing halting problem. The mathematical noncomputability is compensated by the measurability of the values of quantum observables and of the probability distributions for these values. Some previous no-go claims against quantum hypercomputation are then reviewed in the light of this new positive proposal.

Key words: Hilbert's tenth problem, quantum adiabatic theorem, quantum computation

> When we resolve a paradox, we do not decide in favor of one of the conflicting arguments and against the other; rather, we bring out the precise truth of each in order to show they do not conflict on the same ground.
>
> Michael Scriven (1964)

> ...we would be profoundly surprised if the physics of the real world can be properly and fully set out without departing from the set of Turing-machine-computable functions... In short it would – or should – be one of the greatest astonishments of science if the activity of Mother Nature were never to stray beyond the bounds of Turing-machine-computability.
>
> B.J. Copeland and R. Sylvan (1999)

1. Introduction

Ever since the inception of the universal Turing computer – simple but yet encompassingly powerful – there have been continuing efforts to understand its power and its limitations and to extend computation beyond such limitations.

Supported by the convergence of many seemingly different models of computation put forward independently by different people – Turing, Post, Markov and others (Lewis and Papadimitriou, 1981) – a thesis regarding the limits of computability has been framed and has gained much credibility. The Church-Turing thesis can be phrased as

> Every function which would naturally be regarded as computable can be computed by a universal Turing machine.

Minds and Machines **12:** 541–561, 2002.

This thesis is similar to a scientific/physical theory in that both can be proved wrong with newly gathered evidence but can never be proved right just by logic alone – a fact pointed out by Popper for all scientific theories.

The thesis imposes an upper limit on what any computing machine can be designed to do: no more than the universal Turing machine, it asserts. The support the thesis has is the convergence of many, in fact all, (apparently different) classical computation models. Could the reason for this convergence be that all these models share the same mathematical foundation – classical logic? If it is then two implications would follow immediately: (i) the limit of computability expressed by the thesis is also a manifestation of the limit of classical logic itself, and (ii) to push the notion of computability any further, one would have to move beyond classical logic.

Can the notion of computability be enlarged? In principle, there is no reason why not. Proposals to overcome the Turing-machine limit range from models of mathematical principles, such as continuous valued neural networks (Siegelmann, 1995) and DNA computing (Calude and Paun, 2001a), to those of a physical nature based on general arguments (Stannett, 2001), relativity principles, and quantum mechanical principles (Calude and Pavlov, 2001b; Kieu, 2001a; Nielson, 1997).

In this paper we outline a quantum algorithm for the classically noncomputable Turing halting function.

2. Noncomputability in Mathematics

2.1. The Turing halting problem

A version of the proof of the unsolvability of the halting problem based on the Cantor diagonal argument goes as follows. The proof is by contradiction with the assumption of the existence of a computable halting function $h(p, i)$ which has two integer arguments - p is the Gödel encoded integer number for the algorithm and i is its (encoded) integer input:

$$h(p, i) = \begin{cases} 0 & \text{if } p \text{ halts on input } i \\ 1 & \text{if } p \text{ does not} \end{cases} \tag{1}$$

One can then construct a program $r(n)$ having one integer argument n in such a way that it calls the function $h(n, n)$ as a subroutine and

$$\begin{cases} r(n) \text{ halts if } h(n, n) = 1 \\ r(n) \text{ loops infinitely (i.e., never stops) otherwise.} \end{cases}$$

An example in pseudo code for such an $r(n)$ is

```
      PROGRAM r
      INPUT n
 10   CALL h(n, n)
      IF h(n, n) = 0 GOTO 10
      END
```

The application of the halting function h to the program r and input n results in

$$h(r, n) = \begin{cases} 0 & \text{if } h(n, n) = 1 \\ 1 & \text{if } h(n, n) = 0 \end{cases} \tag{2}$$

A contradiction is clearly manifest once we put $n = r$ in the last equation above.

The construction of such a program r is transparently possible, unless the existence of a computable h is wrongly assumed. Thus the contradiction discounts the assumption that there is a classically algorithmic way to determine whether any arbitrarily given program with arbitrary input will halt or not.

However, this reduction argument might be avoided if we distinguish and separate the two classes of quantum and classical algorithms. A *quantum* function $qh(p, i)$, similar to the function in Equation (1), can conceivably exist to determine whether any classical program p will halt on any classical input i or not. Then, the contradiction in Equation (2) would be avoided:

- Either because the quantum halting function qh cannot take as an argument the modified program r, which is now of *quantum* character, because it now has the quantum qh as a subroutine. This will be the case if qh can only accept integers while quantum algorithms, with proper definitions, cannot in general be themselves encoded as integers.
- Or because we cannot prepare with infinite precision the qh input which in general can only be represented by real numbers.

In essence, the way we break the self-referential reasoning here, by the differentiation between quantum and classical algorithms, is similar to the way Russell's paradox (to do with "The set of all sets which are not members of themselves") is solved by the introduction of classes as distinct from sets. (For other lines of argument, see Calude and Pavlov, 2001b; Siegelmann, 1995; Stannett, 2001, for example.)

2.2. Relation to Hilbert's tenth problem

Identities between polynomials with integer coefficients in several unknowns over the natural numbers have been studied for some time in mathematics under the name of Diophantine equations. At the turn of the last century, David Hilbert listed, as challenges for the new century, 23 important problems. Problem number 10 is a decision problem and could be rephrased as:

> Given any polynomial equation with any number of unknowns and with integer coefficients (that is, any Diophantine equation): To devise a universal process according to which it can be determined by a finite number of operations whether the equation has integer solutions.

As a matter of fact, it suffices to restrict the search to non-negative integer solutions for Diophantine equations.

There are only a few special classes of Diophantine equations that are solvable. These include linear (first-degree) equations in the unknowns, for which the existence and absence of solutions can be inferred from the Euclid's algorithm. Also solvable are second-degree equations with only two unknowns, that is, in quadratic form. But Hilbert asked for a *single* general and finite decision procedure that is applicable to any Diophantine equation. See Davis and Hersh (1973) for a general introduction to Diophantine equations and Hilbert's tenth problem. This problem was shown to be undecidable in 1970 (Davis 1982; Matiyasevich 1993). Hilbert's tenth problem could be solved if and only if the Turing halting problem could also be solved. The two are simply equivalent. Consequently, as we have a proof in the last Section that the Turing's is not solvable, Hilbert's tenth problem is noncomputable/undecidable in the most general sense if one accepts, as almost everyone does, the Church–Turing thesis. One would thus have to be content with the fact that individual Diophantine equations need to be considered separately, with a different approach each time. For a precise discussion and the history of this negative result, see Davis (1982) and Matiyasevich (1993); for a semi-popular account, see Casti (2001).

3. Quantum Principles

3.1. The postulates of quantum mechanics

Quantum Physics, including Quantum Mechanics and Quantum Field Theory, is the most successful theory that we have in Science for the description and prediction of phenomena in Nature. And so far, qualitatively and quantitatively, there is not a single discrepancy between the theory and experiments.

According to Quantum Mechanics (Messiah, 1976), pure states of a physical system can capture all that can be said about the system and are associated with vectors, unique up to phases, in some abstract linear vector Hilbert space. (When the system, particularly when it is a subsystem of a bigger entity, cannot be described by a pure state but is in a mixed state, the language of density matrices would be necessary for its description). Acting on the Hilbert space are linear operators, of which hermitean and unitary operators are of particular interest.

In the Schrödinger picture where the time dependency is explicitly carried by the states, the time evolution of the system is governed by the Schrödinger equation, in which the hermitean Hamiltonian operators play a unique role in governing the dynamics. In general, each physical observable is associated with a hermitean

operator; the Hamiltonian operator, for instance, is associated with the system's energy. The real-valued eigenvalues (which can be continuous or discrete) of these hermitean operators restrict the obtainable values under observation. Each time when the associated observable is measured, only one single value, among the eigenvalues given, is obtained. Repetitions of the measurement under identical conditions could yield different measured values each time. And the probability of getting a particular eigenvalue in a measurement is given by the square of the absolute value of the inner product between the corresponding eigenvector and the state describing the system at that instant. (If the system is in a mixed state described by a density matrix, the probability is then given by the trace of the product between the density matrix and the corresponding projector associated with the eigenvector in question.)

After a measurement, the state of the system is a pure state whose representing vector is the same as the eigenvector, up to a phase, corresponding to the eigenvalue obtained. Note that measurement thus is a non-unitary and irreversible operation in general, unless the system is already in the observable eigenstate. Different observables can be measured simultaneously, with the same degree of statistical accuracy, only when the associated hermitean operators commute with each other.

But already seeded in the summary of quantum mechanical postulates above is a fundamental problem of inconsistency. The act of measurement, on the one hand, is itself a process unfolded in time. On the other hand, why should it not be governed by the unitary Schrödinger time-evolution operator?

We shall not delve into the measurement problem here, except to emphasise that the power of all quantum algorithms in quantum computation relies crucially on such mysterious measurement processes.

Also for later use, we now introduce the concept of *measurable* quantities (Geroch and Hartle, 1986). Analogous to the concept of computable numbers in Section 1, a number w is deemed measurable if there exists a finite set of instructions for performing an experiment such that a technician, given an abundance of unprepared raw materials and an allowed error ϵ, is able to obtain a rational number within ϵ of w. The technician is analogous to the computer, the instructions analogous to the computer program, the "abundance of unprepared raw materials" analogous to the infinite Turing tape, initially blank.

In particular, not only the (stochastic) outcomes of an observable are obviously measurable and of interest but so are the probability distributions for these outcomes. The probabilities can be obtained within any given accuracy by increasing the number of measurement repetitions. Later, we make full use of this crucial fact that *the quantum mechanical probabilities are in principle physically computable, in the sense discussed below, from the theory of Quantum Mechanics.*

3.2. PECULIARITIES OF QUANTUM MECHANICS

One of the most important, but least understood, properties of Quantum Mechanics is the randomness in the outcome of a quantum measurement. Even if we prepare the initial quantum states to be *exactly* the same in principle, we can still have different and random outcomes in subsequent measurements. Such randomness is a fact of life in the quantum reality.

In contrast, mathematical algorithms cannot truly generate random numbers but have to be content with pseudo-random number generators. Interesting arguments given by Stannett (2001) imply that Turing machines that can generate truly random numbers cannot halt. This implication also agrees with the result of Algorithmic Information Theory (Chaitin, 1992) in that there is no finite algorithm for an infinite sequence of random numbers.

To reflect that intrinsic and inevitable randomness of reality, on the other hand, the best that Quantum Mechanics, as a physical theory of nature, can do is to list, given the initial conditions, the possible values for measured quantities and some estimate of the probability distributions for those values. On the other hand, not only the values registered in the measurement of some observable but also the associated probability distributions are measurable in the sense that they can be obtained to any desired accuracy by the act of physical measurement. Normally, the values for measurables are quantised so they can be obtained exactly; the probability distributions are real numbers but can be obtained to any given accuracy by repeating the measurements again and again (each time from the same initial quantum state) until the desired statistics are reached. That is how the calculated numbers from Quantum Mechanics can be judged against the measurable numbers obtained from physical experiments. Thus far, there is no evidence of any discrepancy between theory and experiments.

Randomness is, by mathematical definition, incompressible and irreducible. In Algorithmic Information Theory, Chaitin (1992) defines randomness by program-size complexity: a binary string is considered random when the size of the shortest program that generates that string is not "smaller", as measured in bits, than the size of the string itself. We refer readers to the original literature for more technically precise definitions for the cases of finite and infinite strings.

Paradoxically, the quantum reality of Nature somehow allows us to *compress* the *infinitely incompressible* randomness into the *apparently finite* act of preparing the same quantum state over and over again for subsequent measurements! This quantum mechanically *implied infinity* seems to be both needed for and consistent with the finitely measured, see Kieu (2002) and references therein for further discussion.

The related properties of intrinsic randomness and implied infinity are responsible for the hypercomputational ability of Quantum Mechanics.

3.3. COHERENT STATES

One of the simplest and most widely applied problems in Quantum Mechanics is that of the (one-dimensional) Simple Harmonic Oscillator (SHO) with the Hamiltonian

$$H_{\mathrm{SHO}} = (P^2 + X^2)/2, \tag{3}$$

which can also be expressed as

$$H_{\mathrm{SHO}} = a^\dagger a + \frac{1}{2}. \tag{4}$$

The operators $a^\dagger$, a are linearly related to the position and momentum operators, which satisfy the commutation relation $[P, X] = i$,

$$\begin{aligned} X &= \frac{1}{\sqrt{2}}(a + a^\dagger), \\ P &= \frac{i}{\sqrt{2}}(a - a^\dagger). \end{aligned} \tag{5}$$

The operators $a^\dagger$, a thus satisfy different commutation relations

$$\begin{aligned} &[a, a^\dagger] = 1, \\ &[a, a] = [a^\dagger, a^\dagger] = 0. \end{aligned} \tag{6}$$

The spectrum of the number operator $N = a^\dagger a$ that appears in (4) is discrete and spans over the natural numbers. Its eigenstates are termed the number states $|n\rangle$,

$$N|n\rangle = n|n\rangle; \quad n = 0, 1, 2, \cdots \tag{7}$$

These eigenstates also constitute an orthonormal basis for a Fock space, a special type of Hilbert space, and can be constructed by the operators $a^\dagger$ acting on the special "vacuum" state $|0\rangle$, the lowest-eigenvalue state,

$$|n\rangle = \frac{a^{\dagger n}}{\sqrt{n!}}|0\rangle, \tag{8}$$

from which follow the recursive relations

$$\begin{aligned} a^\dagger|n\rangle &= \sqrt{n+1}|n+1\rangle, \\ a|n\rangle &= \sqrt{n}|n-1\rangle. \end{aligned} \tag{9}$$

These relations lead us to the names *creation* and *annihilation* operators respectively for $a^\dagger$ and a.

The number state $|n\rangle$ can be realised in Quantum Optics as one having a definite number of n photons, all at the same frequency. But these number states are not

the states of travelling optical modes generated by idealised lasers (van Enk and Fuchs, 2001), which have an indefinite number of photons. For the description of these modes (Walls and Milburn, 1995), we need the coherent states $|\alpha\rangle$, which are the eigenstates of a and are labeled by the complex number α,

$$a|\alpha\rangle \;=\; \alpha|\alpha\rangle. \tag{10}$$

With the relation to the number states,

$$\begin{aligned} |\alpha\rangle \;&=\; \mathrm{e}^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \\ &=\; \mathrm{e}^{-\frac{|\alpha|^2}{2}} \mathrm{e}^{\alpha a^\dagger} |0\rangle, \end{aligned} \tag{11}$$

the coherent states are not orthogonal but can still be used for spanning the Hilbert space. They have some unique and nice properties, one of which is that they are the states that optimise the amplitude-phase Heisenberg uncertainty relation. The other fact, which we will exploit later, is that they are also the ground states, i.e. the eigenstates having the lowest "energy" eigenvalues, for the family of semi-definite Hamiltonians

$$H_\alpha \;=\; (a^\dagger - \alpha^*)(a - \alpha). \tag{12}$$

With the simple substitution $b = a - \alpha$ we are back to a family of b-labeled SHO Hamiltonians (3), except for the additive constant, all of which have the same spectrum over the natural numbers but with different sets of eigenvectors $|n_b\rangle$.

3.4. The quantum adiabatic theorem

The dynamical evolution of a quantum system is governed by the Hamiltonian through the Schrödinger equation. If the system is closed then the Hamiltonian is time independent. If the system is subject to external influences, whose dynamics are not of direct concern to the investigation, then the Hamiltonian is time dependent; and the modification in the quantum state of the system critically depends on the time T during which the change of the Hamiltonian takes place. This dependency is particularly simplified when the rate of change of the external fields is very fast compared to some intrinsic time scale, whence we can apply the sudden approximation, or is very slow, whence we can appeal to the quantum adiabatic theorem.

The sudden approximation says that if the time change T is sufficiently fast relative to the inverse of the average Hamiltonian during that time, $\Delta\bar{H}$,

$$T \ll \hbar/\Delta\bar{H}, \tag{13}$$

then the dynamical state of the system remains essentially unmodified.

On the other hand, in the case of an infinitely slow, or adiabatic passage, if the system is initially in an eigenstate of the Hamiltonian at the initial time it will, under certain conditions, pass into the eigenstate of the Hamiltonian at the final time that derives from it by continuity (Messiah, 1976). This is the content of the adiabatic theorem, provided the following conditions are satisfied throughout the relevant time interval:

- The instantaneous eigenvalues remain distinct;
- The first and second derivatives of the instantaneous eigenvectors with respect to time are well-defined and piece-wise continuous.

In the next section, this important theorem is exploited to provide a model of quantum computation involving the ground state.

4. Quantum Computation

The underlying laws of all physical phenomena in Nature, to the best of our knowledge, are those given by quantum physics. However, the best present day computers, as they are of classical nature, cannot even in principle simulate quantum systems efficiently. Feynman pointed that out in 1982, see also Benioff (1980), that only quantum mechanical systems may be able to simulate other quantum systems more efficiently. Furthermore, according to Moore's law, the exponential rate of miniaturisation of micro-electronic semiconductor devices will soon, if it has not already, take us to the sub-micron and nano dimensions and beyond. At this scale, quantum physics will become more and more relevant in the design and production of computer components. Heat dissipation in irreversible computation will be yet another problem at these dimensions. Even though reversible classical computation can be implemented in principle, quantum computation, being almost reversible except the final read-out by measurement, could automatically minimise this heating problem.

It is natural to ask if the notion of effective computability, as classically delimited by the Church–Turing thesis, could be extended via quantum principles. Initial efforts seemed to confirm that quantum computability is no more than classical computability (Bernstein and Vazirani, 1997, 1980; Gandy, 1993). However, more recent indications may prove otherwise (Calude and Pavlov, 2001b; Kieu, 2001a). This is the subject of the investigation below.

4.1. "STANDARD" MODEL OF QUANTUM COMPUTATION

According to the "standard" model of quantum computation (see Nielsen and Chuang (2000) for instance), which is a direct generalisation of classical digital computing, the fundamental unit of a quantum computer is the quantum bit, shortened as *qubit*, which is the generalisation of a binary bit. Physical implementation of a qubit could be any (measurable) two-state system: the up and down values

of a quantum spin, or the two polarisation states of a photon, etc. But unlike the binary bit, a qubit can be in a superposition state of its two states/values. Upon measurement the superposition is destroyed, revealing one of the two classical values of a qubit. The two states of a qubit, denoted by $|0\rangle$ and $|1\rangle$, should be unambiguously distinguishable by measurement and thus be orthogonal to each other.

There are three stages of operation for a quantum computer, corresponding to the input, the processing, and finally the output. The input preparation stage can be and has been carried out in laboratories for certain well-known systems. So can the output stage in which the output is read out by an act of measurement – even though quantum measurement is not that well understood, as already alluded to in Section 3.1. The speed of state preparation and measurement, which should be carried out in such a way as not to perturb other subsystems/qubits not being directly measured, is crucial for quantum computation. The information processing stage is the most difficult to implement. In principle, it is governed by the unitary evolution of a set of qubits well isolated from the surroundings to avoid as much of the decoherence effects of the environment as possible. The discovery of error correcting codes for quantum computation was a pleasant surprise. Without this possibility, realisation of quantum computation would have been unthinkable as computers are inevitably and constantly subject to errors induced by either internal interactions or the environment or both.

The power of a quantum computer lies firstly in the massive parallelism resulting directly from the superposition possibility of the quantum states. If each qubit is a superposition of two states then the measurement of such a superimposed N-qubit system could in general access 2^N distinguished states simultaneously. However, such quantum parallelism is not that useful because of the stochastic nature of the measured outcomes. (After all, many classical wave systems, like water waves, can also have superposition but cannot provide a better computation model.) The second and most important power of quantum computation is thought to have its root in *quantum entanglement* (Bell, 1987), which has no counterpart in the classical world (even though it might be expensively simulated by classical means). Quantum entanglement provides the extra dimensions in information storage and processing that distinguish the quantum from the classical. It is the entanglement that allows us to *control* the massive quantum parallelism through selective interference of different computational paths to extract the information desired.

These characteristics have been exploited to reduce the computational complexity of some problems. So far only a few quantum algorithms have been discovered (Grover, 1997; Shor, 1997); most notable is Shor's factorisation algorithm which employs Quantum Fourier Transformation. It is the only known quantum algorithm that could offer an exponential increase in computational speed, due to the interference of different computation paths (as Fourier Transformation is intimately linked to interference) and due to quantum entanglement.

The approach above with qubits and unitary gates of so-called quantum networks has been accepted as the standard model for quantum computation. It has been argued (Bernstein and Vazirani, 1997; Gandy, 1993) that the computability obtainable in this model is not better but is the same as classical computability.

However, it is not the only model available.

4.2. Quantum adiabatic computation

Among the alternative models for quantum computation is the recent proposal (Farhi et al., 2000) to employ quantum adiabatic processes for computation. The idea is to encode the solution of some problem to be solved into the ground state, $|g\rangle$, of some suitable Hamiltonian, H_P. But as it is easier to implement the Hamiltonian than to obtain the ground state, we should start the computation in a different and readily obtainable initial ground state, $|g_I\rangle$, of some initial Hamiltonian, H_I, then deform this Hamiltonian in a time T into the Hamiltonian whose ground state is the desired one, through a time-dependent process,

$$\mathcal{H}\left(\frac{t}{T}\right) = \left(1 - \frac{t}{T}\right) H_I + \frac{t}{T} H_P. \tag{14}$$

The adiabatic theorem of Quantum Mechanics, Section 3.4, stipulates that if the deformation time is sufficiently slow compared to some intrinsic time scale, the initial state will evolve into the desired ground state with high probability – the longer the time, the higher the probability.

Above are two models of quantum computation, but general quantum computation should not be restricted to those. In the following we exploit quantum principles in the most general way in the consideration of Hilbert's tenth problem.

5. Quantum Algorithm for Hilbert's Tenth Problem

Classically, there is no algorithm for Hilbert's tenth problem. Its noncomputability originates from the lack of a general method to verify a negative statement concerning solutions of a Diophantine equation. By direct substitution into the Diophantine polynomial, it is straightforward to verify whether a set of integers is indeed a zero of the polynomial as it is claimed or not. But it is, however, impossible to mathematically verify *in general* a negative statement that a Diophantine polynomial has no zero. The most general way would be to check *all* the integers themselves; obviously, this is not a finite task and thus is not an implementable algorithm. For a particular equation, such as the Diophantine equation of Fermat's last theorem, one may be able to find a specific way to confirm that the equation has no solution. But that specific way is peculiar and only applicable to the equation in consideration, or some related equations, and not to *any* Diophantine equations in general.

Notwithstanding this, a quantum algorithm has been proposed recently (Kieu, 2001a) for Hilbert's tenth problem. We summarise the main points of the algorithm below.

5.1. PRELIMINARIES

Our strategy is that we do not look for the zeroes of the Diophantine polynomial in question, which may not exist, but instead search within the domain of non-negative integers for the absolute minimum of the square of the polynomial, which always exists and is finite. While it is equally hard to find either the zeroes or the absolute minimum in classical computation, we have converted the problem to the realisation of the ground state of a quantum Hamiltonian and there is no known quantum principle against such an act. In fact, there are no known physical principles against it.

It may appear that even the quantum process can only explore a finite domain in a finite time and is thus no better than a classical computing machine. But there is a crucial difference.

In a classical search, even if the global minimum is encountered, it cannot generally be proved that it is the global minimum (unless it is a zero of the Diophantine equation). Armed only with mathematical logic, we would still have to compare it with all other numbers from the infinite domain yet to come, but we obviously can never complete this comparison in finite time – thus, the mathematical noncomputability.

In the quantum case, the global minimum is encoded in the energy of the ground state of a suitable Hamiltonian. Then, by energetic tagging, the global minimum can be confirmed in a finite time. Physical principles can be utilised to identify and/or verify the ground state. These principles are over and above the mathematics which govern the logic of a classical machine and help differentiate the quantum from the classical. Quantum mechanics could "explore" an infinite domain, but only in the sense that it can select, among an infinite number of states, one single state (or a subspace in case of degeneracy) to be identified as the ground state of some given Hamiltonian (which is bounded from below). This "sorting" can be done thanks to physical principles which are not available in the classical case.

The quantum algorithm is based on the key ingredients of:

- The ability of the theory of Quantum Mechanics to describe and predict physical processes to the level of exactness required.
- Our ability to physically implement certain Hamiltonians having infinite numbers of energy levels.

If either of these assumptions fails, the quantum algorithm simply fails and further modifications may or may not work.

In the absence of any known physical principles outlawing these key assumptions, we sketch here an approach to obtain and/or verify the desired ground state

of the Hamiltonian corresponding to the Diophantine polynomial under consideration.

The key factor in the ground state verification is *the probability distribution* calculated numerically from Quantum Mechanics *and* measurable in practice (i.e., by repeating the physical processes to obtain the statistics to any desirable accuracy). By matching the calculated with the measured we then can unambiguously identify the ground state of the relevant Hamiltonian. The information about the existence of a solution, or lack of it, for the given Diophantine polynomial can be inferred from this ground state.

5.2. General approach

It suffices to consider non-negative solutions, if any, of a Diophantine equation. Let us consider a particular example

$$(x+1)^3 + (y+1)^3 - (z+1)^3 + cxyz = 0, \quad c \in Z, \tag{15}$$

with unknowns x, y, and z. To find out whether this equation has any non-negative integer solution by quantum algorithms requires the realisation of a Fock space. Upon this Hilbert space, we construct the Hamiltonian corresponding to (15)

$$H_P = \left((a_x^\dagger a_x + 1)^3 + (a_y^\dagger a_y + 1)^3 - (a_z^\dagger a_z + 1)^3 + c(a_x^\dagger a_x)(a_y^\dagger a_y)(a_z^\dagger a_z)\right)^2,$$

which has a spectrum bounded from below – semidefinite, in fact.

Note that the operators $N_j = a_j^\dagger a_j$ have only non-negative integer eigenvalues n_j, and that $[N_j, H_P] = 0 = [N_i, N_j]$ so these observables are simultaneously measurable. The ground state $|g\rangle$ of the Hamiltonian so constructed has the properties

$$\begin{aligned} N_j|g\rangle &= n_j|g\rangle, \\ H_P|g\rangle &= \left((n_x+1)^3 + (n_y+1)^3 - (n_z+1)^3 + cn_xn_yn_z\right)^2|g\rangle \equiv E_g|g\rangle, \end{aligned}$$

for some (n_x, n_y, n_z).

Thus, a projective measurement of the energy E_g of the ground state $|g\rangle$ will yield the answer for the decision problem: The Diophantine equation has at least one integer solution if and only if $E_g = 0$, and has not otherwise. (If $c = 0$ in our example, we know that $E_g > 0$ from Fermat's last theorem.)

If there is one unique solution then the projective measurements of the observables corresponding to the operators N_j will reveal the values of various unknowns. If there are many solutions, finitely many or infinitely many as in the case of Pythagoras' theorem, $x^2 + y^2 - z^2 = 0$, the ground state $|g\rangle$ will be a linear superposition of states of the form $|n_x\rangle|n_y\rangle|n_z\rangle$, where (n_x, n_y, n_z) are the solutions. In such a situation, the measurement may not yield all the solutions. However, finding all the solutions is not the aim of a decision procedure for this kind of problem.

Notwithstanding this, measurements of N_j of the ground state would always yield some values (n_x, n_y, n_z) and a straightforward substitution would confirm if the equation has a solution or not. Thus the measurement of the ground state either of the energy (with respect to the hermitean operator H_P, provided the zero point can be calibrated) or of the number operators will be sufficient to give the result for the decision problem.

The quantum algorithm with the ground-state oracle is thus clear:

1. Given a Diophantine equation with K unknown x's

$$D(x_1, \cdots, x_K) = 0, \tag{16}$$

we need to simulate on some appropriate Fock space the quantum Hamiltonian

$$H_P = \left(D(a_1^\dagger a_1, \cdots, a_K^\dagger a_K)\right)^2. \tag{17}$$

2. If the ground state could be obtained with high probability and/or unambiguously verified, measurements of appropriate observables would provide the answer to our decision problem.

The key ingredients are the availability of a countably infinite number of Fock states, the ability to construct/simulate a suitable Hamiltonian and to obtain and/or verify its ground state. As a counterpart of the semi-infinite tape of a Turing machine, the Fock space is employed here instead of the qubits of the better known model of quantum computation. Its advantage over the infinitely many qubits which would otherwise be required is obvious.

One way to construct any suitable Hamiltonian that is desired is through the technique of Lloyd and Braunstein (1998). We consider the hermitean operators, where j is the index for the unknowns of the Diophantine equation,

$$\begin{aligned} X_j &= \frac{1}{\sqrt{2}}(a_j + a_j^\dagger), \\ P_j &= \frac{i}{\sqrt{2}}(a_j - a_j^\dagger), \\ [P_j, X_k] &= i\delta_{jk}. \end{aligned} \tag{18}$$

Together with the availability of the fundamental Hamiltonians

$$X_j,\ P_j,\ \left(X_j^2 + P_j^2\right),\ \pm\left(X_k P_j + P_j X_k\right),\ \text{and}\ \left(X_j^2 + P_j^2\right)^2 \tag{19}$$

one could construct the unitary time evolutions corresponding to Hamiltonians of arbitrary hermitean polynomials in $\{X_j, P_j\}$, and hence in $\{a_j^\dagger a_j\}$, to an arbitrary degree of accuracy. These fundamental Hamiltonians correspond to, for example, translations, phase shifts, squeezers, beam splitters and Kerr nonlinearity.

With the polynomial Hamiltonian constructed, we need to identify its ground state. Any approach that allows us to access the ground state will suffice. One way is to employ the quantum computation method of time-dependent Hamiltonians.

5.3. THE APPROACH OF TIME-DEPENDENT HAMILTONIANS

In order to solve Hilbert's tenth problem we need on the one hand such time-dependent physical (adiabatic) processes. On the other hand, the theory of Quantum Mechanics can be used to identify the ground state through the usual statistical predictions from the Schrödinger equation with a truncated number of energy states of the time-dependent Hamiltonian $\mathcal{H}(t/T)$. This way, we can overcome the problem of which states are to be included in the truncated basis for a numerical study of Quantum Mechanics. This also reconciles our approach with the Cantor diagonal argument showing that the problem could not be solved entirely in the framework of classical computation.

Below is an algorithm (Kieu, 2001a) based on this philosophy of exploiting the interplay between the presumably infinite physical world and the theory of Quantum Mechanics calculated in a finite manner on Turing machines. The algorithm presented may not be the most efficient; there could be many variations making better use of the same principles.

It is in general easier to implement some Hamiltonian than to obtain its ground state. We thus should start the computation in a different initial ground state, $|g_I\rangle$, of some initial Hamiltonian, H_I, then, as explained previously, deform this Hamiltonian in a time T into the Hamiltonian whose ground state is the desired one, through a time-dependent process represented by the interpolating Hamiltonian $\mathcal{H}(t/T)$.

One starts, for example, with a Hamiltonian H_I,

$$H_I = \sum_{i=1}^{K} (a_i^\dagger - \alpha_i^*)(a_i - \alpha_i), \tag{20}$$

which admits the readily achievable coherent state $|g_I\rangle = |\alpha_1 \cdots \alpha_K\rangle$ as the ground state. Then, one forms the time-dependent Hamiltonian $\mathcal{H}(t/T)$ in (14), which interpolates in the time interval $t \in [0, T]$ between the initial H_I and H_P.

- *Step 0:* Choose an evolution time T, a probability p which can be made arbitrarily closed to unity, and an accuracy $0 < \epsilon < 1$ which can be made arbitrarily small.
- *Step 1 (on the physical apparatus):* Perform the *physical* quantum time-dependent process which is governed by the time-dependent Hamiltonian $\mathcal{H}(t/T)$ and terminates after a time T. Then, by projective measurement (either of the observable H_p or the number operators $\{N_1, \ldots, N_K\}$) we obtain some state of the form $|\cdots n_i \cdots\rangle$, $i = 1, \cdots, K$.
- *Step 2 (on the physical apparatus):* Repeat the physical process in *Step 1* a number of times, $L(\epsilon, p)$, to build up a histogram of measurement frequencies (for all the states obtained by measurement) until we get a probability distribution $P(T; \epsilon)$ at the time T with an accuracy ϵ for all the measured states. The convergence of this repetition process is ensured by the Weak Law of Large Numbers in probability theory. (An overestimate of the number of

repetitions is $L \geq 1/(\epsilon^2(1-p))$.) Note the lowest energy state so obtained, $|\vec{n}_c\rangle$, as the candidate ground state.

- *Step 3 (on the classical computer):* Choose a truncated basis of M vectors made up of $|\alpha_1 \cdots \alpha_K\rangle$ and its excited states by successive applications of the displaced creation operators $b_i^\dagger \equiv (a_i^\dagger - \alpha_i^*)$ on the initial state.
- *Step 4 (on the classical computer):* Solve the Schrödinger equation in this basis for $\psi(T)$, with the initial state $\psi(0) = |\alpha_1 \cdots \alpha_K\rangle$, to derive a probability distribution $P_{\text{est}}(T; M)$ (through $|\langle\psi(T)|\cdots n_i \cdots\rangle|^2$) which is similar to that of *Step 2* and which depends on the total number M of vectors in the truncated basis.
- *Step 5 (on the classical computer):* If the two probability distributions are not uniformly within the desired accuracy, that is, $|P_{\text{est}}(T; M) - P(T; \epsilon)| > \epsilon$, we enlarge the truncated basis by increasing the size M and go back to the *Step 4* above.
- *Step 6 (on the classical computer):* If the two probability distributions are uniformly within the desired accuracy, that is, $|P_{\text{est}}(T; M) - P(T; \epsilon)| < \epsilon$, then use this truncated basis to diagonalise H_P to yield, within an accuracy which can be determined from ϵ, the approximated ground state $|g'\rangle$ and its energy $E_{g'}$.
- *Step 7 (on the classical computer):* We can now estimate in this truncated basis the gap between the ground state and the first excited state. From this gap, we can make use of the quantum adiabatic theorem and choose a time T such that the system has a high probability of having the system mostly in the ground state

$$\left||\langle g'|\psi(T)\rangle|^2 - 1\right| < \epsilon.$$

We then go back to *Step 1* with this choice of T, to confirm the candidate ground state as the real ground state.

5.4. Discussion of the algorithm

The quantum algorithm above can be proved to terminate (even though it could be after a very long time) and give us the decision result for Hilbert's tenth problem.

The real spectrum of H_p is of integer values (in suitable units), and that is what we also get from measurement. But the spectrum calculated from a finitely truncated basis is not of integer values and will fluctuate with fluctuation size depending on the size of the truncated basis employed. The accuracy ϵ of the measured probability distribution is chosen such that the fluctuation of the ground state energy δ should allow us to conclude whether the ground state energy $E_{g'}$ is zero or not. (δ is in general a function of ϵ and T.)

The proof of termination is somewhat technical and available elsewhere. Such termination is obtained if and when the adding of higher b-number states (those

created from the coherent state by the application of the creation operator $b_i^\dagger \equiv (a_i^\dagger - \alpha_i^*)$) does not change the approximated ground state of H_P beyond a certain range of accuracy.

Even though we can prove that the approximated ground state and its energy will eventually converge to the true values, the mathematical noncomputability results from the fact that their rates of convergence are unknown and unknowable in general. Thus, we cannot use mathematical reasoning alone to determine when to stop adding more states to the truncated basis in order to approximate the ground state correctly. Different truncated bases would give *some* estimates for the ground state but we have no control over these estimates and no idea how good they are. They could be anywhere in relation to the true values. This is nothing but mathematical noncomputability.

To know when the truncated basis is sufficiently large to have the estimated ground state values within any given accuracy, that is, to regain computability, we have to exploit the measurability of physical processes. Because of this measurability we can estimate the true accuracy of our measured values. Then a comparison of results from the Schrödinger equation to these measurable quantities will help determine the accuracy of results from the equation, so regaining the lost computability through the physical world, presumed infinite.

6. Against No-Go Arguments

6.1. Universal quantum turing machines

Our proposal is in contrast to the claim in Bernstein and Vazirani (1997), see also Gandy (1993), that universal quantum Turing machines compute exactly the same class of functions that can be computed by Turing machines, but perhaps more efficiently. The quantum Turing machine approach considered there is a direct generalisation of the classical Turing machine but with qubits and some universal set of one-qubit and two-qubit unitary gates to build up, step by step, dimensionally larger, but still dimensionally finite unitary operations. This universal set is chosen on its ability to evaluate any desired classical logic function. Our approach, on the other hand, is from the start based on infinite-dimension Hamiltonians and also based on the special properties and unique status of their ground states. In effect, our algorithm does not belong to the jurisdiction of the qubit analysis.

6.2. On Gandy's no-go arguments against general quantum computation

Gandy (1993) gave various examples to support a claim, which admittedly is more of a challenge than an assertion, that given a reasonable definition of 'analogue ma-

chine', such a machine cannot, upon accepting (continuously variable) computable input, calculate the values of some number-theoretic noncomputable function.

More precisely, a decision problem can be posed as the question whether an integer $j \in A$ or not, where A is a standard recursively enumerable non-recursive set. Because it is recursively enumerable there exists a total computable function a from the set of natural numbers to itself, $a : \mathcal{N} \to \mathcal{N}$, which enumerates A without repetitions. A special function called the *waiting-time* function is defined as

$$\nu(j) = \mu n[a(n) = j]; \tag{21}$$

that is, $\nu(j)$ gives the least n ('time') upon which j is confirmed to be a member of the set A. Note that ν is a partial recursive function which is not bounded by any total computable function.

Gandy argued that for any particular analogue machine there is an upper bound J on the inputs it can accept. He then claimed that, with given J, one cannot have an analogue machine which will always give correct answers to all the questions $j \in A?$, for $j < J$, unless one knows a bound B for $\beta(J) = \max\{\nu(j) : j < J \& j \in A\}$, the maximum waiting time within the range J.

$\beta(J)$, even though total, is noncomputable – indeed, it eventually majorises every computable function. Of course, if a bound B is known one does not need the analogue machine to settle the decision problem. One just computes $a(n)$, for all $n < B$, to see if j is obtained as a value, and thus belongs to A, or not.

Nevertheless, Gandy also recognised that his claim might not stand up to the kind of analogue machines whose behaviour depends on a single quantum (similar to our process involving Hamiltonians which have discrete spectra of integer values). Neither would the claim be valid if the physical theory involved has elements of non-computability already built-in. But here we have argued all along that Quantum Mechanics with its measurement postulate has, in a sense, some elements of non-computability through its *intrinsic randomness*. To wit, randomness is 'noncomputable' as it cannot be algorithmically computed.

Furthermore, our proposal is not subject to Gandy's treatment since ours is a kind of probabilistic computation, where the probability that we get a wrong answer can be made arbitrarily small but is not exactly zero. Also, his upper bound B turns out to be a product of our quantum hypercomputation: it is an output of the computation rather than a required input.

7. Concluding Remarks

In summary, we have encoded the answer to the question about the existence or lack of non-negative integer solutions for any Diophantine equation into the ground state of some relevant Hamiltonian. This encoding opens a new venue for the study of Hilbert's tenth problem. It turns out that to solve this problem we will need

both the physical time-dependent processes *and* the numerical Quantum Mechanics to identify the ground state through the usual statistical predictions from the Schrödinger equation with a few low-lying energy states of $\mathcal{H}(t/T)$. We do need both the physical world and the classical computer, either of them alone will not suffice:

- Quantum measurements of observables by themselves in the physical world (which is presumably infinite) cannot in general identify the ground state.
- Mathematical computation (on Turing machines) cannot handle infinity in general and thus cannot by itself identify the ground state of Hamiltonians having a countably infinite number of eigenvalues.

Exploiting both worlds, we can overcome the problem of knowing where to truncate the infinite basis for a numerical study of Quantum Mechanics, and achieve a reconciliation with the Cantor diagonal argument which shows that the problem could not be solved entirely in the framework of classical computation.

The key factor in the ground state verification is *the probability distribution*, which not only can be calculated in numerical Quantum Mechanics (with a truncated basis) but also is, as mentioned in Section 3.1, measurable in practice. After all, probability distributions are also physical observables. However, in using the probability distributions as the identification criteria, we have to assume that Quantum Mechanics is able to describe Nature correctly to the precision required. Note also that we have here a peculiar situation in which the computational complexity, that is, the computation time, might not be known exactly *before* carrying out the quantum computation – although it can be estimated approximately.

The situation with our algorithm is just the usual and normal relationship between theory and experiments: the 'correct' theory matches with experiments in some aspects and can be employed to predict other aspects of reality (which might be subsequently verified by new experiments).

It remains to be seen whether the algorithm can be implemented in the physical world (in particular, whether one can construct the required Hamiltonians to the desired accuracy), but our analysis has shown that the algorithm should occupy only finite time duration and finite spatial extent and consume only a finite amount of physical resources. If not prohibited by any physical principles then it can be implemented and will be realisable. If prohibited, on the other hand, because of some yet-to-be-known reasons then in identifying those reasons we will have found new physical principles.

Our decidability study so far only deals with the property of being Diophantine, which does not cover the property of being arithmetical in general (which could involve unbounded universal quantifiers). As such, our consideration has no direct bearing on Gödel's Incompleteness theorem. However, it is conceivable that Gödel's theorem may lose its restrictive power once the concept of mathematical proof is suitably generalised with quantum principles

> Gödel's result displaced logic from the center of the mathematician's world, but in so doing it has challenged us to locate a noncentral but unique place for

that rarity among principles of faith: a passionate form of belief that avows its own shortcomings.

Michael Guillen (1983)

Acknowledgements

I am indebted to Alan Head, Peter Hannaford and Andrew Rawlinson for support and discussions. I would also like to thank Jack Copeland for providing me with the chance to write this paper, and with an unpublished paper by R.O. Gandy. I wish to acknowledge the hospitality extended to me during my stays at the CTP at MIT, and then at the IAS, Princeton, where this paper was written. Fruitful discussions with Stephen Adler, Todd Brun, Edward Farhi, Jeffrey Goldstone and Sam Gutmann during these stays are gratefully acknowledged. So is the financial assistance by the Australian Academy of Science.

References

Bell, J.S. (1987), *Speakable and Unspeakable in Quantum Mechanics*, Cambridge: Cambridge University Press.

Benioff, P. (1980), 'The Computer as a Physical System.' *Journal of Statistical Physics* 22, pp. 563–591.

Bernstein, E. and Vazirani, U. (1997), Quantum Complexity Theory. *SIAM Journal on Computing* 26, pp. 1411.

Calude, C.S. and Paun, G. (2001), *Computing with Cells and Atoms*, Oxford: Taylor and Francis.

Calude, C.S. and Pavlov, B. (2001), 'Coins, Quantum Measurements and Turing's Barrier', Archive quant-ph/0112087.

Casti, J.L. (2001), *Mathematical Mountaintops*, Oxford/New York: Oxford University Press.

Chaitin, G.J. (1992), *Algorithmic Information Theory*, Cambridge: Cambridge University Press.

Copeland, B.J. and Sylvan, R. (1999), 'Beyond the Universal Turing Machine', *Australasian Journal of Philosophy* 77, 46–66.

Davis, M. and Hersh, R. (1973), 'Hilbert's 10^{th} Problem', *Scientific American*, pp. 84–91.

Davis, M. (1982), *Computability and Unsolvability*, New York: Dover.

Davis, M. (2000), *Engines of Logic*, New York: Norton.

Deutsch, D., Ekert, A. and Lupacchini, R. (2000), 'Machines, Logic and Quantum Physics', *The Bulletin of Symbolic Logic* 6, pp. 265–283. See also a review of this paper by E. Knill on http://quickreviews.org/cgi/display.cgi?reviewID=knill.bsl.6.265

Enk, S.J. van and Fuchs, C.A. (2001), Archive quant-ph/0111157.

Etesi, G. and Németi, I. (2001), 'Non-Turing Computations via Malament-Hogarth Space-times', Archive gr-qc/0104023.

Farhi, E., Goldstone, J., Gutmann, S. and Sipser, M. (2000), 'Quantum Computation by Adiabatic Evolution', Archive quant-ph/0001106.

Feynman, R.P. (1982), 'Simulating Physics with Computers' *International Journal of Theoretical Physics* 21, pp. 467.

Gandy, R.O. (1980), 'Church's Thesis and Principles for Mechanisms', in J. Barwise, H.J. Keisler and K. Kunen, eds. *The Kleene Symposium*, Amsterdam: North-Holland

Gandy, R.O. (1993), On the impossibility of using analogue machines to calculate non-computable functions, unpublished. (Gandy handed this paper to Jack Copeland about two weeks before he died. I am grateful to Jack Copeland for giving me access to this hand-written manuscript.)

Geroch, R., and Hartle, J.B. (1986), 'Computability and Physical Theories', *J. Found. Phys.* 16, pp. 533–550.

Grover, L.K. (1997), 'Quantum Mechanics Helps in Searching for a Needle in a Haystack', *Physical Review Letters*. 79, pp. 325–328.

Guillen, M. (1983), *Bridges to Infinity*, Rider & Company.

Kieu, T.D. (2001a), 'Quantum Algorithm for the Hilbert's Tenth Problem', Archive `quant-ph/0110136`. See also Kieu, T.D. (2002), 'Computing the Noncomputable', Archive `quant-ph/0203034`, to appear in *Contemporary Physics*.

Kieu, T.D. (2001b), 'A Reformulation of the Hilbert's Tenth Problem Through Quantum Mechanics', Archive `quant-ph/0111063`.

Kieu, T.D. (2002), 'Quantum Principles and Mathematical Computability', Archive `quant-ph/0205093`.

Lewis, H.R. and Papadimitriou, C.H. (1981), *Elements of the Theory of Computation*, Englewood Cliffs, NJ: Prentice Hall.

Lloyd, S. and Braunstein, S.L. (1998), 'Quantum Computation over Continuous Variables', Archive `quant-ph/9810082`.

Matiyasevich, Y.V. (1993), *Hilbert's Tenth Problem*, Cambridge, MA: MIT Press.

Messiah, A. (1976), *Quantum Mechanics*, Vol. II, Amsterdam: North Holland.

Nagel, E. and Newman, J.R. (1958), *Gödel's Proof*, New York: New York University Press.

Nielsen, M.A. (1997), 'Computable Functions, Quantum Measurements, and Quantum Dynamics', *Physical Review Letters* 79, pp. 2915–2918.

Nielsen, M.A. and Chuang, I.L. (2000), *Quantum Computation and Quantum Information*, Cambridge: Cambridge University Press.

Pour-El, M. and Richards, I. (1979), *Computability in Analysis and Physics*, Berlin: Springer.

Scriven, M. (1964), 'The Mechanical Concept of Mind', in A.R. Anderson, ed., *Mind and Machines*, Englewood Cliffs, NJ: Prentice-Hall.

Shor, P.W. (1997), 'Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer', *SIAM Journal on Computing* 26, pp. 1484–1509.

Siegelmann, H.T. (1995), 'Computation Beyond the Turing Limit', *Science* 268, pp. 545–548.

Stannett, M., 2001, 'Hypercomputation is Experimentally Irrefutable.' Tech. Report CS-01-04 Dept of Computer Science, Sheffield University.

Svozil, K. (1998), 'The Church-Turing Thesis as a Guiding Principle for Physics', in C.S. Calude, J. Casti and M.J. Dinneen, eds., *Unconventional Models of Computation*, Singapore: Springer, pp. 371–385.

Walls, D.F. and Milburn, G.J. (1995), *Quantum Optics*, Berlin: Springer.