Spectral Representation of Some Computably Enumerable Sets with an Application to Quantum Provability[*]

Cristian S. Calude[1],[**] and Kohtaro Tadaki[2],[***]

[1] Department of Computer Science, University of Auckland, Auckland, New Zealand
cristian@cs.auckland.ac.nz
[2] Research and Development Initiative, Chuo University, Tokyo, Japan
tadaki@kc.chuo-u.ac.jp

Abstract. We propose a new type of quantum computer which is used to prove a spectral representation for a class $\mathcal{S}$ of computable sets. When $S \in \mathcal{S}$ codes the theorems of a formal system, the quantum computer produces through measurement all theorems and proofs of the formal system. We conjecture that the spectral representation is valid for all computably enumerable sets. The conjecture implies that the theorems of a general formal system, like Peano Arithmetic or ZFC, can be produced through measurement; however, it is unlikely that the quantum computer can produce the proofs as well, as in the particular case of $\mathcal{S}$. The analysis suggests that showing the provability of a statement is different from writing up the proof of the statement.

1 Introduction

Mathematical results are accepted only if they have been proved: *the proof concludes with the proven statement, the theorem*. The proof comes first and justifies the theorem. Classically, there is no alternative scenario.

The genius mathematician Srinivasa Ramanujan discovered nearly 3900 results [2], many without proofs; nearly all his claims have been proven correct. Ramanujan first *recognised* a true statement and only later that statement was *proven*, hence accepted as a *theorem*. While we don't know how Ramanujan's mind was able to "discover" mathematical true facts, we can ask whether there is a way to understand, and possibly imitate, his approach.

In this paper a new type of quantum computer is used to prove a spectral representation for a class $\mathcal{S}$ of computable sets is proved. For every $S \in \mathcal{S}$ we construct a quantum system in such a way that the elements of S are exactly the eigenvalues of the Hermitian operator representing an observable of the quantum system, i.e. the spectrum of the operator. In particular, S can be represented by the energy of the associated quantum system. The operator associated to

---

$S \in \mathcal{S}$ has a special numerical form which guarantees that by measurement we get both the element and the proof that the element is in S. *We conjecture that the spectral representation is valid for all computably enumerable sets.*

When $S \in \mathcal{S}$ codes the theorems of a formal system, then the associated quantum computer produces through measurement the theorems of the formal system and their proofs. The conjecture implies that every theorem of a general (recursively axiomatisable) formal system, like Peano Arithmetic or ZFC, can be produced through measurement. However, we argue that in this general case the quantum procedure produces, like Ramanujan, only the true the statement, but not its proof. Of course, the proof can be algorithmically generated by a classical algorithm, albeit in a possibly very long time (such a computation makes sense only for statements recognised as "interesting"). For example, if the Riemann hypothesis is produced by the quantum procedure we will know that the famous hypothesis is true. However, to have a formal proof—whose existence is guaranteed by the correctness of the quantum procedure—we may need to run a very long classical procedure. The proof obtained in this way could be rather unsatisfactory, as it may not convey the "understanding", the reason for which the Riemann hypothesis holds true (see also [4]). Although such a proof may not make us "wiser" [1], it may stimulate the search for better arguments.

The paper is structured as follows. In Section 2 we present the basic quantum mechanical facts necessary for describing our quantum systems. In Section 3 we describe a class of computable sets for which we can prove in Section 4 the representability theorem and its application to quantum provability (in Section 5). In Section 6 we discuss the generalisation of the quantum procedure to all computably enumerable sets and in Section 7 its application to quantum provability for arbitrary formal systems.

2   Quantum Mechanical Facts

We start with some basic facts on quantum mechanics needed for this paper. The quantum mechanical arguments are presented at the level of mathematical rigour adopted in quantum mechanics textbooks written by physicists, for example, Dirac [5] and Mahan [8].

A state of a quantum system is represented by a vector in a Hilbert space $\mathcal{H}$. The vector and the space are called *state vector* and *state space*, respectively. The *dynamical variables* of a system are quantities such as the coordinates and the components of momentum and angular momentum of particles, and the energy of the system. They play a crucial role not only in classical mechanics but also in quantum mechanics. Dynamical variables in quantum mechanics are represented by Hermitian operators on the state space $\mathcal{H}$. A dynamical variable of the system is called an *observable* if all eigenvectors of the Hermitian operator representing it form a complete system for $\mathcal{H}$. Normally we assume that a measurement of any observable can be performed upon a quantum system in any state (if we ignore the constructive matter, which is one of the points of this paper).

The set of possible outcomes of a measurement of an observable $\mathcal{O}$ of a system is the eigenvalue spectrum of the Hermitian operator representing $\mathcal{O}$.

Let $\{|m, \lambda\rangle\}$ be a complete orthonormal system of eigenvectors of the Hermitian operator A representing an observable $\mathcal{O}$ such that $A|m, \lambda\rangle = m|m, \lambda\rangle$ for all eigenvalues m of A and all λ, where the parameter λ designates the degeneracy of the eigenspace of A. Suppose that a measurement of $\mathcal{O}$ is performed upon a quantum system in the state represented by a normalized vector $|\Psi\rangle \in \mathcal{H}$. Then the probability of getting the outcome m is given by $p(m) = \sum_\lambda |\langle m, \lambda|\Psi\rangle|^2$, where $\langle m, \lambda|\Psi\rangle$ denotes the inner product of the vectors $|m, \lambda\rangle$ and $|\Psi\rangle$. Moreover, given that the outcome m occurred, the state of the quantum system immediately after the measurement is represented by the normalized vector

$$\frac{1}{\sqrt{p(m)}} \sum_\lambda \langle m, \lambda|\Psi\rangle |m, \lambda\rangle.$$

The *commutator* between two operators A and B is defined to be $[A, B] := AB - BA$. Let $\mathcal{O}_1, \ldots, \mathcal{O}_k$ be observables of a quantum system and let $A_1, \ldots, A_k$ be the Hermitian operators which represent $\mathcal{O}_1, \ldots, \mathcal{O}_k$, respectively. If the Hermitian operators commute to each other, i.e., $[A_j, A_{j'}] = 0$ for all $j, j' = 1, \ldots, k$, then we can perform measurements of all $\mathcal{O}_1, \ldots, \mathcal{O}_k$ simultaneously upon the quantum system in any state. All dynamical variables which we will consider below are assumed to be observables, and we will identify any observable with the Hermitian operator which represents it.

In this paper we consider quantum systems consisting of vibrating particles. The simplest one is the quantum system of *one-dimensional harmonic oscillator*, which consists only of one particle vibrating in one-dimensional space. The dynamical variables needed to describe the system are just one coordinate x and its conjugate momentum p. The *energy* of the system is an observable, called *Hamiltonian*, and is defined in terms of x and p by

$$H = \frac{1}{2m}(p^2 + m^2\omega^2 x^2),$$

where m is the mass of the oscillating particle and ω is 2π times the frequency. The oscillation of the particle is quantized by the *fundamental quantum condition*

$$[x, p] = i\hbar, \tag{1}$$

where $\hbar$ is *Planck's constant*. The *annihilation operator* a of the system is defined by

$$a = \sqrt{\frac{m\omega}{2\hbar}} \left(x + \frac{ip}{m\omega}\right).$$

Its adjoint $a^\dagger$ is called a *creation operator*. The fundamental quantum condition (1) is then equivalently rewritten as

$$[a, a^\dagger] = 1, \tag{2}$$

and the Hamiltonian can be represented in the form

$$H = \hbar\omega\left(a^\dagger a + \frac{1}{2}\right) \tag{3}$$

in terms of the creation and annihilation operators. In order to determine the

values of energy possible in the system, we must solve the eigenvalue problem of H. This problem is reduced to the eigenvalue problem of the observable $N :=$ $a^\dagger a$, called a *number operator*. Using the condition (2), the eigenvalue spectrum of N is shown to equal the set $\mathbb{N}$ of all nonnegative integers. Each eigenspace of N is not degenerate, and the normalized eigenvector $|n\rangle$ of N belonging to an arbitrary eigenvalue $n \in \mathbb{N}$ is given by

$$|n\rangle = \frac{(a^\dagger)^n}{\sqrt{n!}}|0\rangle, \tag{4}$$

where $|0\rangle$ is the unique normalized vector up to a phase factor such that $a|0\rangle = 0$. Since N is an observable, the eigenvectors $\{|n\rangle\}$ forms a complete orthonormal system for the state space. It follows from (3) that the values of energy possible in the system are

$$E_n = \hbar\omega\left(n + \frac{1}{2}\right), \qquad (n = 0, 1, 2, \dots)$$

where the eigenvector of H belonging to an energy E_n is given by (4).

Next we consider the quantum system of *k-dimensional harmonic oscillators* which consists of k one-dimensional harmonic oscillators vibrating independently without no interaction. The dynamical variables needed to describe the system are k coordinates $x_1, \dots, x_k$ and their conjugate momenta $p_1, \dots, p_k$. The Hamiltonian of the system is

$$H = \sum_{j=1}^{k} \frac{1}{2m_j}(p_j^2 + m_j^2\omega_j^2 x_j^2), \tag{5}$$

where m_j is the mass of the jth one-dimensional harmonic oscillator and ω_j is 2π times its frequency. The vibrations of k oscillators are quantized by the fundamental quantum conditions

$$[x_j, p_{j'}] = i\hbar\delta_{jj'}, \qquad [x_j, x_{j'}] = [p_j, p_{j'}] = 0. \tag{6}$$

The annihilation operator a_j of the jth oscillator is defined by

$$a_j = \sqrt{\frac{m_j\omega_j}{2\hbar}}\left(x_j + \frac{ip_j}{m_j\omega_j}\right).$$

The adjoint $a_j^\dagger$ of a_j is the creation operator of the jth oscillator. The fundamental quantum condition (6) is then equivalently rewritten as

$$[a_j, a_{j'}^\dagger] = \delta_{jj'}, \tag{7}$$

$$[a_j, a_{j'}] = [a_j^\dagger, a_{j'}^\dagger] = 0. \tag{8}$$

and the Hamiltonian can be represented in the form

$$H = \sum_{j=1}^{k} \hbar\omega_j\left(N_j + \frac{1}{2}\right) \tag{9}$$

where $N_j := a_j^\dagger a_j$ is the number operator of the jth oscillator. In order to determine the values of energy possible in the system, we first solve the eigenvalue problems of the number operators $N_1, \dots, N_k$. We can do this simultaneously

for all N_j since the number operators commute to each other, i.e., $[N_j, N_{j'}] = 0$ for all $j, j' = 1, \ldots, k$, due to (7) and (8). The eigenvalue spectrum of each N_j is shown to equal $\mathbb{N}$ using (7). We define a vector $|n_1, \ldots, n_k\rangle$ as the tensor product $|n_1\rangle \otimes \cdots \otimes |n_k\rangle$ of $|n_1\rangle, \ldots, |n_k\rangle$, where each $|n_j\rangle$ is defined by (4) using a_j in place of a. For each j, the vector $|n_1, \ldots, n_k\rangle$ is a normalized eigenvector of N_j belonging to an eigenvalue $n_j \in \mathbb{N}$, i.e.,

$$N_j|n_1, \ldots, n_k\rangle = n_j|n_1, \ldots, n_k\rangle. \tag{10}$$

All the vectors $\{|n_1, \ldots, n_k\rangle\}$ form a complete orthonormal system for the state space. It follows from (9) that the values of energy possible in the system are

$$E_{n_1, \ldots, n_k} = \hbar \sum_{j=1}^{k} \omega_j \left(n_j + \frac{1}{2} \right), \qquad (n_1, \ldots, n_k = 0, 1, 2, \ldots)$$

The vector $|n_1, \ldots, n_k\rangle$ is an eigenvector of H belonging to an energy $E_{n_1, \ldots, n_k}$.

The Hamiltonian (5) describes the quantum system of k-dimensional harmonic oscillators where each oscillator does not interact with any others and moves independently. In a general quantum system consisting of k-dimensional harmonic oscillators, each oscillator strongly interacts with all others. Its Hamiltonian has the general form

$$P(a_1, \ldots, a_k, a_1^\dagger, \ldots, a_k^\dagger), \tag{11}$$

where $a_1, \ldots, a_k$ are creation operators satisfying the quantum conditions (7) and (8), and P is a polynomial in $2k$ variables with coefficients of complex numbers such that (11) is Hermitian.[1] For example, we can consider the quantum system of k-dimensional harmonic oscillators whose Hamiltonian is

$$H = \sum_j \hbar \omega_j \left(a_j^\dagger a_j + \frac{1}{2} \right) + \sum_{j \neq j'} g_{jj'} a_j^\dagger a_{j'}.$$

Here the *interaction terms* $g_{jj'} a_j^\dagger a_{j'}$ between the jth oscillator and the j'th oscillator with a real constant $g_{jj'}$ are added to the Hamiltonian (9). Note, however, that solving exactly the eigenvalue problem of an observable in the general form of (11) is not an easy task.

3   A Class of Unary Languages

In this section we introduce a class of unary languages for which the representability theorem proven in the next section holds true.

Let $\mathbb{N}^*$ be the set of all finite sequences $(x_1, \ldots, x_m)$ with elements in $\mathbb{N}$ ($m \in \mathbb{N}$; for $m = 0$ we get the empty sequence ε). Let

$$L((x_1 \ldots x_m), a) = \left(\prod_{i=1}^{m} \{1^{x_i}\}^* \right) \{1^a\}, \tag{12}$$

for all $(x_1, \ldots, x_m) \in \mathbb{N}^*, a \in \mathbb{N}$.

---

[1] In the monomials appearing in P, the order of the variables $x_1, \ldots, x_{2k}$ does not matter. However, since a_j and $a_j^\dagger$ do not commute, in substituting $a_1, \ldots, a_k, a_1^\dagger, \ldots, a_k^\dagger$ into the variables of P the order of these operators makes a difference. Thus, the operator (11) makes sense only by specifying this order.

Theorem 1. *Let $\mathcal{L}_0$ be the minimal class of languages $\mathcal{L}$ over $\{1\}$ containing the languages $\{1^n\}$ for every $n \in \mathbb{N}$, and which is closed under concatenation and the Kleene star operation. Then, $\mathcal{L}_0 = \{L((x_1, \ldots, x_m), a) \mid (x_1, \ldots, x_m) \in \mathbb{N}^*, a \in \mathbb{N}\}$.*

Proof. The class $\mathcal{L}_0$ has the required properties because $L(\varepsilon, a) = \{1^a\}$, the concatenation of $L((x_1, \ldots, x_m, a)$ and $L((y_1, \ldots, y_l), b)$ is $L((x_1, \ldots, x_m), a)L((y_1, \ldots, y_l), b) = L((x_1, \ldots, x_m, y_1, \ldots, y_l), a + b)$ and the Kleene star of $L((x_1, \ldots, x_m), a)$ is $L((x_1, \ldots, x_m), a)^* = L((x_1, \ldots, x_m, a), 0)$. In view of (12), $\mathcal{L}_0$ is included in every class $\mathcal{L}$ satisfying the properties in the statement of the theorem. $\qquad\square$

Corollary 2. *The class $\mathcal{L}_0$ coincides with the minimal class of languages $\mathcal{L}$ over $\{1\}$ which contains the languages $\{1^n\}$ and $\{1^n\}^*$, for every $n \in \mathbb{N}$ and which is closed under concatenation.*

Comment 3. *i) If L is a finite unary language with more than one element, then $L \notin \mathcal{L}_0$.*
ii) The family $\mathcal{L}_0$ is a proper subset of the class of regular (equivalently, context-free) languages.
iii) The language $\{1^p \mid p \text{ is prime}\}$ is not in $\mathcal{L}_0$.

Consider the minimal class $\mathcal{D}_0$ of subsets of $\mathbb{N}$ containing the sets $\{b\}$, for every $b \in \mathbb{N}$, and which is closed under the sum and the Kleene star operation. Here the sum of the sets S, T is the set $S + T = \{a + b \mid a \in S, b \in T\}$; the Kleene star of the set S is the set $S^* = \{a_1 + a_2 + \cdots + a_k \mid k \geq 0, a_i \in S, 1 \leq i \leq k\}$.

Theorem 4. *The following equality holds true: $\mathcal{L}_0 = \{\{1^a \mid a \in S\} \mid S \in \mathcal{D}_0\}$.*

Based on the above theorem, we identify $\mathcal{L}_0$ with $\mathcal{D}_0$ in what follows.

4   The Representation Theorem

Can a set $S \in \mathcal{D}_0$ be represented as the outcomes of a quantum measurement? We answer this question in the affirmative. First we show that the sets in $\mathcal{D}_0$ can be generated by polynomials with nonnegative integer coefficients.

Proposition 5. *For every set $S \in \mathcal{D}_0$ there exists a polynomial with nonnegative integer coefficients F_S in variables $x_1, \ldots, x_k$ such that S can be represented as:*

$$S = \{F_S(n_1, \ldots, n_k) \mid n_1, \ldots, n_k \in \mathbb{N}\}. \tag{13}$$

Proof. Suppose that $S \in \mathcal{D}_0$. It follows from Theorem 4 and (12) that there exist $a_1, \ldots, a_k, a \in \mathbb{N}$ such that $S = \{a_1 n_1 + \cdots + a_k n_k + a \mid n_1, \ldots, n_k \in \mathbb{N}\}$. Thus, (13) holds for the polynomial $F_S(x_1, \ldots, x_k) = a_1 x_1 + \cdots + a_k x_k + a$. $\qquad\square$

Comment 6. *There exist infinitely many sets not in $\mathcal{D}_0$ which are representable in the form (13).*

Motivated by Proposition 5, we show that every set

$$S = \{F(n_1, \ldots, n_k) \mid n_1, \ldots, n_k \in \mathbb{N}\}, \tag{14}$$

where F is a polynomial in k variables with nonnegative integer coefficients, can be represented by the set of outcomes of a *constructive* quantum measurement. For this purpose, we focus on a quantum system consisting of k-dimensional harmonic oscillators whose Hamiltonian has the form

$$H = F(N_1, \ldots, N_k), \tag{15}$$

where $N_1, \ldots, N_k$ is the number operators defined by $N_j = a_j^\dagger a_j$ with the annihilation operator a_j of the jth oscillator. Note that the substitution of $N_1, \ldots, N_k$ into the variables of F is unambiguously defined since the number operators $N_1, \ldots, N_k$ commute to each other.

We say an observable of the form (11) is *constructive* if all coefficients of P are in the form of $p + qi$ with $p, q \in \mathbb{Q}$. Thus, the Hamiltonian (15) is constructive by definition. Actually, a measurement of the Hamiltonian (15) can be performed *constructively* in an intuitive sense. The constructive measurement consists of the following two steps: First, the simultaneous measurements of the number operators $N_1, \ldots, N_k$ are performed upon the quantum system to produce the outcomes $n_1, \ldots, n_k \in \mathbb{N}$ for $N_1, \ldots, N_k$, respectively. This is possible since the number operators commute to each other. Secondly, $F(n_1, \ldots, n_k)$ is calculated and is regarded as the outcome of the measurement of the Hamiltonian (15) itself. This is constructively possible since F is a polynomial with integer coefficients. Thus, the whole measurement process is constructive in an intuitive sense too.

Theorem 7. *For every set S of the form (14) there exists a constructive Hamiltonian H such that the set of all possible outcomes of a measurement of H is S.*

Proof. Consider the Hamiltonian H of the form (15). It is constructive, as we saw above. We show that the eigenvalue spectrum of H equals to S.

First, using (10) we get

$$F(N_1, \ldots, N_k)|n_1, \ldots, n_k\rangle = F(n_1, \ldots, n_k)|n_1, \ldots, n_k\rangle \tag{16}$$

for every $n_1, \ldots, n_k \in \mathbb{N}$. Thus, every element of S is an eigenvalue of H. Conversely, suppose that E is an arbitrary eigenvalue of H. Then there exists a nonzero vector $|\Psi\rangle$ such that $H|\Psi\rangle = E|\Psi\rangle$. Since all vectors $\{|n_1, \ldots, n_k\rangle\}$ form a complete orthonormal system for the state space, there exist complex numbers $\{c_{n_1, \ldots, n_k}\}$ such that $|\Psi\rangle = \sum_{n_1, \ldots, n_k} c_{n_1, \ldots, n_k}|n_1, \ldots, n_k\rangle$. It follows from (16) that

$$\sum_{n_1, \ldots, n_k} c_{n_1, \ldots, n_k} F(n_1, \ldots, n_k)|n_1, \ldots, n_k\rangle = \sum_{n_1, \ldots, n_k} c_{n_1, \ldots, n_k} E|n_1, \ldots, n_k\rangle.$$

Since the vectors $\{|n_1, \ldots, n_k\rangle\}$ are independent, we have

$$c_{n_1, \ldots, n_k}(E - F(n_1, \ldots, n_k)) = 0, \tag{17}$$

for all $n_1, \ldots, n_k \in \mathbb{N}$. Since $|\Psi\rangle$ is nonzero, $c_{\bar{n}_1, \ldots, \bar{n}_k}$ is also nonzero for some $\bar{n}_1, \ldots, \bar{n}_k \in \mathbb{N}$. It follows from (17) that $E = F(\bar{n}_1, \ldots, \bar{n}_k)$. □

5   An Application to Quantum Provability

Let S be a set of the form (14). In the proof of Theorem 7, we consider the measurement of the Hamiltonian of the form (15). In the case where the state $|\Psi\rangle$ over which the measurement of the Hamiltonian is performed is chosen randomly, an element of S is generated randomly as the measurement outcome. In this manner, by infinitely many repeated measurements we get exactly the set S.

If the set S codes the "theorems" of a formal system $\mathcal{S}$—which is possible as S is computable—then $F(n_1, \ldots, n_k) \in S$ is a *theorem* of $\mathcal{S}$ and the numbers $n_1, \ldots, n_k$ play the role of the *proof* which certifies it.

Suppose that a *single* measurement of the Hamiltonian of the form (15) was performed upon a quantum system in a state represented by a normalized vector $|\Psi\rangle$ to produce an outcome $m \in S$, i.e., a theorem. Then, by the definition of theorems, there exists a proof $n_1, \ldots, n_k$ which makes m a theorem, i.e., which satisfies $m = F(n_1, \ldots, n_k)$. Can we extract the proof $n_1, \ldots, n_k$ after the measurement? This can be possible in the following manner: Immediately after the measurement, the system is in the state represented by the normalized vector $|\Phi\rangle$ given by

$$|\Phi\rangle = \frac{1}{\sqrt{C}} \sum_{m=F(n_1,\ldots,n_k)} \langle n_1, \ldots, n_k | \Psi \rangle | n_1, \ldots, n_k \rangle,$$

where C is the probability of getting the outcome m in the measurement given:

$$C = \sum_{m=F(n_1,\ldots,n_k)} |\langle n_1, \ldots, n_k | \Psi \rangle|^2.$$

Since the number operators $N_1, \ldots, N_k$ commute to each other, we can perform the simultaneous measurements of $N_1, \ldots, N_k$ upon the system in the state $|\Phi\rangle$. Hence, by performing the measurements of $N_1, \ldots, N_k$, we obtain any particular outcome $n_1, \ldots, n_k$ with probability $|\langle n_1, \ldots, n_k | \Phi \rangle|^2$. Note that

$$\sum_{m=F(n_1,\ldots,n_k)} |\langle n_1, \ldots, n_k | \Phi \rangle|^2 = \sum_{m=F(n_1,\ldots,n_k)} |\langle n_1, \ldots, n_k | \Psi \rangle|^2 / C = 1.$$

Thus, with probability one we obtain some outcome $n_1, \ldots, n_k$ such that $m = F(n_1, \ldots, n_k)$. In this manner we can immediately extract the proof $n_1, \ldots, n_k$ of the theorem $m \in S$ obtained as a measurement outcome.

6   A Conjecture

In the early 1970s, Matijasevič, Robinson, Davis, and Putnam solved negatively Hilbert's tenth problem by proving the MRDP theorem (see Matijasevič [9] for details) which states that every computably enumerable subset of $\mathbb{N}$ is Diophantine. A subset S of $\mathbb{N}$ is called *computably enumerable* if there exists a (classical) Turing machine that, when given $n \in \mathbb{N}$ as an input, eventually halts if $n \in S$ and otherwise runs forever. A subset S of $\mathbb{N}$ is *Diophantine* if there exists a polynomial $P(x, y_1, \ldots, y_k)$ in variables $x, y_1, \ldots, y_k$ with

integer coefficients such that, for every $n \in \mathbb{N}$, $n \in S$ if and only if there exist $m_1, \ldots, m_k \in \mathbb{N}$ for which $P(n, m_1, \ldots, m_k) = 0$.

Inspired by the MRDP theorem, we conjecture the following:

Conjecture 8 *For every computably enumerable subset S of $\mathbb{N}$, there exists a constructive observable A of the form of* (11) *whose eigenvalue spectrum equals S.*

Conjecture 8 implies that when we perform a measurement of the observable A, a member of the computably enumerable S is stochastically obtained as a measurement outcome. As we indefinitely repeat measurements of A, members of S are being enumerated, just like a Turing machine enumerates S.

In this way a new type of quantum mechanical computer is postulated to exist. How can we construct it? Below we discuss some properties of this hypothetical quantum computer.

As in the proof of the MRDP theorem—in which a whole computation history of a Turing machine is encoded in (the base-two expansions of) the values of variables of a Diophantine equation—*a whole computation history of a Turing machine is encoded in a single quantum state which does not make time-evolution (in the Schrödinger picture).* Namely, a whole computation history of the Turing machine M which recognises S is encoded in an eigenstate of the observable A which is designed appropriately using the creation and annihilation operators. To be precise, let $|\Psi\rangle = \sum_{n_1,\ldots,n_k} c_{n_1,\ldots,n_k} |n_1, \ldots, n_k\rangle$ be an eigenvector of A belonging to an eigenvalue $n \in S$ such that each coefficient $c_{n_1,\ldots,n_k}$ is drawn from a certain finite set $\mathcal{C}$ of complex numbers containing 0 and the set $\{(n_1, \ldots, n_k) \mid c_{n_1,\ldots,n_k} \neq 0\}$ is finite. The whole computation history of M with the input n is encoded in the coefficients $\{c_{n_1,\ldots,n_k}\}$ of $|\Psi\rangle$ such that each finite subset obtained by dividing appropriately $\{c_{n_1,\ldots,n_k}\}$ represents the configuration (i.e., the triple of the state, the tape contents, and the head location) of the Turing machine M at the corresponding time step. The observable A is constructed such that its eigenvector encodes the whole computation history of M, using the properties of the creation and annihilation operators such as

$$a_j^\dagger |n_1, \ldots, n_{j-1}, n_j, n_{j+1}, \ldots, n_k\rangle = \sqrt{n_j + 1}|n_1, \ldots, n_{j-1}, n_j + 1, n_{j+1}, \ldots, n_k\rangle,$$

by which the different time steps are connected in the manner corresponding to the Turing machine computation of M. In the case of $n \notin S$, the machine M with the input n does not halt. Consequently, the length of the whole computation history is infinite and therefore the set $\{(n_1, \ldots, n_k) \mid c_{n_1,\ldots,n_k} \neq 0\}$ is infinite, which implies, because all coefficients belong to the finite set $\mathcal{C}$ of complex numbers, that the norm of $|\Psi\rangle$ is indefinite and hence $|\Psi\rangle$ is not an eigenvector of A. In this manner, any eigenvalue of A is limited to a member of S.

Note that there are many computation histories of a Turing machine depending on its input. In the proposed quantum mechanical computer, the measurement of A chooses one of the computation histories stochastically and the input corresponding to the computation history is obtained as a measurement outcome. The above analysis shows that Conjecture 8 is likely to be true.

The main feature of the proposed quantum mechanical computer is that *the evolution of computation does not correspond to the time-evolution of the underlying quantum system.* Hence, in contrast with a conventional quantum computer, the evolution of computation does not have to form a unitary time-evolution, so it is not negatively influenced by *decoherence*[2], a serious obstacle to the physical realisation of a conventional quantum computer.

Again, in contrast with a conventional quantum computer, this proposed quantum mechanical computer can be physically realisable even as a solid-state device at room temperature (the lattice vibration of solid crystal, i.e., *phonons*), which strongly interacts with the external environment. A member of S is obtained as a measurement outcome in an instant by measuring the observable A. For example, in the case when the observable A is the Hamiltonian of a quantum system, the measurement outcome corresponds to the energy of the system. In this case, we can probabilistically decide—with sufficiently small error probability—whether a given $n \in \mathbb{N}$ is in S: the quantum system is first prepared in a state $|\Psi\rangle$ such that the expectation value $\langle\Psi|A|\Psi\rangle$ of the measurement of the energy over $|\Psi\rangle$ is approximately n, and then the measurement is actually performed. This computation deciding the membership of n to S terminates in an instant if sufficiently high amount of energy (i.e., around n) is pumped.

Kieu [7] proposed a quantum computation based on a Hamiltonian of the form of (15), which is a very special case of (11) used in Conjecture 8. The purpose and method of Kieu's are both quite different from ours. His purpose is to perform hypercomputation, i.e., to solve the membership problem for every c.e. set. On the other hand, his method is based on adiabatic quantum computation and uses the MRDP theorem in a direct manner. Kieu uses only ground states (i.e., the quantum states with the lowest energy), while the whole energy spectrum is needed in our approach. These facts suggest that his method may not be useful for proving Conjecture 8.

7   Quantum Proving without Giving the Proof

In Section 5 we discussed the quantum provability for a formal system whose theorems can be coded by a set S defined as in (14). When an element m is obtained as an outcome of the measurement, we can extract the proof $n_1, \ldots, n_k$ which certifies that m is a theorem of the formal system $\mathcal{S}$, i.e., it satisfies $m = F(n_1, \ldots, n_k)$, by performing the second measurement over the state immediately after the first measurement.

Actually, the proof $n_1, \ldots, n_k$ may be generated slightly before the theorem $F(n_1, \ldots, n_k)$ is obtained, like in the classical scenario. As we saw in Section 4, the measurement of $F(N_1, \ldots, N_k)$ can first be performed by simultaneous measurements of the number operators $N_1, \ldots, N_k$ to produce the

---

[2] Decoherence, which is induced by the interaction of quantum registers with the external environment, destroys the superposition of states of the quantum registers, which plays an essential role in a conventional quantum computation.

outcomes $n_1, \ldots, n_k \in \mathbb{N}$; then, the theorem $m = F(n_1, \ldots, n_k)$, classically calculated from $n_1, \ldots, n_k$, can be regarded as the outcome of the measurement of $F(N_1, \ldots, N_k)$ itself.

In general, the set of all theorems of a (recursively axiomatisable) formal system, such as Peano Arithmetic or ZFC, forms a computably enumerable set and not a computable set of the form (14). In what follows, we argue the plausibility that, for general formal systems, the proof cannot be obtained immediately after the theorem was obtained via the quantum procedure proposed in the previous section.

Fix a formal system whose theorems form a computably enumerable set. As before we identify a formula with a natural number. Let M be a Turing machine such that, given a formula F as an input, M searches all proofs one by one and halts if M finds the proof of F. Assume that Conjecture 8 holds. Then there exists an observable A of an infinite dimensional quantum system such that A is constructive and the eigenvalue spectrum of A is exactly the set of all provable formulae. Thus, we obtain a provable formula as a measurement outcome each time we perform a measurement of A; it is stochastically determined which provable formula is obtained. The probability of getting a specific provable formula F as a measurement outcome depends on the choice of the state $|\Psi\rangle$ on which we perform the measurement of A. In some cases the probability can be very low, and therefore we may be able to get the provable formula F as a measurement outcome only once, even if we repeat the measurement of A on $|\Psi\rangle$ many times.

Suppose that, in this manner, we have performed the measurement of A once and then we have obtained a specific provable formula F as a measurement outcome. Then, where is the proof of F? In the quantum mechanical computer discussed in Section 6, the computation history of the Turing machine M is encoded in an eigenstate of the observable A, hence the proof of F is encoded in the eigenstate of A, which is the state of the underlying quantum system immediately after the measurement.

Is it possible to extract the proof of F from this eigenstate? In order to extract the proof of F from this eigenstate, it is necessary to perform an additional measurement on this eigenstate. However, it is impossible to determine the eigenstate in terms of the basis $\{|n_1, \ldots, n_k\rangle\}$ completely by a *single* measurement due the principle of quantum mechanics. In other words, there does not exist a POVM measurement which can determine all the expansion coefficients $\{c_{n_1, \ldots, n_k}\}$ of the eigenstate with respect to the basis $\{|n_1, \ldots, n_k\rangle\}$ up to a global factor with nonzero probability. This eigenstate is destroyed after the additional measurement and therefore we cannot perform any measurement on it any more. We cannot copy the eigenstate prior to the additional measurement due to the no-cloning theorem (see [3]); and even if we start again from the measurement of A, we may have little chance of getting the same provable formula F as a measurement outcome.

The above analysis suggests that even if we get a certain provable formula F as a measurement outcome through the measurement of A it is very difficult

or unlikely to simultaneously obtain the proof of F.[3] This argument suggests that *for a general formal system proving that a formula is a theorem is different from writing up the proof of the formula.* Of course, since F is provable, there is a proof of F, hence the Turing machine M with the input F will eventually produce that proof. However, this classical computation may take a long time in contrast with the fact—via the measurement of A—it took only a moment to know that the formula F is provable.

As mathematicians guess true facts for no apparent reason we can speculate that human intuition might work as in the above described quantum scenario. As the proposed quantum mechanical computer can operate at room temperature it may be even possible that a similar quantum mechanical process works in the human brain those offering an argument in favour of the quantum mind hypothesis [10]. The argument against this proposition according to which quantum systems in the brain decohere quickly and cannot control brain function (see [11]) could be less relevant as decoherence plays no role in the quantum computation discussed here.

References

1. Aigner, M., Schmidt, V.A.: Good proofs are proofs that make us wiser: interview with Yu. I. Manin. The Berlin Intelligencer, 16–19 (1998),
   `http://www.ega-math.narod.ru/Math/Manin.html`
2. Berndt, B.C.: Ramanujan's Notebooks, Part V. Springer, Heidelberg (2005)
3. Buzek, V., Hillery, M.: Quantum cloning. Physics World 14(11), 25–29 (2001)
4. Calude, C.S., Calude, E., Marcus, S.: Proving and programming. In: Calude, C.S. (ed.) Randomness & Complexity, from Leibniz to Chaitin, pp. 310–321. World Scientific, Singapore (2007)
5. Dirac, P.A.M.: The Principles of Quantum Mechanics, 4th edn. Oxford University Press, London (1958)
6. Hiai, F., Yanagi, K.: Hilbert Spaces and Linear Operators. Makino-Shoten (1995) (in Japanese)
7. Kieu, T.D.: A reformulation of Hilbert's tenth problem through quantum mechanics. Proc. R. Soc. Lond. A 460, 1535–1545 (2004)
8. Mahan, G.D.: Many-Particle Physics, 3rd edn. Kluwer Academic/Plenum Publishers, New York (2010)
9. Matijasevič, Y.V.: Hilbert's Tenth Problem. The MIT Press, Cambridge (1993)
10. Penrose, R., Hameroff, S.: Consciousness in the universe: Neuroscience, quantum space-time geometry and Orch OR theory. Journal of Cosmology 14 (2011),
    `http://journalofcosmology.com/Consciousness160.html`
11. Tegmark, M.: Importance of quantum decoherence in brain processes. Physical Review E 61(4), 4194–4206 (2000)

---

[3] For the formal system $\mathcal{S}$ in Section 5, we can obtain a theorem and its proof simultaneously via measurements since the observable $F(N_1, \ldots, N_k)$ whose measurements produce "theorems" is a function of the commuting observables $N_1, \ldots, N_k$ whose measurements produce "proofs". However, this is unlikely to be true for general formal systems.