Quantum algorithm for Hilbert's 10th problem

based on the paper "Computing the noncomputable"
by Tien D. Kieu

Yury Lifshits

Faculty of Mathematics and Mechanics,
St.Petersburg State University, Russia

FerienAkademie 2003, Course "Quantum computation"

Contents

- Statement of Hilbert's 10th problem
- Classical results
- Adiabatic theorem
- Adiabatic quantum computation
- Short scetch of Kieu's algorithm
- More details of the algorithm
- B.Tsirelson's objection
- Summary

David Hilbert, *Mathematical Problems* [1900]

10. Entscheidung der Lösbarkeit einer diophantischen Gleichung. Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlkoefficienten sei vorgelegt: *man soll ein Verfahren angeben, nach welchen sich mittels einer endlichen Anzahl von Operationen entscheiden lässt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist*.

10. Determination of the Solvability of a Diophantine Equation. Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: *To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers*.

A *Diophantine equation* is an equation of the form

$$P(x_1, \ldots, x_m) = 0,$$

where P is a polynomial with integer coefficients.

Rational integers are $0, \pm 1, \pm 2, \pm 3, \ldots$

Greek mathematician *Diophantus* lived in the 3rd century A.D. So why were Diophantine equation still an open problem in 1900?

In the 10th problem Hilbert asked for a *universal* method for recognizing the solvability of Diophantine equations.

In today's terminology Hilbert's 10th problem is a *decision problem*, i.e. a problem consisting of infinitely many individual questions each of which requires an answer YES or NO. The heart of a decision problem is the requirement to find a *single universal* method which could be applied to every such question.

The 10th problem is the only decision problem among the 23 Hilbert's problems.

An equation

$$P(x_1, \ldots, x_m) = 0$$

has a solution in integers $x_1, \ldots, x_m$ if and only if equation

$$P(p_1 - q_1, \ldots, p_m - q_m) = 0.$$

has a solution in natural numbers $p_1, \ldots, p_m$, $q_1, \ldots, q_m$.

Therefore, one says that the decision problem of recognizing solvability of Diophantine equations in integers *reduces* to the decision problem of recognizing the solvability of Diophantine equations in natural numbers.

An equation

$$P(p_1, \ldots, p_m) = 0$$

has a solution in natural numbers if and only if equation

$$P(w_1^2 + x_1^2 + y_1^2 + z_1^2, \ldots, w_m^2 + x_m^2 + y_m^2 + z_m^2) = 0.$$

has a solution in integers because by Lagrange's theorem every natural number is the sum of four squares.

The decision problem of recognizing solvability of Diophantine equations in integers is *equivalent* to the decision problem of recognizing solvability of Diophantine equations in natural numbers.

Today we know that Hilbert's 10th problem has no solution. That means that it is undecidable as a decision problem.

Theorem (Undecidability of Hilbert's tenth problem) *There is no algorithm that, for a given arbitrary Diophantine equation, would tell whether the equation has a solution or not*.

In this sense one speaks about the *negative solution* of Hilbert's 10th problem.

In next few slides we trace a proof of this theorem.

At first we need do define what we mean by an *algorithm*. We will use the following definition.

An algorithm is a program on the *Pascal** programming language with finite set of integers as an input and either eventually halts producing some integer output or works infinitely. The star symbol means that we use only integers.

There is Church (or Church-Turing) thesis of computability:

If any problem could be algorithmically solved, then it can be solved by Pascal* program.

Main theorem. Let P be a Pascal* program whose input consists of k integers. Then we can construct (there is an algorithm which does it) such a polinomial D that equation

$$D(a_1, \ldots, a_k, x_1, \ldots, x_l) = 0$$

has a solution if and only if P halts on the input $a_1, \ldots, a_k$.

Corollary *There is a polynomial P such that the equation*

$$P(a, x_1, \ldots, x_l) = 0$$

has a solution if and only if a is a prime number.

Let us consider **the Halting problem (HP)**: to decide whether a given program P will halt on a given input or not.

Let us consider each program as a finite text in the finite alphabet. Then we can enumerate all programs in alphabetic order.

Proof of undecidability of HP ad absurdum: we'll show that HP is undecidable even if we take only programs with the single integer input. Assume that there exists a program H with input (p, i) and output

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

where P is the program corresponding to number p.

We can write program R (which will be based on the text of H)

$$\text{such that for each input } n \qquad \begin{cases} R \text{ halts if } h(n,n) = 1; \\ R \text{ never stops otherwise.} \end{cases}$$

Let r be the number of R. Then we get the contradiction in both cases $h(r,r) = 0$ and $h(r,r) = 1$. Thus we have proved the undecidability of Halting problem.

Let us derive the undecidabilty of the Hilbert's 10th problem from the Main theorem and undecidabilty of the Halting problem.

Proof ad absurdum: Suppose that T is a program solving Hilbert's 10th problem. Then we can write the program H with input (p, i) which will do the following. First, by the given number it p reconstructs the program P. Second, by the Main Theorem it constructs the corresponding polynomial D. Finaly, it substitutes i in D and runs T for obtained equation. This program H would solve the Halting Problem which gives us a contradiction.

Theorem (J.P.Jones, D.Sato, H.Wada, D.Wiens, [1976]) *The set of all prime numbers is exactly the set of all positive values assumed by the polynomial*

$$
\begin{aligned}
(k+2)\{\quad 1 \quad & -[wz+h+j-q]^2 \\
& -[(gk+2g+k+1)(h+j)+h-z]^2 \\
& -[2n+p+q+z-e]^2 \\
& -\left[16(k+1)^3(k+2)(n+1)^2+1-f^2\right]^2 \\
& -\left[e^3(e+2)(a+1)^2+1-o^2\right]^2 \\
& -\left[(a^2-1)y^2+1-x^2\right]^2 \\
& -\left[16r^2y^4(a^2-1)+1-u^2\right]^2 \\
& -[n+l+v-y]^2 \\
& -\left[\left((a+u^2(u^2-a))^2-1\right)(n+4dy)^2+1-(x+cu)^2\right]^2 \\
& -\left[(a^2-1)l^2+1-m^2\right]^2 \\
& -\left[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x\right]^2 \\
& -\left[z+pl(a-p)+t(2ap-p^2-1)-pm\right]^2 \\
& -[ai+k+1-l-i]^2 \\
& -\left[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m\right]^2\}\,.
\end{aligned}
$$

Three outstanding mathematical problems:

- Goldbach's conjecture

- The Riemann hypothesis

- The four color conjecture

each can be restated as an assertion that particular Diophantine equation has no solutions.

If we find a quantum algorithm for Hilbert's 10th problem, we also will solve Halting problem. It is very strong result. For example it give us an algorithm for checking unsolvability of equation from Last Fermat's theorem.

David Hilbert, *Mathematical Problems* [1900].

Occasionally it happens that we seek the solution under insufficient hypotheses or in an incorrect sense, and for this reason do not succeed. The problem then arises: to show the impossibility of the solution under the given hypotheses, or in the sense contemplated. Such proofs of impossibility were effected by the ancients, for instance when they showed that the ratio of the hypotenuse to the side of an isosceles triangle is irrational. In later mathematics, the question as to the impossibility of certain solutions plays a preéminent part, and we perceive in this way that old and difficult problems, such as the proof of the axiom of parallels, the squaring of circle, or the solution of equations of the fifth degree by radicals have finally found fully satisfactory and rigorous solutions, although in another sense than that originally intended. It is probably this important fact along with other philosophical reasons that gives rise to conviction (which every mathematician shares, but which no one has as yet supported by a proof) that every definite mathematical problem must necessary be susceptible of an exact settlement, either in the form of an actual answer to the question asked, or by the proof of the impossibility of its solution and therewith the necessary failure of all attempts.

Quantum mechanics

In quantum mechanics we study some physical system. Each time it is in some *state*. We are interested in evolution of state of this system in time. At first, we describe math model. Then we discuss its physical meaning.

Let $(E, \langle \bullet | \bullet \rangle)$ be a Hilbert space and let S be unit sphere in it. We say that $e \sim g$, where $e, g \in S$ if $e = \lambda g$ and $|\lambda| = 1$.

The set of classes of equivalence we call *the set of pure states of the system* and denote these states as $|\alpha\rangle$.

Observables

In our model self-adjoint linear operators in E play the role of *observables*.

$$A : E \to E, \text{ such that } \langle e|Ag\rangle = \langle Ae|g\rangle.$$

Consider operators with descrete spectrum i.e. assume that there exists an orthonormal basis $\{e_j\}$ in E such that

$$Ae_j = \lambda_j e_j.$$

So if

$$x = \sum x_j e_j, \qquad \text{then} \qquad Ax = \lambda_j x_j e_j.$$

Vectors e_j are called *eigenvectors* of operator A, respectively, numbers λ_j are called *eigenvalues*.

Mesurement

Now we describe the mesurement of observable A in the system located in a state $|\psi\rangle$. Let

$$|\psi\rangle = \sum x_j e_j. \qquad \text{Notice that} \qquad \sum |x_j|^2 = 1.$$

Numbers x_j are defined up to a factor λ, $|\lambda| = 1$.

Result of the mesurement is random. We get eigenvalue λ_j with probability $|x_j|^2$. After the mesurement state of the system changes to corresponding eigenvector $|e_j\rangle$.

Time evolution

Now we need to describe time evolution of the system. Not all the trajectories in the set of states are possible. For example, in isolated systems the full energy of system must be constant.

For each system at any time t there is one special observable $H(t)$ that governs the time evolution. This operator is called *hamiltonian*. A quantum system evolves according to the Schrödinger equation

$$i\frac{d}{dt}|\psi(t)\rangle = H(t)|\psi(t)\rangle$$

Eigenvector of the least eigenvalue of H is called *ground state*, all others eigenvectors are called *exited states*.

Some comments

• Two distinctions with classical mechanics: discrete results of some mesurements and impossibility of simultanious mesurments.

• In classical mechanics observables are functions defined on the set of states. Usual examples are velocity, energy, coordinates. Unfortunately, this approach to definition of observables doesn't apply to QM.

• If we take $E = C^n$ we get the model of quantum computer with n qubits.

• In Kieu's algorithm we will use systems with infinite-dimensional space E.

Adiabatic theorem

The Adiabatic theorem states that if

$$T \gg \frac{\|H(0) - H(T)\|}{g^2}$$

where

$$\|H(0) - H(T)\| = \max_{0 \le t \le T} |\langle e(t)|(H(0) - H(P))|g(t)\rangle|$$

and

$$g = \min_{0 \le t \le T} (E_e(t) - E_g(t))$$

then starting from the ground state of H(0) we obtain the ground state of H(T) at the end of evolution. Process satisfying these conditions is called *adiabatic*.

Adiabatic computation, [FGGS, 2000]

For using Adiabatic theorem for computational problems we need:

• to encode the solution of some problem P into the ground state of some suitable Hamiltonian, H_P;

• to choose initial Hamiltonian, H_I, with readily obtainable ground state, $|g_I\rangle$;

• to deform $|g_I\rangle$ through a process with the time depending Hamiltonian

$$H(t) = (1 - \frac{t}{T})H_I + \frac{t}{T}H_P.$$

• If the deformation was sufficiently slow, then we get the desired ground state of H_P, $|g_P\rangle$. Then we can compute the answer using obtained $|g_P\rangle$.

Kieu's algorithm for Hilbert's 10th problem

- For any given diophantine equation construct corresponding Hamiltonian H_P, choose H_I and find $|g_I\rangle$;

- Run the adiabatic process for some time T;

- Mesure the state $|f\rangle$ obtained at T starting from $|g_I\rangle$;

- Verify whether the state $|f\rangle$ is the ground state of H_P. If not, we restart adiabatic evolution with new $T := 10T$.

Construction of H_P

Well-studied Simple Harmonic Oscillator system has the Hamiltonian

$$H_{SHO} = a^\dagger a + \frac{1}{2}$$

Operator $N = a^\dagger a$ is called *number operator*. Its spectrum is descrete and spans over all positive integers. We denote by $|n\rangle$ its eigenvectors.

$$N|n\rangle = n|n\rangle; \quad n = 0, 1, 2, \ldots$$

As H_P for the diophantine equation $D(x_1, \ldots, x_K) = 0$ we take $(D(a_1^\dagger a_1, \ldots, a_K^\dagger$
Then

$$H_P|n_1, \ldots, n_K\rangle = D^2(n_1, \ldots, n_K)|n_1, \ldots, n_K\rangle.$$

Example

If we have equation

$$(x+1)^3 + (y+1)^3 - (z+1)^3 = 0$$

then

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

and

$$H_P|n_x, n_y, n_z\rangle = ((n_x+1)^3 + (n_y+1)^3 - (n_z+1)^3)^2 |n_x, n_y, n_z\rangle.$$

Verification step

• If the numbers $N_i, i = 1, \ldots, K$, obtained by measuring $|f\rangle$, satisfy our equation, then we have a solution.

• We take sufficiently large integer neighbourhood of the numbers N_i. If our numbers don't give us local minimum of $|P|$, then $|f\rangle$ is not a ground state.

• In the remaining case we

a) make some numerical studying of the Hamiltonian $\mathcal{H}(t)$ and

b) make some physical experiments (including changing the initial states and multiple run of the adiabatic evolution) to estimate some(what exactly?) probabilities

to check whether $|f\rangle$ is a ground state.

B.Tsirelson's objection

In paper [Tsirelson, 2001] it was shown that the minimal time T required to obtain desired ground state of H_P may be arbitrarily large.

B.Tsirelson states that if we can't estimate T then the Kieu's algorithm fails.

He also claims that there is no way to "check whether it is the ground state". The argument is "we can solve classically the Schrödinger equation on any finite time interval with any precision".

Summary

- Hilbert's 10th problem is classically undecidable.
- Besides of quantum computation based on qubits there exists quantum adiabatic computation.
- We just scetch the algorithm without any proof and many important details.
- There is no certainity that the Kieu's algorithm works.
- Quantum adiabatic computation may be useful for classically decidable problems. For example, its application for SAT-problem was studied in [FGGS, 2000].