International Journal of Theoretical Physics, Vol. 42, No. 7, July 2003 (© 2003)

Quantum Algorithm for Hilbert's Tenth Problem

Tien D Kieu[1]

Received December 19, 2002

We explore in the framework of Quantum Computation the notion of *Computability*, which holds a central position in Mathematics and Theoretical Computer Science. A quantum algorithm for Hilbert's tenth problem, which is equivalent to the Turing halting problem and is known to be mathematically noncomputable, is proposed where quantum continuous variables and quantum adiabatic evolution are employed. If this algorithm could be physically implemented, as much as it is valid in principle—that is, if certain Hamiltonian and its ground state can be physically constructed according to the proposal—quantum computability would surpass classical computability as delimited by the Church–Turing thesis. It is thus argued that computability, and with it the limits of Mathematics, ought to be determined not solely by Mathematics itself but also by Physical Principles.

KEY WORDS: quantum algorithms; computability; quantum adiabatic computation; hypercomputation.

1. INTRODUCTION

Computation based on the principles of Quantum Mechanics (See, for example, Nielsen and Chuang, 2000) has been shown to offer better performances over classical computation, ranging from the square-root improvement in an unstructured search (Grover, 1997) to the exponential gain in the factorization of integers (Shor, 1997). However superior in reducing the complexity of hard computation, these quantum algorithms and all the others discovered so far are only applicable to the *classically computable* functions. That leaves untouched the class of *classically noncomputable* functions, such as the halting problem for Turing machines (Rogers, 1987). It is in fact widely believed that quantum computation cannot offer anything new about computability (Bernstein and Vazirani, 1997). Contrary to this, we propose that quantum computation may be able to compute the noncomputables, provided certain Hamiltonian and its ground state can be physically constructed. We propose a quantum algorithm for the classically noncomputable Hilbert's tenth problem (Matiyasevich, 1993) which ultimately links

[1] Centre for Atom Optics and Ultrafast Spectroscopy, Swinburne University of Technology, Hawthorn 3122, Australia; e-mail kieu@swin.edu.au.

0020-7748/03/0700-1461/0

to the halting problem for Turing machines in the computation of partial recursive functions.

The practical details of implementation of the quantum algorithm for this class of problems are not considered in this conceptual study, and will be investigated elsewhere.

2. HILBERT'S TENTH PROBLEM

At the turn of the last century, David Hilbert listed 23 important problems, among which the problem number 10 could be rephrased as

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

This decision problem for such polynomial equations, which are also known as Diophantine equations, has eventually been shown in 1970 by Matiyasevich to be undecidable (Davis, 1982; Matiyasevich, 1993) in the Turing sense. It is consequently noncomputable/undecidable in the most general sense if one accepts, as almost everyone does, the Church–Turing thesis of computability. Since exponential Diophantine, with the unknowns in the exponents as in the example of Fermat's last theorem, can be shown to be Diophantine with supplementary equations, the study of Diophantine equations essentially covers the class of partial recursive functions, which is at the foundations of classical algorithms. The undecidability result is thus singularly important: Hilbert's tenth problem could be solved if and only if the Turing halting problem could be.

3. TURING HALTING PROBLEM

The halting problem for Turing machines is also a manifestation of undecidability: a Turing Computation is equivalent to the computation of a partial recursive function, which is defined only for a subset of the integers; as this domain is classically undecidable, one cannot always tell in advance whether the Turing machine will halt (that is, whether the input is in the domain of the partial recursive function) or not (when the input is not in the domain).

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 $h(h, n)$ and

$$\begin{cases} r(n) \text{ halts if } h(n, n) = 1 \\ r(n) \text{ loops infinitely (i.e., never stops) otherwise.} \end{cases} \tag{2}$$

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

$$h(r, n) = \begin{cases} 0 & \text{if } h(n, n) = 1 \\ 1 & \text{if } h(n, n) = 0 \end{cases} \tag{3}$$

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

The construction of such 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.

This contradiction argument might be side stepped if we distinguish and separate the two classes of quantum and classical algorithms. A *quantum* function $qh(p, i)$, similar to Eq. (1), can conceivably exist to determine whether any classical program p will halt on any classical input i or not. The contradiction in Eq. (2) would be avoided if the quantum halting qh cannot take as argument the modified program r, which is now of *quantum* character because it now has quantum qh as a subroutine. This will be the case if qh can only accept integer while quantum algorithms, with proper definitions, cannot in general be themselves encoded as integers. It is clear even in the case of a single qubit that the state $\alpha|0\rangle + \beta|1\rangle$ cannot be encoded as integers for all α and β - simply because of different cardinalities. In fact, the no-cloning theorem (Wooters and Zurek, 1982) of quantum mechanics does restrict the type of operations available to quantum algorithms.

In essence, the way we will break the self-referential reasoning here by the differentiation between quantum and classical algorithms in similar to the way John von Neumann and Bertrand Russell resolved the set theory paradox (to do with "The set of all sets which are not members of themselves") by the introduction of classes as distinct from sets. (For other lines of arguments, see Ord and Kieu (2003)).

4. AN OBSERVATION

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

$$(x + 1)^2 + (y + 1)^3 - (z + 1)^3 + cxyz = 0, \quad c \in Z, \tag{4}$$

with unknowns x, y, and z. To find out whether this equation has any non-negative integer solution by quantum algorithms, it requires the realization of a Fock space built out of the "vacuum" $|0_a\rangle$ by repeating applications of the creation operators

$a_x^\dagger$, $a_y^\dagger$, and $a_z^\dagger$, similarly to that of the 3D simple harmonic oscillators.

$$[a_j, a_j^\dagger] = 1 \quad \text{for } j = x, y, z, \tag{5}$$

$$[a_k, a_j] = [a_k, a_j^\dagger] = 0 \quad \text{for } j \neq k.$$

Upon this Hilbert space, we construct the Hamiltonian corresponding to (3)

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

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 $[N_j, H_P] = 0 = [N_i, N_j]$ sot these observables are compatible—they are simultaneously measurable. The ground state $|g\rangle$ of the Hamiltonian so constructed has the properties

$$N_j|g\rangle = n_j|g\rangle,$$

$$H_P|g\rangle = ((n_x + 1)^3 + (n_y + 1)^3 - (n_z + 1)^3 + cn_x n_y n_z)^2|g\rangle \equiv E_g|g\rangle,$$

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 known 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 or infinitely as in the case of $x^2 + y^2 - z^2 = 0$, the ground state $|g\rangle$ will be a linear superposition of states of the form $|n_x\rangle \otimes |n_y\rangle \otimes |n_z\rangle$, where (n_x, n_y, n_z) are the solutions. In such 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 on the ground state either of the energy, 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 unknowns x's

$$D(x_1, \ldots, x_K) = 0, \tag{6}$$

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

$$H_P = (D(a_1^\dagger a_1, \ldots, a_K^\dagger a_K))^2. \tag{7}$$

2. If the ground state could be obtained with high probability, measurements of appropriate observables would provide the answer for 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/identify its ground state via quantum measurements. As a counterpart of the semi-infinite tape of a Turing machine, the Fock space is employed here instead of the qubits of the more well-known model of quantum computation. Its advantage over the infinitely many qubits which would otherwise be required is obvious.

5. SOME PRELIMINARY COMMENTS

We do not look for the zeroes of the polynomial, $D(x_1, \ldots, x_K)$, which may not exist, but instead search for the absolute minimum of its square which exists,

$$0 \leq \min(D(x_1, \ldots, x_K))^2 \leq (D(0, \ldots, 0))^2,$$

and is finite because $\lim_{x\to\infty}(D(x_1, \ldots, x_K))^2$ diverges.

While it is equally hard to find either the zeroes or the absolute minimum in classical computation, we have converted the problem to the realization of the ground state of a quantum Hamiltonian, and there is no known quantum principle against such act. In fact, there is no known physical principles against it. Let us consider the three laws of thermodynamics concerning energy conservation, entropy of closed systems, and the unattainability of absolute zero temperature. The energy involved in our algorithm is finite, being the ground state energy of some Hamiltonian. The entropy increase which ultimately connects to decoherence effects in a technical problem for all quantum computation in general, and we will discuss this further below. As we will never obtain the absolute zero temperature, we only need to satisfy ourselves that the required ground state can be achieved with a more-than-even chance. Then there is a probability boosting technique, see later, to bring that chance to as closed to unity as one pleases.

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 machine in terms of computability. But there is a crucial difference.

In a classical search even if the global minimum is come across, 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, mathematical noncomputability.

In the quantum case, the global minimum is encoded in the ground state. Then, by energy tagging, the global minimum can be found in finite time and

confirmed, if it is the ground state that is obtained at the end of the computation. And the ground state may be identified and/or verified by physical principles. These principles are over and above the mathematics which govern the logic of a classical machine and help differentiating 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 singe 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 because of energetic reason, which is a physical principle and is not available to mathematical computability.

On the other hand, our proposal is apparently in contrast to the claim in (Bernstein and Vazirani, 1997) that quantum Turing machines compute exactly the same class of functions as do Turing machines, albeit perhaps more efficiently. We could only offer here some speculations about this apparent discrepancy. The quantum Turing machine approach is a direct generalization of that of the classical Turing machines 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 desirable classical logic function. Our approach, on the other hand, is from the start based on infinite-dimension Hamiltonians acting on some Fock space and also based on the special properties and unique status of their ground states. The unitary operations are then followed as the Schrödinger time evolutions. Even at the Hamiltonian level higher orders of the operators a and $a^\dagger$, i.e. not just two-body but many-body interactions in a sense, are already present. The proliferation, which is even more pronounced at the level of the time-evolution operators, together with the infinite dimensionality and the unique energetic status of the vacuum could be the reasons behind the ability to compute, in a finite number of steps, what the dimensionally finite unitary operators of the standard quantum Turing computation cannot do in a finite number of steps. Note that it was the general Hamiltonian computation that was discussed by Benioff (1980) and Feynman (1982) in the conception days of quantum computation.

Indeed, Nielsen (1997) has also found no logical contradiction in applying that most general quantum mechanical principles to the computation of the classical noncomputable, unless certain Hermitean operators cannot somehow be realized as observables or certain unitary processes cannot somehow be admitted as quantum dynamics. And up to now we do not have any evidence nor any principles that prohibit these kinds of observables and dynamics. (Ozawa, 1998 has produced some counter arguments but we think they are not quite applicable here.) See Ord and Kieu (2003).

Our general algorithm above could be realized by, but in no way restricted to, the following methods to simulate the required Hamiltonian and to obtain the ground state adiabatically.

6. SIMULATING THE HAMILTONIANS

One way to construct any suitable Hamiltonian so desired is through the technique of Lloyd and Braunstein (1999). We consider the Hermitean operators, where j is the index of the unknowns of the Diophantine equation,

$$\begin{aligned} X_j &= \frac{1}{\sqrt{2}}(a_j + a_j^\dagger), \\ P_j &= \frac{i}{\sqrt{2}}(a_j - a_j^\dagger), \\ [P_j, X_k] &= i\delta_{jk}. \end{aligned} \tag{8}$$

Together with the availability of the fundamental Hamiltonians

$$X_j,\ P_j,\ \left(X_j^2 + P_j^2\right),\ \pm(X_k P_j + P_j X_k),\ \text{and}\ \left(X_j^2 + P_j^2\right)^2 \tag{9}$$

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 translations, phase shifts, squeezers, beam splitters, and Kerr nonlinearity.

With the polynomial Hamiltonian constructed, we need to obtain its ground state. Any approach that allow us to access the ground state will suffice. One way is perhaps to use that of quantum annealing or cooling (Kadowaki and Nishimori, 1998). Another way is to employ the quantum computation method of adiabatic evolution (Farhi *et al.*, 2000).

7. ADIABATIC QUANTUM EVOLUTION

In the adiabatic approach, one starts with a Hamiltonian H_I whose ground state $|g_I\rangle$ is readily achievable. Then one forms the slowly varying Hamiltonian $\mathcal{H}(s)$, $s = \frac{t}{T}$, which interpolates between H_I and H_P in the time interval $t \in [0,\ T]$

$$\mathcal{H}(s) = (1 - s)H_I + sH_P. \tag{10}$$

Note that we can replace this linear interpolation by some nonlinear one provided the conditions of the adiabatic theorem are observed. According to this theorem, the initial ground state will evolve into our desirable ground state $|g\rangle$ up to a phase:

$$\lim_{T\to\infty} \mathcal{T}\ \exp\left\{-iT\int_0^1 \mathcal{H}(\tau)\,d\tau\right\}|g_I\rangle = e^{i\phi}|g\rangle. \tag{11}$$

For the Hamiltonian (9), an estimate of the time T after which the system remains with high probability in the ground state is

$$T \gg \frac{\|H_I - H_P\|}{g^2}, \tag{12}$$

with

$$\|H_I - H_P\| \equiv \max_{0\le t\le T} |\langle e(t)|(H_I - H_P)|g(t)\rangle|, \tag{13}$$

and

$$g \equiv \min_{0\le t\le T} (E_e(t) - E_g(t)), \tag{14}$$

where $|g(t)\rangle$ and $|e(t)\rangle$ are respectively the instantaneous ground state and the first excited state of (9) with instantaneous eigenvalues $E_g(t)$, $E_e(t)$.

The time-ordering operator on the left hand side of (10) can be approximated as

$$\exp\{-iT\mathcal{H}(\tau_N)\Delta\tau\}\cdots\exp\{-iT\mathcal{H}(\tau_1)\Delta\tau\}$$

for (Farhi *et al.*, 2000)

$$N\Delta\tau = 1,$$

$$\Delta\tau\|H_I - H_P\| \ll 1. \tag{15}$$

Note that we have employed here the "norm" $\|\cdot\|$ as defined in (12) for the various Hamiltonians which are unbounded from above. This norm is the relevant measure for the problem only concerned with the lowest states of the interpolating Hamiltonian (9). In each interval $\Delta\tau$, the unitary operators $\exp\{-i\mathcal{H}(\tau_k)T\Delta\tau\}$, for $k = 1, \ldots, N$, can be expressed through the subdivision of $T\Delta\tau$ into m subintervals of sufficiently small size δs satisfying $m\delta s = T\Delta\tau$,

$$\exp\{-i\mathcal{H}(\tau_k)T\Delta\tau\} = (\exp\{-i\mathcal{H}(\tau_k)\delta_s\})^m.$$

Each of the m factors on the right hand side of the last expression can be now simulated through the approach of (Lloyd and Braunstein, 1999), where it was shown that the number of steps M grows as a small polynomial in the order of the polynomial in the Hamiltonian $\mathcal{H}(\tau_k)$ to be simulated, the accuracy to be enacted, and the time interval $T\Delta\tau$ over which it is to be applied.

In this way, the requirements of the adiabatic conditions on the one hand and of, on the other hand, the simulations of the Hamiltonians in the time interval $T\Delta\tau$ can be satisfied.

8. AN ADIABATIC ALGORITHM

To solve the 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 finitely 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 with the Cantor diagonal arguments which state that the problem could not be solved entirely in the framework of classical computation.

Later is an algorithm (Kieu, 2001a,b,c) 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 other variations making better use of the same philosophy.

It is in general easier to implement some Hamiltonian than to obtain its ground state. We thus should start the computation in yet 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 represented by the interpolating Hamiltonian $\mathcal{H}(t/T)$.

In this approach, inspired by the quantum adiabatic approach, one starts, for example, with a Hamiltonian H_I,

$$H_I = \sum_{i=1}^{K} (a_i^\dagger - \alpha_i^*)(a_i - \alpha_i), \tag{16}$$

which admits the readily achievable coherent state $|g_I\rangle = |\alpha_1 \ldots \alpha_K\rangle$ as the ground state. Then, one forms the time-dependent Hamiltonian $\mathcal{H}(t/T)$ in (9), 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 $|\ldots n_i \ldots\rangle$, $i = 1, \ldots, K$.
- *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 probaility 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 (Renyi, 1970). (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 $|\alpha_1 \ldots \alpha_K\rangle$ and its excited states by successive

applications of the displaced creation operations $b_i^\dagger \equiv (a_i^\dagger - \alpha_i^*)$ on the initial state.

- *Step 4 (on the classical computer)*: Solve the Schrödinger equation in this basis for $\psi(T)$, with the initial state $\psi(0) = |\alpha_1 \ldots \alpha_K\rangle$, to derive a probability distribution $P_{\text{est}}(T; M)$ (through $|\langle\psi(T)|\ldots n_i \ldots\rangle|^2$) 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 diagonals 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 to be in the ground state

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

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

Our point is on computability and not on computational complexity, which depends on individual polynomials. Computability is based on the arguments that the adiabatic time T is *finite* (Kieu, 2001a,b,c; Ruskai, 2002) (for a high probability of achieving the ground state) and that the ground state can be *verified* by employing the theory of Quantum Mechanics. As long as the energy gap is finite so is the computational time. In contrast, the most general classical algorithm for Hilbert's tenth problem (by systematic substituting in integers of larger and larger magnitudes) cannot solve it in principle even allowing for exponentially grown, but finite, amount of time—unless *infinite* amount of time were available, which it is not.

Given a Diophantine equation, the substitution in integers of larger and larger magnitudes is not satisfactory as we do not known when the substitution should be terminated. Likewise, if we want to numerically simulate the quantum algorithm proposed, we would have to use a finitely truncated having M vectors. But we face the same problem of not knowing which M to choose in general. That is why the problem is noncomputable on classical computers.

Even we can estimate T, as in the appendix, for some starting point of the adiabatic computation as we might not be able in general to exactly know T a priori. Were the required adiabatic time T somehow known exactly within classical computation and without the help of quantum computation then the problem might be solves classically. But as Hilbert's tenth problem cannot be solved by classical computation, we will have to resort to quantum computation without *a priori* knowing exactly the time T, except the knowledge that it is *finite*. Constructive logicians (D. Bridges in private communication with Cristian Calude) allow for this algorithmic situation under the so-called Markov's Principle.

9. 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 size ϵ of the measured probability distribution is chosen such that the off-set 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.)

$$\begin{aligned} E_{g'} &= \langle g'|H_P|g'\rangle, \\ &= E_c + \langle r|H_P|r\rangle + 2\mathrm{Re}\langle r|H_P|n_c\rangle, \\ &= E_c + \langle r|H_P\|r\rangle + 2E_c(\mathrm{Re}\rangle r|n_c\rangle), \\ &\equiv E_c + \delta(\epsilon), \end{aligned} \tag{17}$$

where $|r\rangle \equiv |g'\rangle - |n_c\rangle$ and $H_P|n_c\rangle = E_c|n_c\rangle$.

The termination of our algorithm 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 $b_i^\dagger \equiv (a_i^\dagger - \alpha_i^*)$) to the truncated basis does not change the approximated ground state of H_P beyond certain range of accuracy,

$$|\delta(\epsilon)| \leq E_c \neq 0. \tag{18}$$

Even we can prove that the approximated ground state $|g'\rangle$ and its energy will eventually converge to its true values, the mathematical noncomputability results from the fact that their rates of convergence are unknown. Thus, we might not be able to 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. (However, this quantum algorithm has inspired us to reformulate the Hilbert's tenth problem with continuous variables (Kieu, 2001a,b,c), and the mathematical computability of this reformulation, or lack of it, should be investigated further.)

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 determining the accuracy of results from the equation, that is, regaining the lost computability through the physical world, presumably infinite.

10. DECOHERENCE AND ERROR CORRECTION

Our approach above is in fact a combination of the quantum computation of continuous variables and of adiabatic evolution. There exists some error correction protocol for continuous variables (Braunstein, 1998) which could be of help here to protect the wave functions from decoherence. However, the adiabatic computation we exploit is quite robust in general (Childs *et al.*, 2001). An imperfect conventional quantum algorithm might have different sorts of errors than an imperfect adiabatic process, where the system is kept close to the instantaneous ground state over time. Decoherence by the environment inducing transition between levels could be controlled in principle at a temperature that is small compared to the gap (13), given its estimate. Errors introduced by the Hamiltonian simulation may result in a Hamiltonian different from (9) but in a form $\mathcal{H}(t/T) + K(t)$. Recent numerical study (Childs *et al.*, 2001) of small systems has in fact indicated that the adiabatic computation is interestingly robust even for fairly large $K(t)$, provided $K(t)$ varies either sufficiently slowly or sufficiently rapidly (which is more likely to be the case considered here because of the nature of our Hamiltonian simulations).

11. PROBABILITY BOOSTING

Because of the particular nature of the present scheme, the various approximations result in some probability that the final measurement will not find the system in the desired ground state; but appropriate choices of the various time parameters could increase the success probability of the algorithm to more than even. We spell out explicitly here the probability boosting technique, as mentioned in (Bernstein and Vazirani, 1997), that one could subsequently apply.

In our computation, adiabatic or otherwise, the end result, starting from some initial state $|g_I\rangle$, may be contaminated with some excited states other than the

desirable ground state $|g\rangle$,

$$|g_I\rangle \stackrel{\text{time}}{\longmapsto} a|g\rangle + b|e\rangle. \tag{19}$$

If $|a| > |b|$, that is, if there is a better-than-even chance to obtain $|g\rangle$ by measurement then one can boost the success probability to arbitrarily closed to unity by performing a concatenated computation over l Hilbert spaces

$$|g_I\rangle_1 \otimes \cdots |g_I\rangle_l \stackrel{\text{time}}{\longmapsto} \mathcal{N} \sum_{p=0}^{l} a^p b^{l-p} |e\rangle_1 \otimes \cdots \otimes |g\rangle_{k_1} \otimes \cdots \otimes |g\rangle_{k_p} \otimes \cdots \otimes |e\rangle_l, \tag{20}$$

where $\mathcal{N}$ is the normalizing factor. Let us consider the majority amplitudes, when more than half of the l Hilbert spaces return the correct results, $\mathcal{N}a^p b^{l-p}$, $p > \frac{l}{2}$; and the minority amplitudes, $\mathcal{N}a^q b^{l-q}$, $q > \frac{l}{2}$. The ratio of the majority over the minority, $(a/b)^{p-q}$, is clearly boosted for sufficiently large l and for $p \sim O(l)$ and $q \sim O(l)$. The probability distribution for a measurement of the end state in (19), as a consequence, is exponentially dominated by the majority results. In other words, the probability to obtain a majority result which contains the true ground state can be made arbitrarily closed to unity, $(1 - \epsilon')$, provided $|a| > |b|$ and $l > -C \log \epsilon'$. However, the decoherence control for such l concatenated Hilert spaces will be more crucial.

12. CONCLUDING REMARKS

In this paper, we consider and emphasize on the issue of computability in principle, not that of computational complexity. This attempt of broadening of the concept of effective computability, taken into account the quantum mechanical principles, has been argued to be able in principle to decide the classically/Turing undecidables, Hilbert's tenth problem and thus the Turing halting problem in this instance. If this is realizable, and we don't have any evidence of fundamental nature to the contrary, the Church–Turing thesis should be modified accordingly.

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 that of ground state of some relevant Hamiltonian.

The key factor in the ground state verification is *the probability distributions*, which not only can be calculated in numerical Quantum Mechanics (with a truncated basis) but also are 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 (see the appendix later).

On the other hand, if for any reasons the algorithm is not implementable because of physical principles and/or physical resources then it would be an example of information being limited by physics, rather than by logical arguments alone.

Our study is an illustration of "Information is physical" (see Calude and Pavlov, 2001) for another quantum mechanical approach and (Etesi and Németi, 2001) for where the theory of General Relativity is also exploited for the computation of Turing noncomputables).

That some generalization of the notion of computation could help solving the previous undecidability/noncomputability has been recognized in mathematics and was considered by Kleene as quoted in Rogers (1987). But this has not been realizable until now simply because of the nonrecognition of quantum physics as the missing ingredient. Our quantum algorithm could in fact be regarded as an infinite search through the integers in a finite amount of time, the type of search required by Kleene to solve the Turing halting problem.

Our decidability study here only deals with the property of being Diophantine, which does not cover the property of being arithmetic in general, and as such has no direct consequences on the Gödel's Incompleteness theorem (Kieu, 2001a,b). However, it is conceivable that the Gödel's theorem may lose its restrictive power once the concept of proof is suitably generalized with quantum principles.

APPENDIX: GAP ESTIMATION

The question of computational complexity, i.e. how large the adiabatic computational time T is for a high probability of measurement success, is dependent on H_p, i.e. on the specific Diophantine equation in question, and on the initial Hamiltonian H_I. Some estimate for the energy gap (13) is desirable, but not necessary as discussed above. In this appendix we propose such an estimate for the *Step 0* of the quantum algorithm.

It has been shown elsewhere (Kieu, 2001a,b,c; Ruskai, 2002) that in general there should be no level crossing for the ground state except at the end points $t = 0, T$ where the adiabatic process can start or end with some obvious symmetry. Furthermore, the freedom in choosing the initial hamiltonians H_I and their ground states and in performing different adiabatic interpolations, not just as linear as in (9), might be exploited to enable the gap enlargement and to speed up the computation.

We shall employ the simple harmonic oscillators, i.e. Gaussian approximations, to obtain an estimate for the energy gap.

For the various a_i, $a_i^\dagger$ appearing in the interpolating Hamiltonian $\mathcal{H}(s)$ (9) at the time instant s, we use the Bogoliubov ansatz, with real $u_i(s)$ and $v_i(s)$,

$$c_i = u_i(s)a_i + v_i(s)a_i^\dagger,$$
$$a_i = u_i(s)b_i - v_i(s)c_i^\dagger. \tag{A1}$$

The c_i-zero occupation state is denoted by $|0_c\rangle$, where the s-dependence of the state is implicit. The canonicity $[c_i, c_j^\dagger] = \delta_{ij}$ demands

$$u_i^2(s) - v_i^2(s) = 1, \tag{A2}$$

upon which

$$\langle a_i^\dagger a_j\rangle = v_i^2(s)\delta_{ij},$$
$$\langle a_i^\dagger a_j^\dagger\rangle = \langle a_i a_j\rangle = -u_i(s)v_i(s)\delta_{ij}, \tag{A3}$$

where

$$\langle A_{k_i} A_{k_j}\rangle \equiv \langle 0_c|A_{k_i}A_{k_j}|0_c\rangle, \tag{A4}$$

We pay particular attention to the following terms

$$:a_i^\dagger a_i:_c = \big(u_i^2(s) + v_i^2(s)\big)c_i^\dagger c_i - u_i(s)v_i(s)\big(c_i^{\dagger 2} + c_i^2\big),$$
$$:a_i a_i:_c = -2u_i(s)v_i(s)c_i^\dagger c_i + v_i^2(s)c_i^{\dagger 2} + u_i^2(s)c_i^2. \tag{A5}$$

Needed next is a version of the Wick theorem (Itzykson and Zuber, 1985) for the ordinary product involving the operators $A_1, \ldots, A_n$,

$$A_1 \cdots A_n = \sum_{p=0}^{[n/2]} :A_1 \cdots \hat{A}_{k_1} \cdots \hat{A}_{k_{2p}} \cdots A_n:_c$$
$$\times \{\langle A_{k_1}A_{k_2}\rangle \cdots \langle A_{k_{2p-1}}A_{k_{2p}}\rangle + \text{permutations}\}, \tag{A6}$$

where the normal ordering $:\cdots:_c$ is done with respect to some annihilation operators c_i which annihilate some common state $|0_c\rangle$ for various i, $c_i|0_b\rangle = 0$. The Eq. (A6), in which the hatted operators are omitted from the normal ordering, is an exact result and can be proved by induction.

We can now list the various steps of our estimation:

1. We apply the Wick theorem, with respect to c_i's, to the Hamiltonian $\mathcal{H}(s)$ (9)

$$\mathcal{H}(s) = E_b(s)I$$
$$+ \sum_i \text{terms linear in } c_i \text{ and } c_i^\dagger$$
$$+ \sum_i \big(G_i(s)c_i^\dagger c_i + K_i(s)c_i^2 + K_i^*(s)c_i^{\dagger 2}\big)$$

$$+ \sum_{i \neq j} \text{terms involving } c_i^\dagger c_j,\ c_i c_j,\ c_i^\dagger c_j^\dagger$$

$$+ \sum_{ijk\cdots} \text{higher order, normal-ordered terms of } c \text{ and } c^\dagger. \quad \text{(A7)}$$

Note that in this process the higher order terms contribute to the coefficients of lower order ones through products of various expectation values in (A3). With help from (A3) and (A5), the various coefficients $E_b(s)$, $G_i(s)$, $K_i(s)$, ... in the right hand side above can be expressed as polynomials in $(u_i(s), v_i(s))$.

2. We next fix $u_i(s)$, and $v_i(s)$ numerically from (A2) and from the imposition that the coefficients $K_i(s) = 0$ in (A7). Then we can evaluate the coefficients $G_i(s)$ from their polynomial expressions in $(u_i(s), v_i(s))$. From (A7), on the other hand, we see also that

$$G_i(s) = \langle 1_{c_i}|\mathcal{H}(s)|1_{c_i}\rangle - \langle 0_c|\mathcal{H}(s)|0_c\rangle, \quad \text{(A8)}$$

where $|1_{c_i}\rangle = c_i^\dagger|0_c\rangle$. Mathematically, $\min_i|G_i(s)|$ thus provides some indication of the size of the energy gaps of $\mathcal{H}(s)$ around the energy level $E_b(s) = \langle 0_c|\mathcal{H}(s)|0_c\rangle$. Even though $|0_c\rangle$, obtained from the linear Bogoliubov transformations (A1), in general may not be the true ground state of $\mathcal{H}(s)$, we could use $\min_i|G_i(s)|$ as some indicator for the gap g in (13) to estimate T from the adiabaticity condition (11).

Some variations of the above method might yield a better estimate. For instance, one could numerically obtain $(u_i(s), v_i(s))$, and thus $\min_i|G_i(s)|$, by minimizing the energy $E_b(s)$ subjected to the constraints (A2) with or without the constraints $K_i(s) = 0$. The aim of this minimization, if possible, is to select a state $|0_c\rangle$ whose energy expectation value at the time s is as closed to that of the ground state at that instant as allowed by the linear Bogoliubov transformations. Other variations might be involving, instead of (A1), some nonlinear relations, for the canonicity only requires that a and c are to be unitarily transformed, $c = U^\dagger(a^\dagger, a)aU(a^\dagger, a)$.

The accuracy of the estimation and its higher order corrections can be evaluated systematically from the higher order terms in the last line of (A7). Numerical diagonalization of (A7) with a series of truncated bases in $|n_{c_i}\rangle$ of increasing sizes could further provide us more information about the gap thus obtained.

ACKNOWLEDGMENTS

I am indebted to Alan Head for discussions, comments, and suggestions. I also thank Cristian Calude, John Markham, Boris Pavlov, Andrew Rawlinson, and Khai Vu for discussions; Gregory Chaitin, Bryan Dalton, Ray Sawyer, Boris

Tsirelson and Ray Volkas for email correspondence; and K. Svozil, G. Etesi, and I. Németi for bringing their works to my attention.

NOTE ADDED IN PROOF

The author has recently obtained a criterion based on the final probability distribution, which can be measured to arbitrary precision, for identifying the ground state of H_P at time T. See Kieu (2003) for more details.

REFERENCES

Benioff, P. (1980). The computer as a physical system. *Journal of Statistical Physics* **22**, 563–591.

Bernstein, E. and Vazirani, U. (1997). Quantum complexity theory. *SIAM Journal of Computing* **26**, 1411.

Braunstein, S. (1998). Error correction for continuous variables. *Physical Review Letters* **80**, 4084.

Calude, C. S. and Pavlov, B. (2001). Coins, quantum measurements and Turing's barrier. *Preprint* quant-ph/0112087.

Childs, A. M., Farhi, E., and Preskill, J. (2001). Robusteness of adiabatic quantum computation. *Preprint* quant-ph/0108048.

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

Etesi, G. and Németi, I. (2001). Non-Turing computations via Malament-Hogarth space-times, gr-qc/0104023.

Farhi, E., Goldstone, J., Gutmann, S., and Sipser, M. (2000). Quantum computation by adiabatic evolution. *Preprint* quant-ph/0001106.

Feynman, R. P. (1982). Simulating physics with computers. *International Journal of Theoretical Physics* **21**, 467.

Grover, L. K. (1997). Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters* **79**, 325–328.

Itzykson, C. and Zuber, J.-B. (1985). *Quantum Field Theory*, McGraw-Hill, New York.

Kadowaki, T. and Nishimori, H. (1998). Quantum annealing in the transverse Ising model. *Physical Review E* **58**, 5355.

Kieu, T. D. (2001a). A reformulation of the Hilbert's tenth problem through Quantum Mechanics. *Preprint* quant-ph/0111063.

Kieu, T. D. (2001b). Gödel's Indompleteness, Chaitin's Ω and Quantum Physics, quant-ph/0111062.

Kieu, T. D. (2002). Computing the noncomputable. *Contemporary Physics* **44**, 51–71.

Kieu, T. D. (2003). Numerical simulations of a quantum algorithm for Hilbert's tenth problem. *Preprint* quant-ph/0304114.

Lloyd, S. and Braunstein, S. L. (1999). Quantum computation over continuous variables. *Physical Review Letters* **82**, 1784.

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

Nielsen, M. A. (1997). Computable functions, quantum measurements, and quantum dynamics, *Physical Review Letters* **79**, 2915–2918.

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

Ord, T. and Kieu, T. D. (2003). The diagonal method and hypercomputation. *Preprint* math-LO/0307020.

Ozawa, M. (1998). Measurability and computability. *Preprint* quant-ph/9809048.
Renyi, A. (1970). *Probability Theory*, North-Holland, New York.
Rogers, H., Jr. (1987). *Theory of Recursive Functions and Effective Computability*, MIT Press, Cambridge, MA.
Ruskai, M. B. (2002). Comments on adiabatic quantum algorithms. *Preprint* quant-ph/0203127.
Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal of Computing* **26**, 1484–1509.
Wooters, W. K. and Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature* **299**, 802–803.