Quantum Proving Without Giving the Proof

Kohtaro Tadaki

Research and Development Initiative, Chuo University
Tokyo, Japan

Joint work with Cristian S. Calude

Supported by JSPS KAKENHI, Grant-in-Aid for Challenging Exploratory Research (23650001)
Abstract

We propose a new type of quantum computer which is based on a spectral representation for a class $\mathcal{FS}$ of computable sets. When a set in $\mathcal{FS}$ codes the theorems of a formal system, the quantum computer produces through measurement all theorems 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 $\mathcal{FS}$ where a theorem and its proof can be simultaneously produced.

The analysis suggests that showing the provability of a statement is different from writing up the proof of the statement.
Proof and Provable Formula

**Formula**  In a general formal system, such as Peano Arithmetic or ZFC, a *formula* is a finite string over a certain alphabet with a certain property.

**Proof**  A *proof* is a sequence of formulae

\[ F_1, F_2, F_3, \ldots, F_n \]

such that each \( F_i \) is either an axiom, or \( F_i \) is obtained by applying an inference rule to \( F_{m_1}, F_{m_2}, \ldots, F_{m_k} \) with \( m_1, \ldots, m_k < i \).

**Provability**  A formula \( F \) is called *provable* (or a *theorem*) if there exists a proof \( F_1, F_2, F_3, \ldots, F_n \) such that \( F_n \) is exactly \( F \).

Thus, showing a formula provable can be regarded as solving a certain kind of combinatorial problem about the *existence* of a sequence of finite strings with a certain property. Then, *can we show a formula provable without writing up the proof of the formula?*
Metaphorical Example from Computational Complexity Theory

We may consider a formal system where
(i) a formula is exactly a positive integer, and
(ii) a proof of a formula $n$ is a nontrivial factor of $n$. Thus, a provable formula is exactly a composite number.

Fact in Computational Complexity Theory

There exists an efficient primality test. Namely, there exists a polynomial-time algorithm which can decide whether a given positive integer is composite, or not.

$\Rightarrow$ Deciding whether a given formula is provable, or not, is computationally easy in the formal system.

Belief in Modern Cryptography

Factoring a composite number is computationally hard. Namely, there does not exit a polynomial-time algorithm which can find a non-trivial factor of a given composite number.

$\Rightarrow$ Writing up the proof of a provable formula is likely computationally hard in the formal system.
Aim of This Talk

In the metaphorical formal system, showing the provability of a provable formula seems computationally easier than writing up the proof of the provable formula.

The aim of this talk is to consider the possibility that the same happens in a general formal system, such as Peano Arithmetic or ZFC, whose provable formulae form a computably enumerable set and not a computable set, as in the metaphorical formal system, based on quantum mechanics.
Quantum Mechanics
Basic Ingredients in Quantum Mechanics

• A state of a quantum system is represented by a vector in a Hilbert space \( \mathcal{H} \). The vector and the space are called \textit{state vector} and \textit{state space}, respectively.

• The \textit{dynamical variables} of a system are quantities such as the coordinates and the components of momentum 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 \textit{Hermitian operators} on the state space \( \mathcal{H} \).

• A dynamical variable of the system is called an \textit{observable} if all eigenvectors of the Hermitian operator representing it form a basis for \( \mathcal{H} \).

• All dynamical variables which we will consider below are \textit{assumed to be observables}, and we will identify any observable with the Hermitian operator which represents it.

• 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 talk).
Basic Ingredients in Quantum Mechanics

Postulate [Quantum Measurements I]

The set of possible outcomes of a measurement of an observable $A$ of a system is the eigenvalue spectrum of $A$.  

\[ \square \]
Examples of Quantum Systems
Example 1

One-Dimensional Harmonic Oscillator
Example 1: One-Dimensional Harmonic Oscillator

- The quantum system of one-dimensional harmonic oscillator 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

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

where $m$ is the mass of the oscillating particle and $\omega$ is $2\pi$ times the frequency of vibration.

- The commutator between two operators $A$ and $B$ is defined to be

\[
[A, B] := AB - BA.
\]

The oscillation of the particle is quantized by the fundamental quantum condition

\[
[x, p] = i\hbar,
\]

where $\hbar$ is Planck’s constant.
Example 1: One-Dimensional Harmonic Oscillator

- 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**.

- In terms of the creation and annihilation operators, the fundamental quantum condition is equivalently rewritten as

$$[a, a\dagger] = 1.$$

- The Hamiltonian can be also represented in the form

$$H = \hbar\omega \left( N + \frac{1}{2} \right),$$

where $N := a\dagger a$ is an observable, called a **number operator**.
Example 1: One-Dimensional Harmonic Oscillator

- In order to determine the values of energy possible in the system, based on the postulate we must solve the eigenvalue problem of $H$. This problem is reduced to the eigenvalue problem of the number operator $N := a^\dagger a$.

- Using the fundamental quantum condition $[a, a^\dagger] = 1$, the eigenvalue spectrum of $N$ is shown to equal the set $\mathbb{N}$ of all nonnegative integers.

- The eigenvector of $N$ belonging to an arbitrary eigenvalue $n \in \mathbb{N}$ is given by

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

  (1)

  where $a|0\rangle = 0$.

- Hence, the values of energy possible in the system are

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

  where the eigenvector of $H$ belonging to an energy $E_n$ is given by (1).
Example 2

\(\kappa\)-Dimensional Harmonic Oscillators
Example 2: $k$-Dimensional Harmonic Oscillators

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

- The Hamiltonian of the system is

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

where $m_j$ is the mass of the $j$th one-dimensional harmonic oscillator and $\omega_j$ is $2\pi$ times the frequency of its vibration.

- The vibrations of $k$ oscillators are quantized by the fundamental quantum conditions

\[ [x_j, p_{j'}] = i\hbar \delta_{jj'}, \quad [x_j, x_{j'}] = [p_j, p_{j'}] = 0. \]
**Example 2: $k$-Dimensional Harmonic Oscillators**

- The annihilation operator $a_j$ of the $j$th 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 $j$th oscillator.

- In terms of the creation and annihilation operators, the fundamental quantum condition is equivalently rewritten as
  \[
  [a_j, a_{j'}^\dagger] = \delta_{jj'}, \quad [a_j, a_j] = [a_{j'}^\dagger, a_{j'}^\dagger] = 0.
  \]

- The Hamiltonian can be also represented in the form
  \[
  H = \sum_{j=1}^{k} \frac{\hbar \omega_j}{2} \left(N_j + \frac{1}{2}\right)
  \]
  where $N_j := a_j^\dagger a_j$ is the number operator of the $j$th oscillator.
Example 2: $k$-Dimensional Harmonic Oscillators

- In order to determine the values of energy possible in the system, we first solve the eigenvalue problems of the number operators $N_1, \ldots, N_k$.

- The eigenvalue spectrum of each $N_j$ is shown to equal $\mathbb{N}$.

- 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 (1) using $a_j$ in place of $a$. For each $j$, the vector $|n_1, \ldots, n_k\rangle$ is an eigenvector of $N_j$ belonging to an eigenvalue $n_j \in \mathbb{N}$, i.e.,

$$N_j|n_1, \ldots, n_k\rangle = n_j|n_1, \ldots, n_k\rangle.$$ 

- Hence, the values of energy possible in the system are

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

The vector $|n_1, \ldots, n_k\rangle$ is an eigenvector of $H$ belonging to an energy $E_{n_1, \ldots, n_k}$.
Interacting
$k$-Dimensional Harmonic Oscillators
The previous example of Hamiltonian 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

$$H = P(a_1, \ldots, a_k, a_1^\dagger, \ldots, a_k^\dagger),$$

where $a_1, \ldots, a_k$ are creation operators satisfying the fundamental quantum conditions

$$[a_j, a_{j'}^\dagger] = \delta_{jj'}, \quad [a_j, a_{j'}] = [a_j^\dagger, a_{j'}^\dagger] = 0,$$

and $P$ is a polynomial in $2k$ variables with coefficients of complex numbers such that (2) is Hermitian.
• 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 $j$th oscillator and the $j'$th oscillator with a real constant $g_{jj'}$ are added to the Hamiltonian describing the (non-interacting) $k$-dimensional harmonic oscillators.
A Class of Unary Languages
A Class of Unary Languages

We introduce a class of unary languages for which the representability theorem proven later holds true.

**Definition** Let $\mathbb{N}^*$ be the set of all finite sequences $(x_1, \ldots, x_m)$ with elements in $\mathbb{N}$ ($m \in \mathbb{N}$). Let

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

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

**Theorem** 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,

$$\mathcal{L}_0 = \{L((x_1, \ldots, x_m), a) \mid (x_1, \ldots, x_m) \in \mathbb{N}^*, a \in \mathbb{N}\}. \hfill \square$$

**Remark**

- If $L$ is a finite unary language with more than one element, then $L \notin \mathcal{L}_0$.
- The family $\mathcal{L}_0$ is a proper subset of the class of regular (equivalently, context-free) languages.
A Class of Unary Languages: Reformulation of $L_0$

Consider the minimal class $D_0$ 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 $S, T \subset \mathbb{N}$ is the set

$$S + T = \{a + b \mid a \in S, b \in T\};$$

the Kleene star of the set $S \subset \mathbb{N}$ 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** The following equality holds true:

$$L_0 = \{\{1^a \mid a \in S\} \mid S \in D_0\}.$$

Based on the above theorem, we identify $L_0$ with $D_0$ in what follows.
The Representation Theorem
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** 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:

$$S = \{ F_S(n_1, \ldots, n_k) \mid n_1, \ldots, n_k \in \mathbb{N} \}.$$
The Representation Theorem

• Motivated by the above proposition, we show that every set

\[ S = \{ F(n_1, \ldots, n_k) \mid n_1, \ldots, n_k \in \mathbb{N} \}, \]

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

\[ H = F(N_1, \ldots, N_k), \]

where \( N_1, \ldots, N_k \) is the number operators defined by \( N_j = a_j^\dagger a_j \).

This type of Hamiltonian is a special case of the general form of interacting \( k \)-dimensional harmonic oscillators.
The Representation Theorem

**Definition** We say an observable of the form \( P(a_1, \ldots, a_k, a_1^\dagger, \ldots, a_k^\dagger) \) is **constructive** if all coefficients of \( P \) are in the form of \( p + qi \) with \( p, q \in \mathbb{Q} \).

- Thus, the Hamiltonian \( F(N_1, \ldots, N_k) \) is constructive by definition.

- Actually, a measurement of the Hamiltonian \( F(N_1, \ldots, N_k) \) can be performed **constructively** in an intuitive sense. The constructive measurement consists of the following two steps:

  (i) 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.

  (ii) Secondly, \( F(n_1, \ldots, n_k) \) is calculated and is regarded as the outcome of the measurement of the Hamiltonian \( F(N_1, \ldots, N_k) \) 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.
The Representation Theorem

Theorem [Representation Theorem] For every set $S$ of the form

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

there exists a constructive Hamiltonian $H$, i.e., $F(N_1, \ldots, N_k)$, such that the set of all possible outcomes of a measurement of $H$ is $S$. □

- In the proof, we consider the measurement of the Hamiltonian

$$H = F(N_1, \ldots, N_k).$$

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 $S$. 
An Application to Quantum Provability
An Application to Quantum Provability

Regarding $S$ as a formal system

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

In $FS$, the proof is obtained immediately after a theorem is obtained

Suppose that a single measurement of the Hamiltonian $H = F(N_1,\ldots,N_k)$ was performed upon a quantum system to produce an outcome $m \in S$, i.e., a theorem of $FS$.

Then, by the definition of theorems, there exists a proof $n_1,\ldots,n_k$ 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 by performing additional simultaneous measurements of $N_1,\ldots,N_k$ immediately after the first measurement based on the postulate of quantum measurements.

Thus we can immediately extract the proof of a theorem after the theorem is obtained as a measurement outcome.
An Application to Quantum Provability

**Postulate** [Quantum Measurements II]

Let \( \{|m, \lambda\}\} \) be a complete orthonormal system of eigenvectors of an observable \( A \) such that \( A|m, \lambda\rangle = m|m, \lambda\rangle \) for all eigenvalues \( m \) of \( A \) and all \( \lambda \).

Suppose that a measurement of \( A \) is performed upon a quantum system in the state represented by a normalized vector \( |\Psi\rangle \in \mathcal{H} \). Then

(i) **[Probability]** the probability of getting any specific 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 \( |\Psi\rangle \).

(ii) **[Post-measurement state]** Moreover, given that the outcome \( m \) occurred, the state of the quantum system immediately after the measurement is represented by the vector

\[
\frac{1}{\sqrt{p(m)}} \sum_{\lambda} \langle m, \lambda|\Psi\rangle |m, \lambda\rangle.
\]
A Conjecture
A Conjecture

In the early 1970s, Matijasevič, Robinson, Davis, and Putnam solved negatively Hilbert’s tenth problem by proving the MRDP theorem which states that every computably enumerable subset of \( \mathbb{N} \) is Diophantine.

Inspired by the MRDP theorem, we conjecture the following:

Conjecture

For every computably enumerable subset \( S \) of \( \mathbb{N} \), there exists a constructive observable \( A \) of the form of \( A = P(a_1, \ldots, a_k, a_1^\dagger, \ldots, a_k^\dagger) \) whose eigenvalue spectrum equals \( S \).

- The conjecture implies that when we perform a measurement of the observable \( A \), a member of the c.e. set \( S \) 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 \( S \).
A Conjecture

[posted again]

For every computably enumerable subset $S$ of $\mathbb{N}$, there exists a constructive observable $A$ of the form of $A = P(a_1, \ldots, a_k, a_1^{\dagger}, \ldots, a_k^{\dagger})$ whose eigenvalue spectrum equals $S$.

- In this way a new type of quantum mechanical computer is postulated to exist. How can we construct the quantum mechanical computer, i.e., the observable $A$?

  Below we discuss some properties of this hypothetical quantum computer.

- As in the proof of the MRDP theorem in which a computation history of a Turing machine is encoded in 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.*
A Conjecture

Conjecture [posted again]

For every computably enumerable subset \( S \) of \( \mathbb{N} \), there exists a constructive observable \( A \) of the form of \( A = P(a_1, \ldots, a_k, a_1^\dagger, \ldots, a_k^\dagger) \) whose eigenvalue spectrum equals \( S \).

- Namely, a 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 of complex numbers including 0.

  The 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 of the Turing machine \( M \) at the corresponding time step.
**A Conjecture**

**Conjecture** [posted again]

For every computably enumerable subset $S$ of $\mathbb{N}$, there exists a constructive observable $A$ of the form of $A = P(a_1, \ldots, a_k, a_1^\dagger, \ldots, a_k^\dagger)$ whose eigenvalue spectrum equals $S$.

- The observable $A$ is constructed such that its eigenvector encodes the 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. This implies 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 $S$. 

36
A Conjecture

**Conjecture** [posted again]
For every computably enumerable subset $S$ of $\mathbb{N}$, there exists a constructive observable $A$ of the form of $A = P(a_1, \ldots, a_k, a_1^\dagger, \ldots, a_k^\dagger)$ whose eigenvalue spectrum equals $S$.

- The above analysis shows that the conjecture is likely to be true.

Main Feature

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, it may not be negatively influenced by decoherence, a serious obstacle to the physical realisation of a conventional quantum computer.
Quantum Proving
Without Giving the Proof
Quantum Proving Without Giving the Proof

• In the above we discussed the quantum provability for the formal system $\mathcal{FS}$. We saw that we can extract the proof of a theorem by performing an additional measurement immediately after the theorem is obtained as a measurement outcome.

• 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 $\{F(n_1, \ldots, n_k) \mid n_1, \ldots, n_k \in \mathbb{N}\}$.

  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 above.
Quantum Proving Without Giving the Proof

- Fix a formal system whose theorems form a c.e. 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 the conjecture holds. Then there exists an observable $A$ of a 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 $A$.

  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. 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.
Quantum Proving Without Giving the Proof

• 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 hypothetical quantum mechanical computer 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 completely by a single measurement due to the principle of quantum mechanics.

• Note that 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; and even if we start again from the measurement of $A$, we may have little chance of getting the same provable formula $F$. 
Quantum Proving Without Giving the Proof

• 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 that, via the measurement of $A$, it took only a moment to know that the formula $F$ is provable.

Consequence of the conjecture

The above analysis suggests that even if we get a certain provable formula $F$ as a measurement outcome it is very difficult or unlikely to simultaneously obtain the proof of $F$.

  Namely, it suggests that for a general formal system, proving that a formula is provable is different from writing up the proof of the formula.
Concluding Remarks

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 may operate at room temperature it may be even possible that a similar quantum mechanical process works in the human brain.

Future Direction

The future work aims at proving the conjecture.

Conjecture [posted again]

For every computably enumerable subset $S$ of $\mathbb{N}$, there exists a constructive observable $A$ of the form of $A = P(a_1, \ldots, a_k, a_1^\dagger, \ldots, a_k^\dagger)$ whose eigenvalue spectrum equals $S$. $\square$
Appendix
Commuting Observables

Let $A_1, \ldots, A_k$ be observables of a quantum system. If the observables $A_1, \ldots, A_k$ 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 $A_1, \ldots, A_k$ simultaneously upon the quantum system in any state.
The MRDP Theorem

In the early 1970s, Matijasevič, Robinson, Davis, and Putnam solved negatively Hilbert’s tenth problem by proving the MRDP theorem which states that every computably enumerable subset of $\mathbb{N}$ is Diophantine.

A subset $S$ of $\mathbb{N}$ is called \textit{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 \textit{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 $P(n, m_1, \ldots, m_k) = 0$. 