Some recent development aroused from Hilbert's tenth problem

Yuri Matiyasevich

Steklov Institute of Mathematics at St. Petersburg

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. De la possibilité de résoudre une équation diophantienne. On donne une équation de Diophante à un nombre quelconque d'inconnues et à coefficients entiers rationnels: *on demande de trouver une méthode par laquelle, au moyen d'un nombre fini d'opérations, on pourra distinguer si l'équation est résoluble en nombres entiers rationnels.*

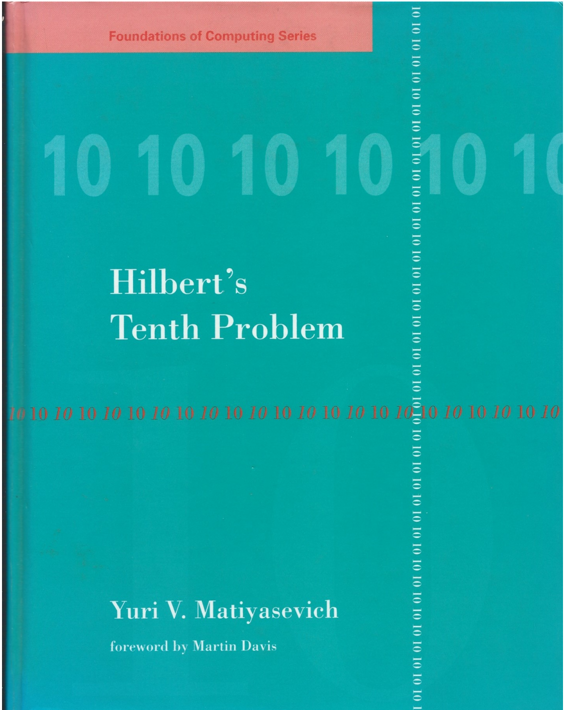
10. Determination of the solvability of a Diophantine equation. Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: *To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable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

математическая логика и основания математики

Ю. В. Матиясевич

ДЕСЯТАЯ ПРОБЛЕМА ГИЛЬБЕРТА

1993


Foundations of Computing Series
Hilbert's
Tenth Problem
Yuri V. Matiyasevich
foreword by Martin Davis

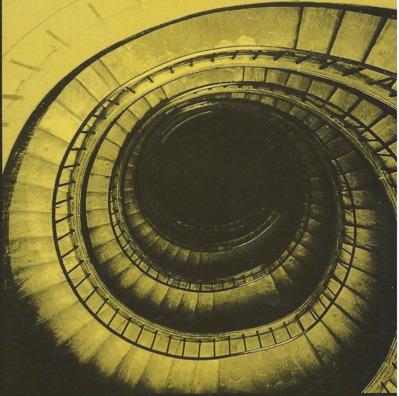
1993

AXIOMES

Le dixième problème de Hilbert
Son indécidabilité

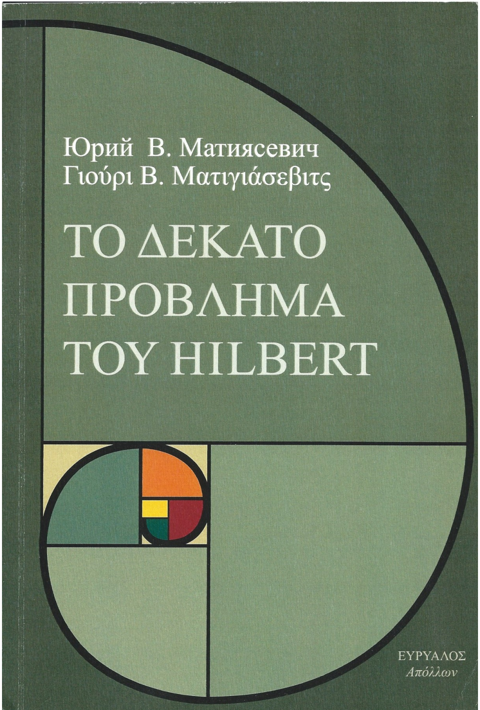
Youri MATIIASSEVITCH

Traduction de
P. CEGIELSKI et D. RICHARD



MASSON

1995


Юрий В. Матиясевич
Γιούρι Β. Ματιγιάσεβιτς
ΤΟ ΔΕΚΑΤΟ
ΠΡΟΒΛΗΜΑ
ΤΟΥ HILBERT
ΕΥΡΥΑΛΟΣ
Απόλλων

2022

Feb. 19, 2019
From Christos Grammatikas <grammatikas.christos@gmail.com>

Dear Professor Матиясевич,

We are in the process of translating into Greek your masterpiece

Десятая Проблема Гильберта

and we are wondering if you might be kind enough to contribute some sort of presentation for the Greek edition. This could take any form that you judge appropriate, from a short introduction to a more substantial comment, either in Russian or in English.

With our best regards,

Christos Grammatikas
EURYALOS editions

Feb. 20, 2019
From Yuri Matiyasevich <yumat@pdmi.ras.ru>

Dear Professor Grammatikas,

.

.

.

Are you doing the translation

A) from the Russian original?

B) from the English translation?

C) from the French translation?

Feb. 22, 2019
Christos Grammatikas <grammatikas.christos@gmail.com>

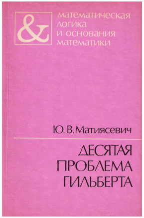
Dear Professor Matiyasevich,

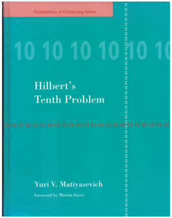
First of all, I will answer your questions. For the translation we use all of A, B, C.

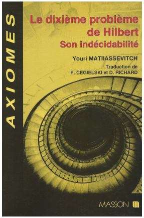
The main translator is a high school professor, Demosthenes Stalides($\Delta\eta\mu o\sigma\theta\varepsilon\nu\eta\varsigma\ \Sigma\tau\alpha\lambda\iota\delta\eta\varsigma$), using the English version.

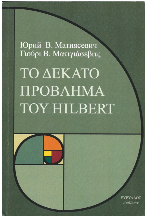
As I have a working knowledge of the Russian language (I studied it for two and a half years) and can also rely on the help of collaborators who are not mathematicians but fluent in Russian, my role consists on eventual adjustments in order to bring the text closer to the style of the Russian original.

Living in Paris for over fifty years now, I consult also frequently the French translation.









⋮

Bibliography

⋮

Patrick Cégielski
La théorie de corps réel-clos inductifs est une extension conservative de l'Arithmétique de Peano
Comptes Rendus de l'Académie des Sciences. Série I. Mathématique, 310(5), 239–242, 1990.

⋮

The future second edition of the book will contain in the Bibliography:

⋮

Patrick Cégielski, Denis Richard, and Maxim Vsemirnov
On the additive theory of prime numbers
Fundamenta Informaticae 81, No. 1-3, 83–96, 2007

⋮

Hilbert's tenth problem: *The theory* $\mathrm{Th}_{\exists}(\mathbb{N}, +, \times)$ *is undecidable.*

$$\exists x_1, \ldots, x_n \left[P(x_1, \ldots, x_n) = 0 \right]$$

Hilbert's tenth problem: *The theory* $\mathrm{Th}_\exists(\mathbb{N}, +, \times)$ *is undecidable.*

Julia Robinson [1969]: *The theory* $\mathrm{Th}_\exists(\mathbb{N}, +, \times, \mathbb{P})$ *is undecidable (where* $\mathbb{P}$ *is the set of all prime numbers).*

Hilbert's tenth problem: *The theory* $\mathrm{Th}_{\exists}(\mathbb{N}, +, \times)$ *is undecidable.*

Julia Robinson [1969]: *The theory* $\mathrm{Th}_{\exists}(\mathbb{N}, +, \times, \mathbb{P})$ *is undecidable (where* $\mathbb{P}$ *is the set of all prime numbers).*

Open Question: *Is the theory* $\mathrm{Th}(\mathbb{N}, +, \mathbb{P})$ *undecidable ?*

Hilbert's tenth problem: *The theory* $\mathrm{Th}_{\exists}(\mathbb{N},+,\times)$ *is undecidable.*

Julia Robinson [1969]: *The theory* $\mathrm{Th}_{\exists}(\mathbb{N},+,\times,\mathbb{P})$ *is undecidable (where* $\mathbb{P}$ *is the set of all prime numbers).*

Open Question: *Is the theory* $\mathrm{Th}(\mathbb{N},+,\mathbb{P})$ *undecidable ?*

Goldbach's conjecture: $\forall n \exists p, q [p \in \mathbb{P} \,\&\, q \in \mathbb{P} \,\&\, p + q = 2n + 4]$

Hilbert's tenth problem: *The theory* $\mathrm{Th}_\exists(\mathbb{N}, +, \times)$ *is undecidable.*

Julia Robinson [1969]: *The theory* $\mathrm{Th}_\exists(\mathbb{N}, +, \times, \mathbb{P})$ *is undecidable (where* $\mathbb{P}$ *is the set of all prime numbers).*

Open Question: *Is the theory* $\mathrm{Th}(\mathbb{N}, +, \mathbb{P})$ *undecidable ?*

Goldbach's conjecture: $\forall n \exists p, q[p \in \mathbb{P} \,\&\, q \in \mathbb{P} \,\&\, p + q = 2n + 4]$

The infinitude of twin primes: $\forall n \exists m[n + m \in \mathbb{P} \,\&\, n + m + 2 \in \mathbb{P}]$

Hilbert's tenth problem: *The theory* $\mathrm{Th}_\exists(\mathbb{N},+,\times)$ *is undecidable.*

Julia Robinson [1969]: *The theory* $\mathrm{Th}_\exists(\mathbb{N},+,\times,\mathbb{P})$ *is undecidable (where* $\mathbb{P}$ *is the set of all prime numbers).*

Open Question: *Is the theory* $\mathrm{Th}(\mathbb{N},+,\mathbb{P})$ *undecidable ?*

P. T. Bateman, C. G. Jockusch, and A. R. Woods [1993, under some number-theoretical hypothesis.] *The theory* $\mathrm{Th}(\mathbb{N},+,\mathbb{P})$ *is undecidable.*

Hilbert's tenth problem: *The theory* $\mathrm{Th}_\exists(\mathbb{N}, +, \times)$ *is undecidable.*

Julia Robinson [1969]: *The theory* $\mathrm{Th}_\exists(\mathbb{N}, +, \times, \mathbb{P})$ *is undecidable (where* $\mathbb{P}$ *is the set of all prime numbers).*

Open Question: *Is the theory* $\mathrm{Th}(\mathbb{N}, +, \mathbb{P})$ *undecidable ?*

P. T. Bateman, C. G. Jockusch, and A. R. Woods [1993, under some number-theoretical hypothesis.] *The theory* $\mathrm{Th}(\mathbb{N}, +, \mathbb{P})$ *is undecidable.*

Open Question: *Is the theory* $\mathrm{Th}_\exists(\mathbb{N}, +, \mathbb{P})$ *decidable* ?

Hilbert's tenth problem: *The theory* $\mathrm{Th}_\exists(\mathbb{N}, +, \times)$ *is undecidable.*

Julia Robinson [1969]: *The theory* $\mathrm{Th}_\exists(\mathbb{N}, +, \times, \mathbb{P})$ *is undecidable (where* $\mathbb{P}$ *is the set of all prime numbers).*

Open Question: *Is the theory* $\mathrm{Th}(\mathbb{N}, +, \mathbb{P})$ *undecidable ?*

P. T. Bateman, C. G. Jockusch, and A. R. Woods [1993, under some number-theoretical hypothesis.] *The theory* $\mathrm{Th}(\mathbb{N}, +, \mathbb{P})$ *is undecidable.*

Open Question: *Is the theory* $\mathrm{Th}_\exists(\mathbb{N}, +, \mathbb{P})$ *decidable* ?

A. Woods [2000, under some number-theoretical hypothesis.] *The theory* $\mathrm{Th}_\exists(\mathbb{N}, +, \mathbb{P})$ *is decidable.*

Hilbert's tenth problem: *The theory* $\mathrm{Th}_\exists(\mathbb{N}, +, \times)$ *is undecidable.*

Julia Robinson [1969]: *The theory* $\mathrm{Th}_\exists(\mathbb{N}, +, \times, \mathbb{P})$ *is undecidable (where* $\mathbb{P}$ *is the set of all prime numbers).*

Open Question: *Is the theory* $\mathrm{Th}(\mathbb{N}, +, \mathbb{P})$ *undecidable ?*

P. T. Bateman, C. G. Jockusch, and A. R. Woods [1993, under some number-theoretical hypothesis.] *The theory* $\mathrm{Th}(\mathbb{N}, +, \mathbb{P})$ *is undecidable.*

Open Question: *Is the theory* $\mathrm{Th}_\exists(\mathbb{N}, +, \mathbb{P})$ *decidable* ?

A. Woods [2000, under some number-theoretical hypothesis.] *The theory* $\mathrm{Th}_\exists(\mathbb{N}, +, \mathbb{P})$ *is decidable.*

P. Cegielski, D. Richard, and M. Vsemirnov [2007] *The theory* $\mathrm{Th}_\exists\big(\mathbb{N}, +, n \longmapsto p_n, n \longmapsto p_n \mod (n)\big)$ *is undecidable.*

Main technical tool used for proving the undecidability of Hilbert's tenth problem

DPRM-Theorem. *Every effectively listable set of natural numbers* $\mathfrak{M}$ *can be represented in the following way:*

$$a \in M \iff \exists x_1 \dots x_n [P(x_1, \dots, x_n) = a]$$

where $P(x_1, \dots, x_n)$ *is a polynomial with integer coefficients.*

DPRM – after Martin Davis, Hilary Putnam, Julia Robinson, and Yuri M.

Corollary. *There exists a polynomial* $P(x_1, \dots, x_n)$ *such that the set of its positive values is exactly the set of prime numbers:*

$$a \text{ is prime } \iff \exists x_1 \dots x_n [P(x_1, \dots, x_n) = a].$$

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 (for non-negative integer values of the 26 variables) by the polynomial*

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

Computer verification of DPRM-theorem

Karol Pak

The Matiyasevich Theorem; Diophantine sets

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

Mario Carneiro

A Lean formalization of Matiyasevič's Theorem,

`https://arxiv.org/abs/1802.01795v1`, 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)

Who needs difficult problems?

Cryptography

DE GRUYTER DOI 10.1515/gcc-2014-0011 — Groups Complex. Cryptol. 2014; 6 (2):103–120

Research Article

Alexei Myasnikov and Vitalii Roman'kov

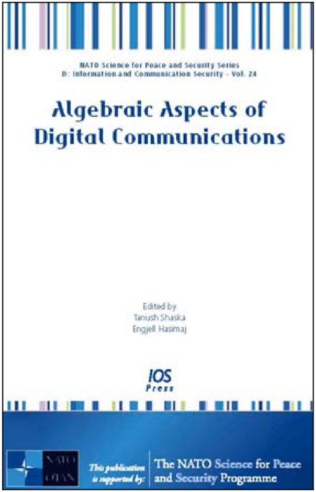
Diophantine cryptography in free metabelian groups: Theoretical base

Introduction

In this paper we study so-called Diophantine cryptology, a collection of cryptographic schemes where the computational security assumptions are based on hardness of solving some Diophantine equations ...

Due to Matiyasevich we know that the classical Diophantine problem (over integers $\mathbb{Z}$) is undecidable ...

There are some obvious advantages of using Diophantine equations in cryptography. First of all, the language of Diophantine equations is quite universal ... the real measure of universality in this case comes from a beautiful MRDP theorem, the result (due collectively to Matiyasevich, Robinson, Davis and Putnam) [15, 17], which states that every computably enumerable set is Diophantine.



Algebraic Aspects of Digital Communications

Volume 24 NATO Science for Peace and Security Series - D: Information and Communication Security
Editors: T. Shaska and E. Hasimaj
August 2009, 296 pp., hardcover
ISBN: 978-1-60750-019-3
Price: US$174 / €120 / £108

Ustimenko, V.

On the cryptographical properties of extremal algebraic graphs

pp. 256-281

V. Ustimenko

On the cryptographical properties of extremal algebraic graphs

Summary: We consider some properties of stream ciphers related to arithmetical dynamical systems over a commutative ring K.

...

The straightforward generalization of such encryption can be used in a public key mode. We introduce much more general algorithms in terms of automata related to directed algebraic graphs with high girth indicator.

...

The family of infinite algebraic directed graphs with the large girth indicator can be defined over infinite commutative ring K. Some theoretical examples of encryption algorithms related to such families are considered in the case of $K = \mathbb{Z}$ and Gaussian complex numbers. They use prime generating polynomials (Matijasevic's polynomials) and can be implemented on classical Turing machine or probabilistic machine (quantum computer, in particular).

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.*

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®

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]

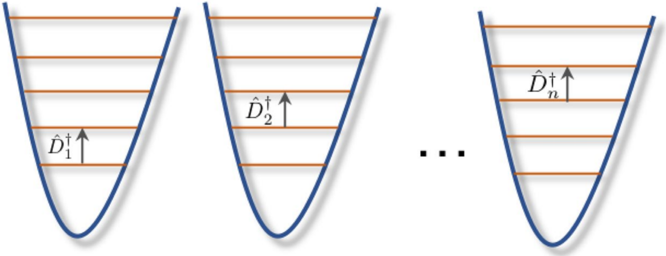


Figure 1. A physical system for simulating Diophantine equations with n variables. The system is either n trapped ions or an n–mode coherent field. The controls $\hat{D}_1^\dagger, \ldots, \hat{D}_n^\dagger$ independently address each subsystem. For ions, the controls excite transitions between nearest 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.

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.

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

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

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

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

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