60 Years of DPR-theorem and 50 Years of DPRM-theorem

Proofs, Improvements, Applications, and Open Questions

Yu. V. Matiyasevich

Steklov Institute of Mathematics at St. Petersburg

logic.pdmi.ras.ru/~yumat

The two theorems

DPR-theorem (Martin Davis, Hilary Putnam, Julia Robinson [1961]). *Every effectively enumerable set $\mathfrak{M}$ of n-tuples of natural numbers has an exponential Diophantine representation of the form*

$$\langle a_1, \dots, a_n \rangle \in \mathfrak{M} \Longleftrightarrow \exists x_1 \dots x_m \\ \{E_1(a_1, \dots, a_n, x_1, \dots, x_m) = E_2(a_1, \dots, a_n, x_1, \dots, x_m)\}$$

where $E_1(a_1, \dots, a_n, x_1, \dots, x_m)$ and $E_2(a_1, \dots, a_n, x_1, \dots, x_m)$ are expression constructed by combining the variables and particular natural numbers using the traditional rules of addition, multiplication and exponentiation.

An improvement of DPR-theorem (DPRM-theorem [1970]). *Every effectively enumerable set $\mathfrak{M}$ of n-tuples of natural numbers has a Diophantine representation*

$$\langle a_1, \dots, a_n \rangle \in \mathfrak{M} \Longleftrightarrow \exists x_1 \dots x_m \{P(a_1, \dots, a_n, x_1, \dots, x_m) = 0\}$$

where $P(a_1, \dots, a_n, x_1, \dots, x_m)$ is a polynomial with integer coefficients.

Plan of the talk

- Proofs
- Improvements
- Some applications
- Some Open Problems

Part I. Proofs

Original proof of DPRM-theorem

DPRM-theorem. *Every effectively enumerable set $\mathfrak{M}$ has a Diophantine representation*

Step 1. Construct of an arithmetical formula with many bounded universal quantifiers (after Kurt Gödel)

Step 2. Transform this formula into Davis normal form with single bounded universal quantifier

Step 3. Eliminate the single bounded universal quantifier through the use of exponential Diophantine equation

Step 4. Transform the exponential Diophantine equation into an equivalent Diophantine equation

"1" + "2" + "3" = DPR-theorem

DPR + "4" = DPRM-theorem

An alternative version of the original proof of DPRM-theorem

DPRM-theorem. *Every effectively enumerable set $\mathfrak{M}$ has a Diophantine representation*

Step 1. Construct of an arithmetical formula with many bounded universal quantifiers (after Kurt Gödel)

Step 2. **REPEAT:**

  Step 3. Eliminate the innermost bounded universal quantifier through the use of exponential Diophantine equation

  Step 4. Transform the exponential Diophantine equation into an equivalent Diophantine equation

Step 3. Elimination of bounded universal quantifier

1959 Martin Davis and Hilary Putnam: conditional technique under the assumption of the existence of arbitrary long non-constant arithmetical progressions consisting entirely of prime numbers (the existence proved by Ben Green and Terence Tao in 2004)

1960 Julia Robinson: unconditional technique using arbitrarily long arithmetical progressions with large prime factors

1972 Yuri Matiyasevich: instead of prime numbers one can use multiplicative version of Dirichlet principle

1993 Yuri Matiyasevich: a completely different technique (the bounded universal quantifier is replaced by summation)

Step 1. Arithmetization

DPR-theorem. *Every effectively enumerable set $\mathfrak{M}$ has an exponential Diophantine representation*

Step 1. Construct of an arithmetical formula with many bounded universal quantifiers (after Kurt Gödel)

Step 2. Transform this formula into Davis normal form with single bounded universal quantifier

Step 3. Eliminate the single bounded universal quantifier through the use of exponential Diophantine equation

"1" + "2" + "3" = DPR-theorem

Step 1. Purely existential arithmetization

DPR-theorem. *Every effectively enumerable set $\mathfrak{M}$ has an exponential Diophantine representation*

Step 1. Construct of an arithmetical formula presenting given effectively enumerable set *without* using universal quantifiers

"1" = DPR-theorem

Purely existential arithmetization was done for:

- Turing machines (Yu. Matiyasevich 1976, 1993)
- register machines (J. P. Jones and Yu. Matiyasevich 1983)
- partial recursive functions (Yu. Matiyasevich 1994)
- universal technique of existential arithmetization (Yu. Matiyasevich 2009)

Step 4. Elimination of exponentiation

Original technique:

1952 Julia Robinson: a sufficient condition for the possibility to perform such transformation

1970 Yuri Matiyasevich: the fulfillment of this condition by the sequence of Fibonacci numbers

Modern technique: usage of the second order recurrent sequence of solutions of Pell equation

A slight modifications: some third and fourth order recurrent sequences could be used (Maxim Vsemirnov 1995, 1997)

Computer verification of DPRM-theorem

Karol Pąk

The Matiyasevich Theorem. Preliminaries

Formalized Mathematics, 25(4):315–322, 2017.

Diophantine sets. Preliminaries

Formalized Mathematics, 26(1):81–90, 2018.

Benedikt Stock, Abhik Pal, Maria Antonia Oprea, Yufei Liu, Malte Sophian Hassler, Simon Dubischar, Prabhat Devkota, Yiping Deng, Marco David, Bogdan Ciurezu, Jonas Bayer and Deepak Aryal

Hilbert Meets Isabelle: Formalisation of the DPRM Theorem in Isabelle

EasyChair Preprint no. 152, May 22, 2018

Dominique Larchey-Wendling and Yannick Forster

Hilbert's Tenth Problem in Coq

4th International Conference on Formal Structures for Computation and Deduction (FSCD 2019)

Leibniz International Proceedings in Informatics, No.27, 2019

Restricted proofs of DPRM-theorem

- How weak can be a formal system sufficient for proving DPRM-theorem?

- What formal system are not sufficient for proving DPRM-theorem?

Part II. Improvements

DPRM-theorem

DPRM-theorem improved (Yu. Matiyasevich & Julia Robinson 1975) *Every effectively enumerable set $\mathfrak{M}$ of n-tuples of natural numbers has a Diophantine representation of the form*

$$\langle a_1, \dots, a_n \rangle \in \mathfrak{M} \Longleftrightarrow \exists x_1 \dots x_{13} \{ P(a_1, \dots, a_n, x_1, \dots, x_{13}) = 0 \}$$

where $x_1, \dots, x_{13}$ range over the natural numbers.

DPRM-theorem improved (Yu. Matiyasevich 1975/1982) *Every effectively enumerable set $\mathfrak{M}$ of n-tuples of natural numbers has a Diophantine representation of the form*

$$\langle a_1, \dots, a_n \rangle \in \mathfrak{M} \Longleftrightarrow \exists x_1 \dots x_9 \{ P(a_1, \dots, a_n, x_1, \dots, x_9) = 0 \}$$

where $x_1, \dots, x_9$ range over the natural numbers.

DPRM-theorem improved (Zhi-Wei Sun 1992/2017) *Every effectively enumerable set $\mathfrak{M}$ of n-tuples of natural numbers has a Diophantine representation of the form*

$$\langle a_1, \dots, a_n \rangle \in \mathfrak{M} \Longleftrightarrow \exists x_1 \dots x_{11} \{ P(a_1, \dots, a_n, x_1, \dots, x_{11}) = 0 \}$$

where $x_1, \dots, x_{11}$ range over the integers.

DPR-theorem

DPR-theorem improved (Yu. Matiyasevich 1979) *Every effectively enumerable set $\mathfrak{M}$ of n-tuples of natural numbers has an exponential Diophantine representation of the form*

$$\langle a_1, \dots, a_n \rangle \in \mathfrak{M} \iff$$
$$\exists x_1 x_2 x_3 \{E_1(a_1, \dots, a_n, x_1, x_2, x_3) = E_2(a_1, \dots, a_n, x_1, x_2, x_3)\}$$

DPR-theorem improved (J. P. Jones & Yu. Matiyasevich 1981) *Every effectively enumerable set $\mathfrak{M}$ of n-tuples of natural numbers has a unary exponential Diophantine representation of the form*

$$\langle a_1, \dots, a_n \rangle \in \mathfrak{M} \iff$$
$$\exists x_1 x_2 x_3 \{E_1(a_1, \dots, a_n, x_1, x_2, x_3) = E_2(a_1, \dots, a_n, x_1, x_2, x_3)\}$$

where $E_1(a_1, \dots, a_n, x_1, x_2, x_3)$ and $E_2(a_1, \dots, a_n, x_1, x_2, x_3)$ are expression constructed by combining the variables and particular natural numbers using the traditional rules of addition, multiplication and unary exponentiation 2^x.

Single-fold representations

Definition. A purely existential representation

$$\langle a_1, \ldots, a_n \rangle \in \mathfrak{M} \Longleftrightarrow$$
$$\exists x_1 \ldots x_m \{E_1(a_1, \ldots, a_n, x_1, \ldots, x_m) = E_2(a_1, \ldots, a_n, x_1, \ldots, x_m)\}$$

is single-fold if for every $a_1, \ldots, a_n$ the x's, if they exist, are unique.

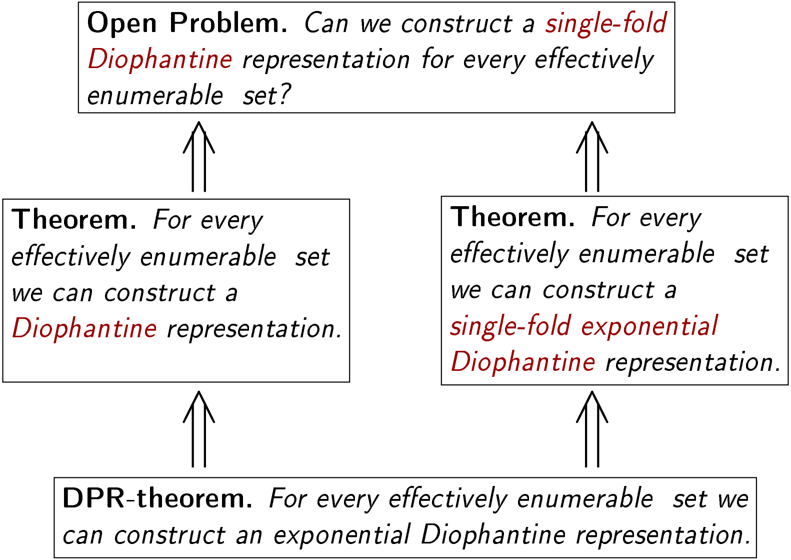
DPR-theorem improved (Yu. Matiyasevich 1974) *Every effectively enumerable set $\mathfrak{M}$ of n-tuples of natural numbers has a single-fold exponential Diophantine representation of the form*

$$\langle a_1, \ldots, a_n \rangle \in \mathfrak{M} \Longleftrightarrow$$
$$\exists x_1 x_2 x_3 \{E_1(a_1, \ldots, a_n, x_1, x_2, x_3) = E_2(a_1, \ldots, a_n, x_1, x_2, x_3)\}$$

DPR-theorem improved (J. P. Jones & Yu. Matiyasevich 1982) *Every effectively enumerable set $\mathfrak{M}$ of n-tuples of natural numbers has a unary single-fold exponential Diophantine representation of the form*

$$\langle a_1, \ldots, a_n \rangle \in \mathfrak{M} \Longleftrightarrow$$
$$\exists x_1 x_2 x_3 \{E_1(a_1, \ldots, a_n, x_1, x_2, x_3) = E_2(a_1, \ldots, a_n, x_1, x_2, x_3)\}$$

An Open Problem



Open Problem. *Can we construct a single-fold Diophantine representation for every effectively enumerable set?*

Theorem. *For every effectively enumerable set we can construct a Diophantine representation.*

Theorem. *For every effectively enumerable set we can construct a single-fold exponential Diophantine representation.*

DPR-theorem. *For every effectively enumerable set we can construct an exponential Diophantine representation.*

Part III. Some applications

Equations with Finitely Many Solutions

Suppose that we have an equation

$$P(a, x_1, \ldots, x_m) = 0, \tag{$*$}$$

and somehow we know that for every value of the parameter a the equation has at most finitely many solutions in natural numbers $x_1, \ldots, x_m$.

This fact can be expressed in two ways:

1. The equation $(*)$ has at most $\nu(a)$ solutions;
2. For every solution of $(*)$ we have

$$x_1 < \sigma(a), \ldots, x_m < \sigma(a)$$

Here ν and σ should be some suitable functions defined for every a.

Effectivization

Theorem (Axel Thue [1909]). *Let F be an integral binary form such that F(x, 1) has at least three distinct zeros. Let m be a non-zero integer. Then the equation*

$$F(x, y) = m \tag{$*$}$$

has at most finitely many solutions.

Theorem (Alan Baker [1968]). *Let F(x, y) be as above. Then one can effectively find a number $B(m)$ such that $(*)$ implies that*

$$\max\{x, y\} < B(m).$$

An impossible effectivization

Let

$$E_1(a, x_1, x_2, x_3) = E_2(a, x_1, x_2, x_3)$$

be the equation from a single-fold exponential Diophantine representation of some undecidable effectively enumerable set. Then

- we can bound the number of solutions for any value of the parameter *a* by 1;
- we cannot bound the unique solution of this equation by any total (i.e., defined for all values of its argument) effectively computable function of *a*.

The above equation is non-effectivizable in principle.

Open problem. *Is there exist a non-effectivizable genuine Diophantine equation?*

To this end it would be sufficient to establish the existence of finite-fold Diophantine representations for all effectively enumerable sets

Compression of Diophantine sets

$$a \in \mathfrak{M} \Longleftrightarrow \exists x_1 \ldots x_m \{P(a, x_1, \ldots, x_m) = 0\}$$

$$\mathfrak{M}_n = \mathfrak{M} \cap \{1, \ldots, n\}$$

$$B_n = b_1 \ldots b_a \ldots b_n \qquad b_a = \begin{cases} \text{"1"}, & \text{if } a \in \mathfrak{M} \\ \text{"0"} & \text{otherwise} \end{cases}$$

$$B_n \xrightarrow{f} A_n \xrightarrow{f^{-1}} B_n$$

How short such a binary string A_n could be?

Diophantine sets admit very high compression

$$a \in \mathfrak{M} \Longleftrightarrow \exists x_1 \ldots x_m \{P(a, x_1, \ldots, x_m) = 0\}$$

$$B_n = b_1 \ldots b_a \ldots b_n \qquad b_a = \begin{cases} \text{“1”}, & \text{if } a \in \mathfrak{M} \\ \text{“0”} & \text{otherwise} \end{cases}$$

$$B_n \xrightarrow{f} A_n \xrightarrow{f^{-1}} B_n$$

$$A_n = \tilde{n}\widetilde{q_n}$$

where

$$\tilde{n} \text{ is the binary notation of } n$$

$$q_n \text{ is the number of “1” in } B_n$$

$$\widetilde{q_n} \text{ is the binary notation of } q_n$$

(the binary notations are padded by leading zeros to the length $\lceil \log_2(n+1) \rceil$)

The length of A_n is $2\lceil \log_2(n+1) \rceil$

Computational chaos in Number Theory

Gregory Chaitin constructed a particular one-parameter exponential Diophantine equation and considered the set of all values of the parameter for which the equation has infinitely many solutions:

$$a \in \mathfrak{M} \Longleftrightarrow \exists^{\infty} x_1 \dots x_m \{E_1(a, x_1, x_2, \dots, x_m) = E_2(a, x_1, x_2, \dots, x_m)\}$$

Theorem (G. Chaitin 1987). *Prefix-free Kolmogorov complexity* of this set is equal to n.

$$\mathfrak{M}_n = \mathfrak{M} \cap \{1, \dots, n\} \qquad B_n = b_1 \dots b_a \dots b_n \xrightarrow{f} A_n \xrightarrow{f^{-1}} B_n$$

Corollary 1. *For every (prefix-free) f the length of A_n is at least $n - C_f$ for some constant C_f.*

Corollary 2. *For every consistent finitely generated formal system S there are only finitely many values of a for which we can deduce from S the validity either of $a \in \mathfrak{M}$ or of $a \notin \mathfrak{M}$.*

Informally, one can say that the set $\mathfrak{M}$ is completely chaotic.

More computational chaos in Number Theory

Toby Ord and Tien D. Kieu [2003] constructed another particular one-parameter exponential Diophantine equation which for every value of the parameter has only finitely many solutions and considered the set of all values of the parameter for which the equation has even number of solutions:

$$a \in \mathfrak{M} \Longleftrightarrow \exists^{\text{even}} x_1 \ldots x_m \{E_1(a, x_1, x_2, \ldots, x_m) = E_2(a, x_1, x_2, \ldots, x_m)\}$$

They proved that the prefix-free Kolmogorov complexity of this set is also equal to n.

Even more computational chaos in Number Theory

Theorem (Yu. Matiyasevich 2006). *Let $\mathfrak{U}$ be a decidable infinite set with infinite complement. One can construct an exponential Diophantine equation which for every value of the parameter has only finitely many solutions and such that for the set*

$$a \in \mathfrak{M} \Longleftrightarrow \exists^{\mathfrak{U}} x_1 \ldots x_m \{E_1(a, x_1, x_2, \ldots, x_m) = E_2(a, x_1, x_2, \ldots, x_m)\}$$

the prefix-free Kolmogorov complexity of its initial segment

$$\mathfrak{M}_n = \mathfrak{M} \bigcap \{a \,|\, a \leq n\}$$

of this set is equal to n.

Open Problem. *Is there similar computational chaos in realm of Diophantine equations?*

Hilbert's 10th Problem

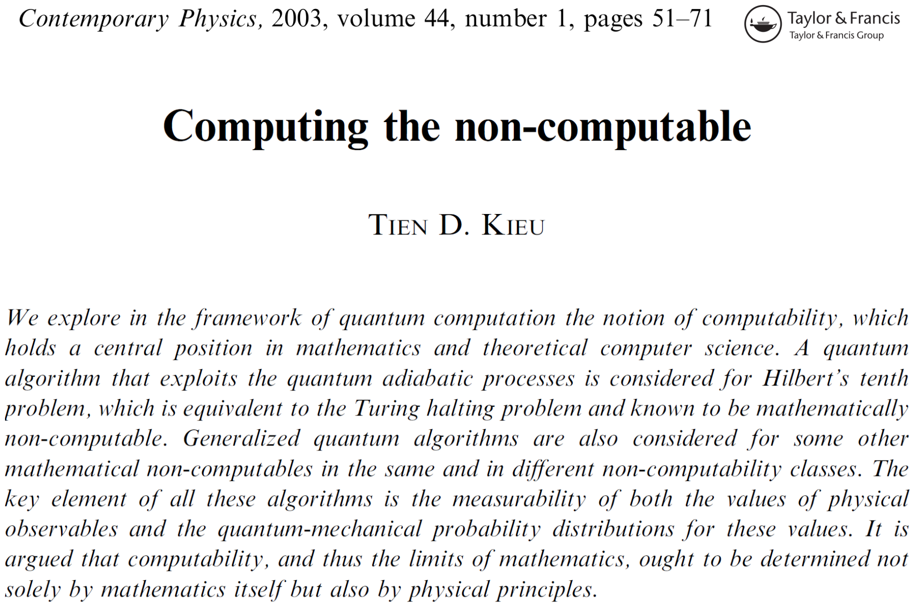
10. Determination of the Solvability of a Diophantine Equation. Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: *To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable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

David Hilbert, *Mathematical Problems* [1900]

DPRM-theorem $+$ **Church's Thesis**

Corollary. *Hilbert's tenth problem is undecidable*

Beyond Church's Thesis?



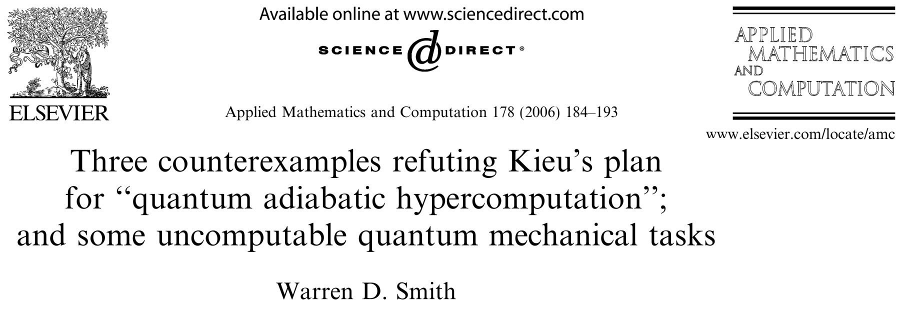
Contemporary Physics, 2003, volume 44, number 1, pages 51–71

Taylor & Francis
Taylor & Francis Group

Computing the non-computable

Tien D. Kieu

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 that exploits the quantum adiabatic processes is considered for Hilbert's tenth problem, which is equivalent to the Turing halting problem and known to be mathematically non-computable. Generalized quantum algorithms are also considered for some other mathematical non-computables in the same and in different non-computability classes. The key element of all these algorithms is the measurability of both the values of physical observables and the quantum-mechanical probability distributions for these values. It is argued that computability, and thus the limits of mathematics, ought to be determined not solely by mathematics itself but also by physical principles.



Available online at www.sciencedirect.com

SCIENCE DIRECT®

ELSEVIER

Applied Mathematics and Computation 178 (2006) 184–193

APPLIED MATHEMATICS AND COMPUTATION

www.elsevier.com/locate/amc

Three counterexamples refuting Kieu's plan for "quantum adiabatic hypercomputation"; and some uncomputable quantum mechanical tasks

Warren D. Smith

From Abstract: Tien D. Kieu ... had claimed to have a scheme showing how, in principle, physical "quantum adiabatic systems" could be used to solve the prototypical computationally undecidable problem, Turing's "halting problem"...

There were several errors in those papers, most which ultimately could be corrected. More seriously, we here exhibit counterexamples to a crucial step in Kieu's argument... These counterexamples destroy Kieu's entire plan and there seems no way to correct the plan to escape them.

Nevertheless, there are some important consequences salvageable from Kieu's idea ...

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Applied Mathematics and Computation 178 (2006) 184–193

APPLIED MATHEMATICS AND COMPUTATION

www.elsevier.com/locate/amc

Three counterexamples refuting Kieu's plan for "quantum adiabatic hypercomputation"; and some uncomputable quantum mechanical tasks

Warren D. Smith

21 Shore Oaks Drive, Stony Brook, NY 11790, USA

Kieu here made an error about Diophantine equations. He seemed to have the idea that we only need to worry about Diophantine equations $D = 0$ with *unique* solutions, leading to H_P with unique ("nondegenerate") ground states. In fact, it is commonplace for Diophantine equations to have an *infinite* number of solutions, and indeed the only polynomial Diophantine equations presently known to achieve Turing-completeness always do have either an infinite number, or no, solutions (it being Turing-undecidable which)

However, this error is repairable. The present author (who was serving as the referee on one of Kieu's papers) was able to modify the proof of Jones and Matijasevic [6] concerning "singlefold 2-exponential Diophantine equations". By so doing I was able to construct Turing-complete 2-exponential Diophantine functions D which always have a *unique global minimum*. The value of D at this minimum is a nonnegative integer and it is Turing-undecidable whether it is zero. (I call these "singlemin" Diophantines.)

I was then able to show how to modify Kieu's construction to be based on these instead of on polynomial Diophantine equations.[1] So this error was not fatal.

[1] This comes at the cost of making the physical interpretation less attractive and less realistic-sounding.

(2020) 10:1195 | https://doi.org/10.1038/s41598-019-56804-1

SCIENTIFIC
REPORTS
natureresearch

Uncomputability and complexity of quantum control

Denys I. Bondar[1] & Alexander N. Pechen[2,3]

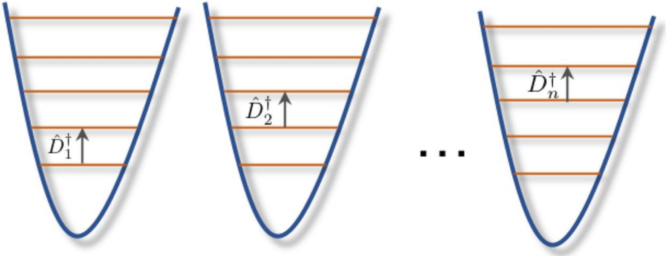


Figure 1. A physical system for simulating Diophantine equations with n variables. The system is either n trapped ions or an n–mode coherent field. The controls $\hat{D}_1^\dagger, \ldots, \hat{D}_n^\dagger$ independently address each subsystem. For ions, the controls excite transitions between nearest levels, and transfer population of the highest excited state down to the ground state. For coherent states, the control for the i-th mode is the displacement $\hat{D}_i$ by the

(2020) 10:1195 | https://doi.org/10.1038/s41598-019-56804-1

SCIENTIFIC REPORTS

natureresearch

Uncomputability and complexity of quantum control

Denys I. Bondar[1] & Alexander N. Pechen[2,3]

Discussion

Computability of quantum control problems has been analyzed. A realistic situation, when a number of controls is finite, has been considered. We have shown that within this setting solving quantum control problems is equivalent to solving Diophantine equations. As a consequence, quantum control is Turing complete. The established equivalence is a new technique for quantum technology that, e.g., allows to construct quantum problems belonging to a specific complexity class. Examples of a multimode coherent field control are explicitly constructed. The negative answer to the Hilbert's tenth problem implies that there is no algorithm deciding whether there is a control policy connecting two quantum states represented by arbitrary pure or mixed density matrices, i.e., the most general fixed-time quantum state-to-state control problem is not algorithmically solvable. This result applies to the problems of finding exact as well approximate solutions for sufficiently small errors. Our method opens up an opportunity to recast many open mathematical problems, including the Riemann hypothesis, as quantum control tasks. The uncovered non-algorithmic nature makes quantum control a fruitful research area.

The Riemann Hypothesis (RH) as a Diophantine equation

Theorem (Alan Turing 1939) $\mathrm{RH} \in \Pi_2^0$

$$\mathrm{RH} \iff \forall x_1 \dots x_m \exists y_1 \dots y_n \phi(x_1, \dots x_m, y_1 \dots y_n)$$

Theorem (Georg Kreisel 1958) RH $\in \Pi_1^0$

$$\mathsf{RH} \iff \forall x_1 \dots x_m \psi(x_1, \dots x_m)$$

Corollary of the above + DPRM-theorem. *We can construct a particular polynomial with integer coefficients $R(x_1, \dots, x_m)$ such that*

$$\begin{aligned} \mathsf{RH} \quad &\iff \quad \forall x_1 \dots x_m R(x_1, \dots, x_m) \neq 0 \\ &\iff \quad \neg\exists x_1 \dots x_m R(x_1, \dots, x_m) = 0 \end{aligned}$$

A reformulation of the Riemann Hypothesis

Theorem (Yu. Matiyasevich 2018). *Consider the following system of conditions:*

$$2^{\ell} \leq n < 2^{\ell+1}, \qquad 2^{m} \leq q < 2^{m+1},$$

$$s = \frac{B^{n+1}\left(B^{(n+1)n} - n - 1\right) + n}{\left(B^{n+1} - 1\right)^{2}}, \qquad t = \frac{\left(2^{m} - 1\right)\left(B^{n^2} - 1\right)}{B^{n} - 1},$$

$$\binom{t}{r} \equiv 1 \pmod{2}, \qquad rs - u \equiv \frac{B^{n^2-n}\left(B^{n} - 1\right)}{B - 1}q \pmod{B^{n^2}},$$

$$u = \mathrm{rem}\left(rs, B^{n^2-n}\right), \quad p = \mathrm{rem}\left(r, B^{n} + 1\right), \quad mp < nq - 15\ell^{2}q\sqrt{n},$$

where B denotes $2^{\ell+m+1}$.

- *If the Riemann Hypothesis is true then the above system has no solution in positive integers $\ell, m, n, p, q, r, s, t, u$.*
- *If the Riemann Hypothesis is false then the above system has infinitely many such solutions.*

Vector addition systems

Introduced by Richard M. Karp and Raymond E. Miller in 1969 as a tool to study distributed computations

A *vector addition system* is a set $\{V_1, \ldots, V_m\}$ of vectors of the same size with *integer* coefficients. One can pass in one step from a vector A to the vector $A + V_k$ for any k *provided that all entries to both A and $A + V_k$ are natural numbers*.

$$A \longrightarrow A + V_{k_1} \longrightarrow A + V_{k_1} + V_{k_2} \longrightarrow \ldots$$

Comparison Problem.

INPUT: Two systems of vector addition $\{V_1, \ldots, V_m\}$ and $\{W_1, \ldots, W_n\}$ and a vector A

QUESTION: Is it true that every vector reachable from A in the first system is also reachable from A in the second system?

Theorem (Michael Rabin 1966, 1972, not published). *The Comparison Problem is undecidable.*

Unification of terms

Set of variables $\mathcal{X} = \{x_1, x_2, \ldots\}$
Set of symbols of functions $\mathcal{F} = \{f_1, f_2, \ldots, \}$
Set of terms $\mathcal{T} = \{, \ldots, f_1(x_1, f_2(x_1, x_2)), \ldots, f_1(f_2(x_2, x_2), x_3), \ldots\}$

First order unification Problem

INPUT: Two terms T' and T''

QUESTION: Is there exists a substitution $\phi : \mathcal{X} \longrightarrow \mathcal{T}$ which makes T' and T'' identical, $T'\Big|_\phi \equiv T''\Big|_\phi$?

An example. $T' = f_1(x_1, f_2(x_1, x_2))$ $T'' = f_1(f_2(x_2, x2), x_3)$

$$\begin{aligned} \phi : \ x_1 &\longmapsto f_2(x_2, x_2) \\ \phi : \ x_2 &\longmapsto x_2 \\ \phi : \ x_3 &\longmapsto f_2(f_2(x_2, x_2), x_2) \end{aligned}$$

$$T'\Big|_\phi \equiv f_1(f_2(x_2, x_2), f_2(f_2(x_2, x_2), x_2)) \equiv T''\Big|_\phi$$

Unification of terms

An algorithm for the first order unification problem was proposed in 1965 by J. Robinson (John Alan Robinson)

Theorem (Warren D. Goldfarb 1981). *Second order unification problem is undecidable*

$$n \leftrightsquigarrow T_n = \underbrace{f(f(\dots f}_{n \text{ times}}(x)\dots))$$

$$T_{m+n} \equiv T_m\Big|_{x \longrightarrow T_n} \qquad T_{m\times n} \equiv ?$$

There are many other kinds of the inification problem, and the undecidability of some of them was established by different authors via the DPRM-theorem

From Diophantine equations to differential equations

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

$$\Psi(\tau_1,\ldots,\tau_m) \;=\; \sum_{x_1,\ldots,x_m=0}^{\infty} \psi_{x_1,\ldots,x_m}\tau_1^{x_1}\ldots\tau_m^{x_m}$$

$$\tau_k\frac{\partial}{\partial\tau_k}t_k^{x_k}=x_kt_k^{x_k} \qquad \left(t_k\frac{\partial}{\partial t_k}\right)^d t_k^{x_k}=x_k^dt_k^{x_k}$$

$$P\left(\tau_1\frac{\partial}{\partial\tau_1},\ldots,\tau_m\frac{\partial}{\partial\tau_m}\right)\Psi(\tau_1,\ldots,\tau_m)=\frac{1}{(1-\tau_1)\ldots(1-\tau_m)} \qquad (**)$$

$$\sum_{x_1,\ldots,x_m=0}^{\infty} P(x_1,\ldots,x_m)\psi_{x_1,\ldots,x_m}\tau_1^{x_1}\ldots\tau_m^{x_m}=\sum_{x_1,\ldots,x_m=0}^{\infty}\tau_1^{x_1}\ldots\tau_m^{x_m}$$

$$P(x_1,\ldots,x_m)\psi_{x_1,\ldots,x_m}=1 \qquad \Leftrightarrow \qquad \psi_{x_1,\ldots,x_m}=\frac{1}{P(x_1,\ldots,x_m)}$$

Differential equation (**) has a solution if and only if Diophantine equation (*) has no solutions.

An application of the undecidability of Hilbert's 10th problem

Theorem (Jan Denef and Leonard Lipshitz 1984). *There is no algorithm for deciding, for an arbitrary polynomial Q, whether partial differential equation*

$$Q\left(\tau_1, \ldots, \tau_m, \frac{\partial}{\partial \tau_1}, \ldots, \frac{\partial}{\partial \tau_m}\right) \Psi(\tau_1, \ldots, \tau_m) = 0$$

has a solution in the form of a (formal) power series.

An application of DPRM-theorem

Theorem (Jan Denef and Leonard Lipshitz 1984). *We can construct polynomials with integer coefficients* $Q_{k,\ell}(x_1,\ldots,x_{2m})$*,* $k=1,\ldots,K$*,* $\ell=1,\ldots,L$*, such that:*

- *the system of partial differential equations*

$$\begin{array}{rcl} \displaystyle\sum_{\ell=1}^{L} Q_{1,\ell}\left(\tau_1,\ldots,\tau_m,\frac{\partial}{\partial\tau_1},\ldots,\frac{\partial}{\partial\tau_m}\right)\Psi_\ell(\tau_1,\ldots,\tau_m) & = & 0 \\ \multicolumn{3}{c}{\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots} \\ \displaystyle\sum_{\ell=1}^{L} Q_{K,\ell}\left(\tau_1,\ldots,\tau_m,\frac{\partial}{\partial\tau_1},\ldots,\frac{\partial}{\partial\tau_m}\right)\Psi_\ell(\tau_1,\ldots,\tau_m) & = & 0 \end{array}$$

has a solution in (formal) power series $\Psi_1(\tau_1,\ldots,\tau_m),\ldots,\Psi_L(\tau_1,\ldots,\tau_m)$ *with rational coefficients;*

- *no such solution is computable.*

Proof uses the existence of non-intersecting effectively enumerable sets which cannot be separated by a decidable set

Diophantine Games

Introduced by James P. Jones in 1974 based on ideas of Michael O. Rabin

$$P(a_1, \dots, a_m, x_1, \dots, x_m) = 0$$

Peter selects the values of the parameters $a_1, \dots, a_m$
Ursula selects the values of the unknowns $x_1, \dots, x_m$

- Peter selects a_1
- Ursula selects x_1
- Peter selects a_2
- Ursula selects x_2
- ....
- Peter selects a_m
- Ursula selects x_m

Ursula is the winner if and only if the value of the polynomial is to equal to 0.

Powerless winner

Theorem (J. P. Jones 1982) *In the game*

$$
\begin{aligned}
&\Big\{\{a_1 + a_6 + 1 - x_4\}^2 \cdot \{\langle (a_6 + a_7)^2 + 3a_7 + a_6 - 2x_4\rangle^2 \\
&+ \Big\langle [(x_9 - a_7)^2 + (x_{10} - a_9)^2]\,[(x_9 - a_6)^2 + (x_{10} - a_8)^2((x_4 - a_1)^2 \\
&+ (x_{10} - a_9 - x_1)^2)]\,[(x_9 - 3x_4)^2 + (x_{10} - a_8 - a_9)^2]\,[(x_9 - 3x_4 - 1)^2 \\
&+ (x_{10} - a_8 a_9)^2] - a_{12} - 1\Big\rangle^2 + \langle [x_{10} + a_{12} + a_{12} x_9 a_4 - a_3]^2 \\
&+ [x_5 + a_{13} - x_9 a_4]^2\rangle\} - x_{13} - 1\Big\}\{a_1 + x_5 + 1 - a_5\}\Big\{\langle (x_5 - x_6)^2 \\
&+ 3x_6 + x_5 - 2a_5\rangle^2 + \Big\langle [(a_{10} - x_6)^2 + (a_{11} - x_8)^2]\,[(a_{10} - x_5)^2 \\
&+ (a_{11} - x_7)^2((a_5 - a_1)^2 + (a_{11} - x_8 - a_2)^2)]\,[(a_{10} - 3a_5)^2 \\
&+ (a_{11} - x_7 - x_8)^2]\,[(a_{10} - 3a_5 - 1)^2 + (a_{11} - x_7 x_8)^2] - x_{11} - 1\Big\rangle^2 \\
&+ \langle [a_{11} + x_{11} + x_{11} a_{10} x_3 - x_2]^2 + [a_{11} + x_{12} - a_{10} x_3]^2\rangle\Big\} = 0
\end{aligned}
$$

Ursula has a winning strategy but no computable winning strategy.

Proof is based on the existence of so called simple effectively enumerable sets

Other applications of DPRM-theorem to games

In 1970 Alistair H. Lachlan introduced another kind of game as a possible tool to establish results about the lattice of effectively enumerable sets. He conjectured that for these games it can be decided which of the two players has the winning strategy. He obtained partial results in this direction but in 2006 Martin Kummer proved many results about undecidability of Lachlan's games using DPRM-theorem.

An undecidable problem of Harvey M. Friedman

Let $\mathcal{P}$ be the class of all polynomials with integer coefficients (in an arbitrary number of variables of arbitrary high degrees).

If $P \in \mathcal{P}$ and V is a set of numbers, then $P(V)$ will denote the set of all values assumed by polynomial P when its variables take (independently) all values from V.

$$\mathfrak{F} = \left\{ n_{\in \mathbb{Z}^+} : \exists P_{\in \mathcal{P}} \Big(n = \max(P(\mathbb{Z})) \,\&\, P([-3,3]) \subseteq (-\ln(n)^{\frac{1}{3}}, \ln(n)^{\frac{1}{3}}) \Big) \right\}$$

Here $[-3,3]$ is the set of all real numbers between -3 and 3.

Teorem (H. M. Friedman 2004). *The set $\mathfrak{F}$ is undecidable.*

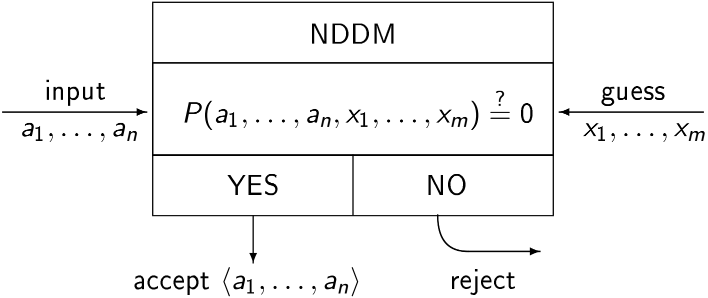
$$\mathfrak{G} = \left\{ n_{\in \mathbb{Z}^+} : \exists P_{\in \mathcal{P}} \Big(n = \max(P(\mathbb{Z})) \,\&\, P([-\tfrac{3}{2}, \tfrac{3}{2}]) \subseteq (-\ln(n)^{\frac{1}{3}}, \ln(n)^{\frac{1}{3}}) \Big) \right\}$$

Teorem (H. M. Friedman 2004). *The set $\mathfrak{G}$ is decidable.*

Part IV. Some open problems

Non-Deterministic Diophantine Machine (NDDM)

Introduced by Leonard Adleman and Kenneth Manders in 1976



NDDM

input

$a_1, \ldots, a_n$

$P(a_1, \ldots, a_n, x_1, \ldots, x_m) \overset{?}{=} 0$

guess

$x_1, \ldots, x_m$

YES

NO

accept $\langle a_1, \ldots, a_n \rangle$

reject

DPRM-theorem: *NDDMs are as powerful as, say, Turing machines, i.e., every set acceptable by a Turing machine is accepted by some NDDM, and, of course, vice versa.*

Open problem. *Are NDDMs as efficient as Turing machines?*

Complexity measures

Turing machine	**Diophantine machines**
• TIME	• SIZE
• SPACE	

SIZE can be defined as the least possible value of

$$\max\{|x_1|, \dots, |x_m|\},$$

or (non-equivalently) as

$$|x_1| + \cdots + |x_m|,$$

or (non-equivalently) as

$$|x_1 + \cdots + x_m|$$

where $|x|$ is the binary length of x ($|x| \approx \log_2(x)$, $x \approx 2^{|x|}$)

Class **D**

Introduced by Leonard Adleman and Kenneth Manders in 1975

Class **D** consists of all sets $\mathfrak{M}$ having representations of the form

$$\langle a_1, \ldots, a_n \rangle \in \mathfrak{M} \iff \exists x_1 \ldots x_m \{P(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0 \,\&\, |x_1| + \cdots + |x_m| \leq Q(|a_1| + \cdots + |a_n|)\}$$

where P and Q are polynomials and $|x|$ denotes the binary length of x.

Nota bene: it is not required that

$$\langle a_1, \ldots, a_n \rangle \in \mathfrak{M} \iff \exists x_1 \ldots x_m \{P(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0\}$$

Open problem $\mathbf{D}\overset{?}{=}\mathbf{NP}$

$$\langle a_1, \dots, a_n \rangle \in \mathfrak{M} \iff \exists x_1 \dots x_m \{ P(a_1, \dots, a_n, x_1, \dots, x_m) = 0 \,\&\, |x_1| + \dots + |x_m| \le Q(|a_1| + \dots + |a_n|) \}$$

Conjecture (L. Adleman & K. Manders 1975). D=NP

Theorem (Bernard R. Hodgson & Clement F. Kent 1983, Stasis Yukna 1982). *Class* **NP** *can be defined as the class of sets having Davis bounded normal form*

$$\langle a_1, \dots, a_n \rangle \in \mathfrak{M} \iff \exists x \Big\{ |x| \le A(|a_1| + \dots + |a_n|) \,\&\, \forall y \Big\{ y \le B(|a_1| + \dots + |a_n|) \Rightarrow \exists z_1 \dots z_m \Big\{ \mathop{\&}_{k=1}^{m} |z_k| \le C_k(|a_1| + \dots + |a_n|) \,\&\, R(a_1, \dots, a_n, x, y, z_1, \dots, z_m) = 0 \Big\} \Big\} \Big\}$$

where A, B, C_1, ..., C_m, and R are polynomials.

Millenium problem (Clay Mathematical Institute, 2000). $\mathrm{P}\overset{?}{=}\mathrm{NP}$

D vs NP

Trivial fact. D $\subseteq$ NP.

Theorem (K. Manders & L. Adleman 1978). *Class* D *contains* NP*-complete problems.*

Theorem (K. Manders & L. Adleman 1975).

$$\{\langle a, b, c\rangle : a = b^c\} \in \mathbf{D}$$

Conditions sufficient for **D=NP**

Prototypical theorem. *If certain set* $\mathfrak{M}$ *belongs to* **D**, *then* **D=NP**

Examples 1 (K. Manders & L. Adleman 1975).

$$\mathfrak{M} = \left\{ m : m = \sum_{k=0}^{K} m_k 4^k,\ \ m_k \in \{0,1\} \right\}$$

Examples 2 (J. P. Jones & Yu. Matiyasevich 1984).

$$\mathfrak{M} = \left\{ \langle m, n \rangle : m = \sum_{k=0}^{K} m_k 2^k,\ \ n = \sum_{k=0}^{K} n_k 2^k,\ \ m_k \le n_k \right\}$$

Conditions sufficient for **D=NP**

Prototypical theorem. *If certain set* $\mathfrak{M}$ *belongs to* **D**, *then* **D=NP**

Examples 3 (Ramarathanam Venkatesan & Sivaramakrishnan Rajagopalan, 1992).

$$\mathfrak{M} = \Big\{ \langle a, b\rangle : \text{for every odd prime factor } p \text{ of } b \\ \text{the residue of } a \bmod p \text{ is even} \Big\}$$

Theorem (Ramarathanam Venkatesan & Sivaramakrishnan Rajagopalan, 1992). *If* **D=NP** *then Randomized Diophantine Problem is average-case complete.*