Hilbert's tenth problem
(tutorial)

Yuri Matiyasevich

Steklov Institute of Mathematics at St.Petersburg, Russia

http://logic.pdmi.ras.ru/~yumat

Hilbert's Tenth Problem

The Statement

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*.

Hilbert's Tenth Problem

The Statement

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*.

Hilbert's Tenth Problem

The Statement

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*.

David Hilbert, *Mathematical Problems* [1900]

Hilbert's Tenth Problem

Terminology

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*.

Hilbert's Tenth Problem

Terminology

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.

Hilbert's Tenth Problem

Terminology

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.

Diophantus was a Greek mathematician.

Hilbert's Tenth Problem

Range of Unknowns

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*.

Hilbert's Tenth Problem

Range of Unknowns

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*.

Rational integers are nothing else but numbers $0, \pm 1, \pm 2, \ldots$ which will be called during my talk just integers.

Hilbert's Tenth Problem

Range of Unknowns

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*.

Rational integers are nothing else but numbers $0, \pm 1, \pm 2, \ldots$ which will be called during my talk just integers.

Greek mathematician *Diophantus* lived in the 3rd century A.D.

Hilbert's Tenth Problem

Terminology

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*.

Hilbert's Tenth Problem

Terminology

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*.

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.

Hilbert's Tenth Problem

Terminology

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*.

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.

Non-negative Integers vs All Integers

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

Non-negative Integers vs All Integers

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

Has this equation solutions in integers?

Non-negative Integers vs All Integers

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

Has this equation solutions in integers?
Yes, and this is trivial.

Non-negative Integers vs All Integers

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

Has this equation solutions in integers?
Yes, and this is trivial.

Has this equation solutions in non-negative integers?

Non-negative Integers vs All Integers

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

Has this equation solutions in integers?
Yes, and this is trivial.

Has this equation solutions in non-negative integers?
No, and this isn't trivial.

From all integers to non-negative integers

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 non-negative integers $p_1, \ldots, p_m$, $q_1, \ldots, q_m$.

From all integers to non-negative integers

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 non-negative integers $p_1, \ldots, p_m$, $q_1, \ldots, q_m$.

So 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 non-negative integers.

From Non-negative Integers to All Integers

An equation

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

has a solution in non-negative integers 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 non-negative integer is the sum of four squares.

From Non-negative Integers to All Integers

An equation

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

has a solution in non-negative integers 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 non-negative integer 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 non-negative integers.

From Non-negative Integers to All Integers

An equation

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

has a solution in non-negative integers 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 non-negative integer 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 non-negative integers.

We will deal with solving Diophantine equations in non-negative integers so all lower-case italic letters will range over $0, 1, 2, \ldots$

Hilbert's Tenth Problem

Terminology

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*.

Thue problem (word problem for semigroups)

The first undecidable decision problem in mathematics proper

Andrei A. Markov
1903–1979

Emil L. Post
1897–1954

Hilbert's Tenth Problem

"The begger"

Recursively enumerable sets of positive integers and their decision problems. *Bulletin AMS*, **50**, 284–316 (1944); reprinted in: The Collected Works of E. L. Post, Davis, M. (ed), Birkhäuser, Boston, 1994.

Hilbert's 10th problem "begs for an unsolvability proof"

Emil L. Post
1897–1954

Parametric Equations

Diophantine Sets

A *family* of Diophantine equations:

$$P(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0,$$

where P is a polynomial with integer coefficients

Parametric Equations

Diophantine Sets

A *family* of Diophantine equations:

$$P(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0,$$

where P is a polynomial with integer coefficients, the variables of which are split into two groups:

- the *parameters* $a_1, \ldots, a_n$;
- the *unknowns* $x_1, \ldots, x_m$.

Parametric Equations

Diophantine Sets

A *family* of Diophantine equations:

$$P(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0,$$

where P is a polynomial with integer coefficients, the variables of which are split into two groups:

- the *parameters* $a_1, \ldots, a_n$;
- the *unknowns* $x_1, \ldots, x_m$.

Consider the set $\mathfrak{M}$ such that

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

Parametric Equations

Diophantine Sets

A *family* of Diophantine equations:

$$P(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0,$$

where P is a polynomial with integer coefficients, the variables of which are split into two groups:

- the *parameters* $a_1, \ldots, a_n$;
- the *unknowns* $x_1, \ldots, x_m$.

Consider the set $\mathfrak{M}$ such that

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

Sets having such *representations* are called *Diophantine*.

Examples

Some easy examples of Diophantine sets:

Examples

Some easy examples of Diophantine sets:

- *the set of all squares*, represented by equation

$$a - x^2 = 0;$$

Examples

Some easy examples of Diophantine sets:

- *the set of all squares*, represented by equation

$$a - x^2 = 0;$$

- *the set of all composite numbers*, represented by equation

$$a - (x_1 + 2)(x_2 + 2) = 0;$$

Examples

Some easy examples of Diophantine sets:

- *the set of all squares*, represented by equation

$$a - x^2 = 0;$$

- *the set of all composite numbers*, represented by equation

$$a - (x_1 + 2)(x_2 + 2) = 0;$$

- *the set of all positive integers which are not powers of 2*, represented by equation

$$a - (2x_1 + 3)(x_2 + 1) = 0.$$

Listable Sets

Given a parametric Diophantine equation

$$P(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$$

we can effectively list all n-tuples from the Diophantine set $\mathfrak{M}$ represented by this equation. Namely, we need only to look over, in some order, all $(n + m)$-tuples of possible values of all variables $a_1, \ldots, a_n$, $x_1, \ldots x_m$ and check every time whether the equality holds or not. As soon as it does, we put the tuple $\langle a_1, \ldots, a_n \rangle$ on the list of elements of $\mathfrak{M}$. In this way every tuple from $\mathfrak{M}$ will sooner or later appear on the list, maybe many times.

Listable Sets

Given a parametric Diophantine equation

$$P(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$$

we can effectively list all n-tuples from the Diophantine set $\mathfrak{M}$ represented by this equation. Namely, we need only to look over, in some order, all $(n+m)$-tuples of possible values of all variables $a_1, \ldots, a_n$, $x_1, \ldots x_m$ and check every time whether the equality holds or not. As soon as it does, we put the tuple $\langle a_1, \ldots, a_n \rangle$ on the list of elements of $\mathfrak{M}$. In this way every tuple from $\mathfrak{M}$ will sooner or later appear on the list, maybe many times.

Definition A set $\mathfrak{M}$ of n-tuples of natural numbers is called *listable* or *effectively enumerable*, if there is an algorithm which would print in some order, possibly with repetitions, all elements of the set $\mathfrak{M}$.

From Evident to Unbelievable

Evident fact. Every Diophantine set is effectively enumerable.

From Evident to Unbelievable

Evident fact. Every Diophantine set is effectively enumerable.

Martin Davis' Conjecture. Every effectively enumerable set is Diophantine.

From Evident to Unbelievable

Evident fact. Every Diophantine set is effectively enumerable.

Martin Davis' Conjecture. Every effectively enumerable set is Diophantine.

Corollary of Davis' Conjecture *There is a polynomial Q such that the equation*

$$Q(a, x_1, \ldots, x_m) = 0$$

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

From Evident to Unbelievable

Evident fact. Every Diophantine set is effectively enumerable.

Martin Davis' Conjecture. Every effectively enumerable set is Diophantine.

Corollary of Davis' Conjecture *There is a polynomial Q such that the equation*

$$Q(a, x_1, \ldots, x_m) = 0$$

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

Corollary of Davis' Conjecture *There is a polynomial P such that the equation*

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

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

Listing Listable Sets

A *list of all listable sets*:

$$\mathfrak{M}_0, \mathfrak{M}_1, \ldots, \mathfrak{M}_k, \ldots$$

Formally, for every n there exists a listable set $\mathfrak{U}_n$ of $(n+1)$-tuples such that

$$\langle a_1, \ldots, a_n \rangle \in \mathfrak{M}_k \iff \langle a_1, \ldots, a_n, k \rangle \in \mathfrak{U}_n.$$

Listing Listable Sets

A *list of all listable sets*:

$$\mathfrak{M}_0, \mathfrak{M}_1, \ldots, \mathfrak{M}_k, \ldots$$

Formally, for every n there exists a listable set $\mathfrak{U}_n$ of $(n+1)$-tuples such that

$$\langle a_1, \ldots, a_n \rangle \in \mathfrak{M}_k \Longleftrightarrow \langle a_1, \ldots, a_n, k \rangle \in \mathfrak{U}_n.$$

Being listable, $\mathfrak{U}_n$ has a Diophantine representation:

$$\langle a_1, \ldots, a_n, a_{n+1} \rangle \in \mathfrak{U}_n \Longleftrightarrow$$
$$\exists y_1 \ldots y_M \{ U_n(a_1, \ldots, a_n, a_{n+1}, y_1, \ldots, y_M) = 0 \}.$$

Universal Equations

Collapse of Diophantine Hierarchy

Corollary of Martin Davis Conjecture *For every n there exist an equation*

$$U_n(a_1, \ldots, a_n, k, y_1, \ldots, y_M) = 0 \tag{1}$$

which is universal *in the following sense: For every Diophantine equation*

$$P(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0 \tag{2}$$

one can effectively find a particular number k_P such that, for given value of the parameters $a_1, \ldots, a_n$, equation (??) has a solution in $x_1, \ldots, x_m$ if and only if equation

$$U_n(a_1, \ldots, a_n, k_P, y_1, \ldots, y_M) = 0$$

has a solution in $y_1, \ldots, y_M$.

First Step

Theorem (Martin Davis [1950]) *Every listable set* $\mathfrak{M}$ *has a representation of the form*

$$\langle a_1, \ldots, a_n \rangle \in \mathfrak{M} \Longleftrightarrow$$
$$\exists z \forall y_{\leq z} \exists x_1 \ldots x_m \{ P(a_1, \ldots, a_n, x_1, \ldots, x_m, y, z) = 0 \}.$$

First Step

Theorem (Martin Davis [1950]) *Every listable set $\mathfrak{M}$ has a representation of the form*

$$\langle a_1, \ldots, a_n \rangle \in \mathfrak{M} \Longleftrightarrow$$
$$\exists z \forall y_{\leq z} \exists x_1 \ldots x_m \{ P(a_1, \ldots, a_n, x_1, \ldots, x_m, y, z) = 0 \}.$$

Such representations have become known as *Davis normal form*.

First Step

Theorem (Martin Davis [1950]) *Every listable set* $\mathfrak{M}$ *has a representation of the form*

$$\langle a_1, \ldots, a_n \rangle \in \mathfrak{M} \Longleftrightarrow$$
$$\exists z \forall y_{\leq z} \exists x_1 \ldots x_m \{ P(a_1, \ldots, a_n, x_1, \ldots, x_m, y, z) = 0 \}.$$

Such representations have become known as *Davis normal form*.

Theorem (Kurt Gödel [1931]). Every effectively enumerable set $\mathfrak{M}$ has an arithmetical representation.

DPR-theorem

A Mile-Stone on the Way to the Proof of Davis' Conjecture

Theorem (Martin Davis, Hilary Putnam, Julia Robinson [1961])
Every listable set $\mathfrak{M}$ has an *exponential Diophantine representation*, i.e., a representation of the form

$$\langle a_1, \ldots, a_n \rangle \in \mathfrak{M} \Longleftrightarrow$$
$$\exists x_1 \ldots x_m \{ E_{\mathrm{L}}(a_1, \ldots, a_n, x_1, \ldots, x_m) \;=\; E_{\mathrm{R}}(a_1, \ldots, a_n, x_1, \ldots, x_m) \}$$

where E_{L} and E_{R} are expression constructed by traditional rules from the variables and particular positive integers by addition, multiplication and exponentiation.

DPR-theorem

A Mile-Stone on the Way to Undecidability of Hilbert's 10th problem

Theorem (Martin Davis, Hilary Putnam, Julia Robinson [1961]). The analogue of Hilbert's tenth problem for exponential Diophantine equations is undecidable.

An exponential Diophantine equation has the form

$$E_1(x_1, x_2, \ldots, x_m) = E_2(x_1, x_2, \ldots, x_m)$$

where E_1 and E_2 are expression constructed by combining the variables and particular natural numbers using the traditional rules of addition, multiplication and exponentiation.

Missing link

From Exponential Diophantine equations to Genuine Diophantine Equations

After the work of Davis-Putnam-Robinson, in order to prove the undecidability of Hilbert's 10th problem it was sufficient to find a particular Diophantine equation with 3 parameters such that

$$a^b = c \iff \exists z_1 \dots z_m \{A(a, b, c, w_1, \dots, w_m) = 0\} \qquad (*)$$

Missing link

From Exponential Diophantine equations to Genuine Diophantine Equations

After the work of Davis-Putnam-Robinson, in order to prove the undecidability of Hilbert's 10th problem it was sufficient to find a particular Diophantine equation with 3 parameters such that

$$a^b = c \iff \exists z_1 \dots z_m \{A(a, b, c, w_1, \dots, w_m) = 0\} \qquad (*)$$

Theorem (Julia Robinson [1952]) Such an equation $(*)$ exists provided that there exists a two-parameter Diophantine equation

$$J(u, v, y_1, \dots, y_n) = 0$$

such that

- in every solution $u < v^v$;
- for every k there exists a solution with $u > v^k$.

Missing link

From Exponential Diophantine equations to Genuine Diophantine Equations

After the work of Davis-Putnam-Robinson, in order to prove the undecidability of Hilbert's 10th problem it was sufficient to find a particular Diophantine equation with 3 parameters such that

$$a^b = c \iff \exists z_1 \dots z_m \{A(a, b, c, w_1, \dots, w_m) = 0\} \qquad (*)$$

Theorem (Julia Robinson [1952]) Such an equation $(*)$ exists provided that there exists a two-parameter Diophantine equation

$$J(u, v, y_1, \dots, y_n) = 0$$

such that

- in every solution $u < v^v$;
- for every k there exists a solution with $u > v^k$.

Relations between u and v with these two properties were named by Julia Robinson *relations of exponential growth*; today they are known also as *Julia Robinson predicates*.

Mathematical Reviews 1962, 24A, page 574, review A3061:

Davis, Martin; Putnam, Hilary; Robinson, Julia. The decision problem for exponential Diophantine equations. Ann. Math. (2), **74** 425–436 (1961).

. . . These results are superficially related to Hilbert's tenth problem on (ordinary, i.e., non-exponential) Diophantine equations. The proof of the authors'results, though very elegant, does not use recondite facts in the theory of numbers nor in the theory of r.e. [recursively enumerable] sets, and so it is likely that the present result is not closely connected with Hilbert's tenth problem. . .

Also it is not altogether plausible that all (ordinal) Diophantine problems are uniformly reducible to those in a fixed number of variables of fixed degree, which would be the case if all r.e. sets were Diophantine.

Mathematical Reviews 1962, 24A, page 574, review A3061:

Davis, Martin; Putnam, Hilary; Robinson, Julia. The decision problem for exponential Diophantine equations. Ann. Math. (2), **74** 425–436 (1961).

. . . These results are superficially related to Hilbert's tenth problem on (ordinary, i.e., non-exponential) Diophantine equations. The proof of the authors'results, though very elegant, does not use recondite facts in the theory of numbers nor in the theory of r.e. [recursively enumerable] sets, and so it is likely that the present result is not closely connected with Hilbert's tenth problem. . .

Also it is not altogether plausible that all (ordinal) Diophantine problems are uniformly reducible to those in a fixed number of variables of fixed degree, which would be the case if all r.e. sets were Diophantine.

G.Kreisel

Word Equations vs Diophantine Equations

Andrei A. Markov
1903–1979

Solving a word equation in the two-letter alphabet $\{\alpha_0, \alpha_1\}$ can be easily reduced to solving a particular Diophantine equation thanks to the following fact: *every* 2×2 *matrix with natural number entries and determinant equal to 1 can be represented in a unique way as the product of matrices* $A_0 = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ *and* $A_1 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ *and hence a word* $\alpha_{i_1} \ldots \alpha_{i_n}$ *can be represented by the four entries of the matrix* $A_{i_1} \ldots A_{i_n}$.

Word Equations vs Diophantine Equations

Andrei A. Markov
1903–1979

Solving a word equation in the two-letter alphabet $\{\alpha_0, \alpha_1\}$ can be easily reduced to solving a particular Diophantine equation thanks to the following fact: *every* 2×2 *matrix with natural number entries and determinant equal to 1 can be represented in a unique way as the product of matrices* $A_0 = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ *and* $A_1 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ *and hence a word* $\alpha_{i_1} \ldots \alpha_{i_n}$ *can be represented by the four entries of the matrix* $A_{i_1} \ldots A_{i_n}$.

G. S. Makanin [1977]: *Word equations are decidable*

Word Equations

Main alphabet: $A_n = \{\alpha_1, \ldots, \alpha_n\}$

Word Equations

Main alphabet: $A_n = \{\alpha_1, \ldots, \alpha_n\}$

Alphabet of unknowns: $U = \{\upsilon_1, \ldots, \upsilon_m\}$

Word Equations

Main alphabet: $A_n = \{\alpha_1, \ldots, \alpha_n\}$

Alphabet of unknowns: $U = \{\upsilon_1, \ldots, \upsilon_m\}$, $A_n \cap U = \emptyset$

Word Equations

Main alphabet: $A_n = \{\alpha_1, \ldots, \alpha_n\}$

Alphabet of unknowns: $U = \{\upsilon_1, \ldots, \upsilon_m\}$, $A_n \cap U = \emptyset$

Word equation: $P = Q$ where $P, Q \in (A_n \cup U)^*$

Word Equations

Main alphabet: $A_n = \{\alpha_1, \ldots, \alpha_n\}$

Alphabet of unknowns: $U = \{\upsilon_1, \ldots, \upsilon_m\}$, $A_n \cap U = \emptyset$

Word equation: $P = Q$ where $P, Q \in (A_n \cup U)^*$

Solution: words $V_1, \ldots, V_m \in A_n^*$ such that

$$P^{\upsilon_1,\ldots,\upsilon_m}_{V_1,\ldots,V_m} \equiv Q^{\upsilon_1,\ldots,\upsilon_m}_{V_1,\ldots,V_m}$$

From Words to Numbers

(First Numbering: Matrices)

W.o.l.g $n = 2$, i.e., $A_2 = \{\alpha_1, \alpha_2\}$

From Words to Numbers

(First Numbering: Matrices)

W.o.l.g $n = 2$, i.e., $A_2 = \{\alpha_1, \alpha_2\}$

Lemma. Every 2×2 matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with natural number elements and the determinant equal to 1 can be represented in a unique way as the product of matrices $M_1 = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ and $M_2 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

From Words to Numbers

(First Numbering: Matrices)

W.o.l.g $n = 2$, i.e., $A_2 = \{\alpha_1, \alpha_2\}$

Lemma. Every 2×2 matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with natural number elements and the determinant equal to 1 can be represented in a unique way as the product of matrices $M_1 = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ and $M_2 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

$$"\alpha_{i_1} \dots \alpha_{i_k}" \quad \sim \quad M_{i_1} \times \cdots \times M_{i_k}$$

From Words to Numbers

(First Numbering: Matrices)

W.o.l.g $n = 2$, i.e., $A_2 = \{\alpha_1, \alpha_2\}$

Lemma. Every 2×2 matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with natural number elements and the determinant equal to 1 can be represented in a unique way as the product of matrices $M_1 = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ and $M_2 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

$$
\begin{aligned}
"\alpha_{i_1} \ldots \alpha_{i_k}" &\sim M_{i_1} \times \cdots \times M_{i_k} \\
\upsilon_1, \ldots, \upsilon_m &\sim a_1, b_1, c_1, d_1, \ldots, a_m, b_m, c_m, d_m
\end{aligned}
$$

From Words to Numbers

(First Numbering: Matrices)

W.o.l.g $n = 2$, i.e., $A_2 = \{\alpha_1, \alpha_2\}$

Lemma. Every 2×2 matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with natural number elements and the determinant equal to 1 can be represented in a unique way as the product of matrices $M_1 = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ and $M_2 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

$$
\begin{aligned}
"\alpha_{i_1} \ldots \alpha_{i_k}" &\sim M_{i_1} \times \cdots \times M_{i_k} \\
\upsilon_1, \ldots, \upsilon_m &\sim a_1, b_1, c_1, d_1, \ldots, a_m, b_m, c_m, d_m
\end{aligned}
$$

$$
P = Q \sim \begin{array}{l}
P_{11}(\ldots, a_i, b_i, c_i, d_i, \ldots,) = Q_{11}(\ldots, a_i, b_i, c_i, d_i, \ldots,) \\
P_{12}(\ldots, a_i, b_i, c_i, d_i, \ldots,) = Q_{12}(\ldots, a_i, b_i, c_i, d_i, \ldots,) \\
P_{21}(\ldots, a_i, b_i, c_i, d_i, \ldots,) = Q_{21}(\ldots, a_i, b_i, c_i, d_i, \ldots,) \\
P_{22}(\ldots, a_i, b_i, c_i, d_i, \ldots,) = Q_{22}(\ldots, a_i, b_i, c_i, d_i, \ldots,)
\end{array}
$$

From Words to Numbers

(First Numbering: Matrices)

W.o.l.g $n = 2$, i.e., $A_2 = \{\alpha_1, \alpha_2\}$

Lemma. Every 2×2 matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with natural number elements and the determinant equal to 1 can be represented in a unique way as the product of matrices $M_1 = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ and $M_2 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

$$
\begin{aligned}
"\alpha_{i_1} \ldots \alpha_{i_k}" &\sim M_{i_1} \times \cdots \times M_{i_k} \\
\upsilon_1, \ldots, \upsilon_m &\sim a_1, b_1, c_1, d_1, \ldots, a_m, b_m, c_m, d_m
\end{aligned}
$$

$$
P = Q \sim \begin{array}{c}
P_{11}(\ldots, a_i, b_i, c_i, d_i, \ldots,) = Q_{11}(\ldots, a_i, b_i, c_i, d_i, \ldots,) \\
P_{12}(\ldots, a_i, b_i, c_i, d_i, \ldots,) = Q_{12}(\ldots, a_i, b_i, c_i, d_i, \ldots,) \\
P_{21}(\ldots, a_i, b_i, c_i, d_i, \ldots,) = Q_{21}(\ldots, a_i, b_i, c_i, d_i, \ldots,) \\
P_{22}(\ldots, a_i, b_i, c_i, d_i, \ldots,) = Q_{22}(\ldots, a_i, b_i, c_i, d_i, \ldots,) \\
a_1 d_1 - b_1 c_1 = \cdots = a_m d_m - b_m c_m = 1
\end{array}
$$

From Words to Numbers

(Second Numbering: Fibonacci weights)

Every word $X = "\beta_{i_m}\beta_{i_{m-1}}\ldots\beta_{i_1}"$ in the binary alphabet $B = \{\beta_0, \beta_1\} = \{0, 1\}$ can be viewed as the number

$$x = i_m u_m + i_{m-1} u_{m-1} + \cdots + i_1 u_1$$

written in positional system with weights of digits being the Fibonacci numbers $u_1 = 1$, $u_2 = 1$, $u_3 = 2$, $u_4 = 3$, ... (rather than traditional 1, 2, 4, 8, 16, ...).

From Words to Numbers

(Second Numbering: Fibonacci weights)

Every word $X = "\beta_{i_m}\beta_{i_{m-1}}\ldots\beta_{i_1}"$ in the binary alphabet $B = \{\beta_0, \beta_1\} = \{0, 1\}$ can be viewed as the number

$$x = i_m u_m + i_{m-1} u_{m-1} + \cdots + i_1 u_1$$

written in positional system with weights of digits being the Fibonacci numbers $u_1 = 1$, $u_2 = 1$, $u_3 = 2$, $u_4 = 3$, ... (rather than traditional 1, 2, 4, 8, 16, ...).

"0"∼0	"00"∼0	"000"∼0	"0000"∼0	"00000"∼0
"1"∼1	"01"∼1	"001"∼1	"0001"∼1	"00001"∼1
	"10"∼1	"010"∼1	"0010"∼1	"00010"∼1
	"11"∼2	"011"∼2	"0011"∼2	"00011"∼2
		"100"∼2	"0100"∼2	"00100"∼2
		"101"∼3	"0101"∼3	"00101"∼3
		"110"∼3	"0110"∼3	"00110"∼3
		"111"∼4	"0111"∼4	"00111"∼4

From Words to Numbers

(Second Numbering: Fibonacci weights)

Every word $X = "\beta_{i_m}\beta_{i_{m-1}}\ldots\beta_{i_1}"$ in the binary alphabet $B = \{\beta_0, \beta_1\} = \{0, 1\}$ can be viewed as the number

$$x = i_m u_m + i_{m-1} u_{m-1} + \cdots + i_1 u_1$$

written in positional system with weights of digits being the Fibonacci numbers $u_1 = 1$, $u_2 = 1$, $u_3 = 2$, $u_4 = 3$, ... (rather than traditional 1, 2, 4, 8, 16, ...).

"1"∼1	"10"∼1	"100"∼2	"1000"∼3	"10000"∼5
	"11"∼2	"101"∼3	"1001"∼4	"10001"∼6
		"110"∼3	"1010"∼4	"10010"∼6
		"111"∼4	"1011"∼5	"10011"∼7
			"1100"∼5	"11100"∼8
			"1101"∼6	"11101"∼9
			"1110"∼6	"11110"∼9
			"1111"∼7	"11111"∼10

From Words to Numbers

(Second Numbering: Fibonacci weights)

Every word $X = "\beta_{i_m}\beta_{i_{m-1}}\ldots\beta_{i_1}"$ in the binary alphabet $B = \{\beta_0, \beta_1\} = \{0, 1\}$ can be viewed as the number

$$x = i_m u_m + i_{m-1} u_{m-1} + \cdots + i_1 u_1$$

written in positional system with weights of digits being the Fibonacci numbers $u_1 = 1$, $u_2 = 1$, $u_3 = 2$, $u_4 = 3$, ... (rather than traditional 1, 2, 4, 8, 16, ...).

"10"∼1	"100"∼2	"1000"∼3	"10000"∼5
	"110"∼3	"1010"∼4	"10010"∼6
		"1100"∼5	"10100"∼7
		"1110"∼6	"10110"∼8
			"11000"∼8
			"11010"∼9
			"11100"∼10
			"11110"∼11

From Words to Numbers

(Second Numbering: Zeckendorf's words)

""$\sim$0	"1010"$\sim$4	"100000"$\sim$8	"101010"$\sim$12
"10"$\sim$1	"10000"$\sim$5	"100010"$\sim$9	"1000000"$\sim$13
"100"$\sim$2	"10010"$\sim$6	"100100"$\sim$10	"1000010"$\sim$14
"1000"$\sim$3	"10100"$\sim$7	"101000"$\sim$11	"1000100"$\sim$15

From Words to Numbers

(Second Numbering: Zeckendorf's words)

""∼0	"1010"∼4	"100000"∼8	"101010"∼12
"10"∼1	"10000"∼5	"100010"∼9	"1000000"∼13
"100"∼2	"10010"∼6	"100100"∼10	"1000010"∼14
"1000"∼3	"10100"∼7	"101000"∼11	"1000100"∼15

Zeckendorf's Theorem. Every positive integer x can be represented in the form

$$x = i_m u_m + i_{m-1} u_{m-1} + \cdots + i_1 u_1$$

with additional restrictions $i_m = 1$, $i_1 = 0$, $i_{k+1} i_k = 0$, and in unique way.

From Words to Numbers

(Second Numbering: Zeckendorf's words)

""∼0	"1010"∼4	"100000"∼8	"101010"∼12
"10"∼1	"10000"∼5	"100010"∼9	"1000000"∼13
"100"∼2	"10010"∼6	"100100"∼10	"1000010"∼14
"1000"∼3	"10100"∼7	"101000"∼11	"1000100"∼15

Zeckendorf's Theorem. Every positive integer x can be represented in the form

$$x = i_m u_m + i_{m-1} u_{m-1} + \cdots + i_1 u_1$$

with additional restrictions $i_m = 1$, $i_1 = 0$, $i_{k+1} i_k = 0$, and in unique way.

Zeckendorf's words: they do not begin with "0", do not end with "1", and do not contain "11".

From Words to Numbers

(Third Numbering: Infinite Alphabet)

Every word "$\alpha_{i_k}\alpha_{i_{k-1}}\dots\alpha_{i_1}$" in the infinite alphabet $A_\infty = \{\alpha_1, \alpha_2, \dots\}$ can be presented by the Zeckendorf word

$$"10^{i_k}10^{i_{k-1}}\dots10^{i_1}".$$

From Words to Numbers

(Third Numbering: Infinite Alphabet)

Every word "$\alpha_{i_k}\alpha_{i_{k-1}}\dots\alpha_{i_1}$" in the infinite alphabet $A_\infty = \{\alpha_1, \alpha_2, \dots\}$ can be presented by the Zeckendorf word

$$"10^{i_k}10^{i_{k-1}}\dots10^{i_1}".$$

We get, via Fibonacci numbers, a natural one-to-one correspondence between words in the infinite alphabet A_∞ and natural numbers.

From Words to Numbers

(Third Numbering: Infinite Alphabet)

Every word "$\alpha_{i_k}\alpha_{i_{k-1}}\dots\alpha_{i_1}$" in the infinite alphabet $A_\infty = \{\alpha_1, \alpha_2, \dots\}$ can be presented by the Zeckendorf word

$$"10^{i_k}10^{i_{k-1}}\dots10^{i_1}".$$

We get, via Fibonacci numbers, a natural one-to-one correspondence between words in the infinite alphabet A_∞ and natural numbers.

""∼0	"1010"∼4	"100000"∼8	"101010"∼12
"10"∼1	"10000"∼5	"100010"∼9	"1000000"∼13
"100"∼2	"10010"∼6	"100100"∼10	"1000010"∼14
"1000"∼3	"10100"∼7	"101000"∼11	"1000100"∼15

""∼0	"$\alpha_1\alpha_1$"∼4	"α_5"∼8	"$\alpha_1\alpha_1\alpha_1$"∼12
"α_1"∼1	"α_4"∼5	"$\alpha_3\alpha_1$"∼9	"α_6"∼13
"α_2"∼2	"$\alpha_2\alpha_1$"∼6	"$\alpha_2\alpha_2$"∼10	"$\alpha_4\alpha_1$"∼14
"α_3"∼3	"$\alpha_1\alpha_2$"∼7	"$\alpha_1\alpha_3$"∼11	"$\alpha_3\alpha_2$"∼15

From Words to Numbers
(Concatenation)

$$
\begin{array}{rcl@{\qquad\qquad}rcl}
X & = & "\beta_{i_m} \dots \beta_{i_1}" & Y & = & "\beta_{j_n} \dots \beta_{j_1}" \\
x & = & i_m u_m + \dots + i_1 u_1 & y & = & j_n u_n + \dots + j_1 u_1
\end{array}
$$

From Words to Numbers
(Concatenation)

$$\begin{array}{rclcrcl} X & = & "\beta_{i_m} \dots \beta_{i_1}" & & Y & = & "\beta_{j_n} \dots \beta_{j_1}" \\ x & = & i_m u_m + \dots + i_1 u_1 & & y & = & j_n u_n + \dots + j_1 u_1 \end{array}$$

$$Z = XY = "\beta_{i_m} \dots \beta_{i_1} \beta_{j_n} \dots \beta_{j_1}"$$

From Words to Numbers
(Concatenation)

$$\begin{array}{rclcrcl} X & = & "\beta_{i_m} \ldots \beta_{i_1}" & & Y & = & "\beta_{j_n} \ldots \beta_{j_1}" \\ x & = & i_m u_m + \cdots + i_1 u_1 & & y & = & j_n u_n + \cdots + j_1 u_1 \end{array}$$

$$Z = XY = "\beta_{i_m} \ldots \beta_{i_1} \beta_{j_n} \ldots \beta_{j_1}"$$

$$z \quad =$$

From Words to Numbers
(Concatenation)

$$\begin{array}{rcl} X & = & "\beta_{i_m} \ldots \beta_{i_1}" \\ x & = & i_m u_m + \cdots + i_1 u_1 \end{array} \qquad \begin{array}{rcl} Y & = & "\beta_{j_n} \ldots \beta_{j_1}" \\ y & = & j_n u_n + \cdots + j_1 u_1 \end{array}$$

$$Z = XY = "\beta_{i_m} \ldots \beta_{i_1} \beta_{j_n} \ldots \beta_{j_1}"$$

$$z = i_m u_{m+n} + \cdots + i_1 u_{1+n} + j_n u_n + \cdots + j_1 u_1$$

From Words to Numbers
(Concatenation)

$$u_{k+n} = u_k u_{n+1} + u_{k-1} u_n$$

$$\begin{array}{rclcrcl} X & = & "\beta_{i_m} \dots \beta_{i_1}" & & Y & = & "\beta_{j_n} \dots \beta_{j_1}" \\ x & = & i_m u_m + \dots + i_1 u_1 & & y & = & j_n u_n + \dots + j_1 u_1 \end{array}$$

$$Z = XY = "\beta_{i_m} \dots \beta_{i_1} \beta_{j_n} \dots \beta_{j_1}"$$

$$z = i_m u_{m+n} + \dots + i_1 u_{1+n} + j_n u_n + \dots + j_1 u_1$$

From Words to Numbers
(Concatenation)

$$\boxed{u_{k+n} = u_k u_{n+1} + u_{k-1} u_n}$$

$$\begin{array}{rclcrcl} X & = & "\beta_{i_m} \dots \beta_{i_1}" & & Y & = & "\beta_{j_n} \dots \beta_{j_1}" \\ x & = & i_m u_m + \dots + i_1 u_1 & & y & = & j_n u_n + \dots + j_1 u_1 \end{array}$$

$$Z = XY = "\beta_{i_m} \dots \beta_{i_1} \beta_{j_n} \dots \beta_{j_1}"$$

$$\begin{aligned} z &= i_m u_{m+n} + \dots + i_1 u_{1+n} + j_n u_n + \dots + j_1 u_1 \\ &= i_m(u_m u_{n+1} + u_{m-1} u_n) + \dots + i_1(u_1 u_{n+1} + u_0 u_n) + y \end{aligned}$$

From Words to Numbers
(Concatenation)

$$\boxed{u_{k+n} = u_k u_{n+1} + u_{k-1} u_n}$$

$$\begin{array}{rclcrcl} X & = & "\beta_{i_m} \dots \beta_{i_1}" & & Y & = & "\beta_{j_n} \dots \beta_{j_1}" \\ x & = & i_m u_m + \dots + i_1 u_1 & & y & = & j_n u_n + \dots + j_1 u_1 \end{array}$$

$$Z = XY = "\beta_{i_m} \dots \beta_{i_1} \beta_{j_n} \dots \beta_{j_1}"$$

$$\begin{aligned} z &= i_m u_{m+n} + \dots + i_1 u_{1+n} + j_n u_n + \dots + j_1 u_1 \\ &= i_m(u_m u_{n+1} + u_{m-1} u_n) + \dots + i_1(u_1 u_{n+1} + u_0 u_n) + y \\ &= (i_m u_m + \dots + i_1 u_1) u_{n+1} + (i_m u_{m-1} + \dots + i_1 u_0) u_n + y \end{aligned}$$

From Words to Numbers
(Concatenation)

$$\boxed{u_{k+n} = u_k u_{n+1} + u_{k-1} u_n}$$

$$\begin{array}{rclcrcl} X & = & "\beta_{i_m} \dots \beta_{i_1}" & & Y & = & "\beta_{j_n} \dots \beta_{j_1}" \\ x & = & i_m u_m + \dots + i_1 u_1 & & y & = & j_n u_n + \dots + j_1 u_1 \end{array}$$

$$Z = XY = "\beta_{i_m} \dots \beta_{i_1} \beta_{j_n} \dots \beta_{j_1}"$$

$$\begin{aligned} z &= i_m u_{m+n} + \dots + i_1 u_{1+n} + j_n u_n + \dots + j_1 u_1 \\ &= i_m(u_m u_{n+1} + u_{m-1} u_n) + \dots + i_1(u_1 u_{n+1} + u_0 u_n) + y \\ &= \underbrace{(i_m u_m + \dots + i_1 u_1)}_{x} u_{n+1} + (i_m u_{m-1} + \dots + i_1 u_0) u_n + y \end{aligned}$$

From Words to Numbers
(Concatenation)

$$\boxed{u_{k+n} = u_k u_{n+1} + u_{k-1} u_n}$$

$$\begin{array}{rclcrcl} X & = & "\beta_{i_m} \dots \beta_{i_1}" & & Y & = & "\beta_{j_n} \dots \beta_{j_1}" \\ x & = & i_m u_m + \dots + i_1 u_1 & & y & = & j_n u_n + \dots + j_1 u_1 \end{array}$$

$$Z = XY = "\beta_{i_m} \dots \beta_{i_1} \beta_{j_n} \dots \beta_{j_1}"$$

$$\begin{aligned} z &= i_m u_{m+n} + \dots + i_1 u_{1+n} + j_n u_n + \dots + j_1 u_1 \\ &= i_m(u_m u_{n+1} + u_{m-1} u_n) + \dots + i_1(u_1 u_{n+1} + u_0 u_n) + y \\ &= \underbrace{(i_m u_m + \dots + i_1 u_1)}_{x} u_{n+1} + \underbrace{(i_m u_{m-1} + \dots + i_1 u_0)}_{x_1} u_n + y \end{aligned}$$

From Words to Numbers
(Concatenation)

$$\boxed{u_{k+n} = u_k u_{n+1} + u_{k-1} u_n}$$

$$\begin{array}{rclcrcl} X & = & "\beta_{i_m} \dots \beta_{i_1}" & & Y & = & "\beta_{j_n} \dots \beta_{j_1}" \\ x & = & i_m u_m + \dots + i_1 u_1 & & y & = & j_n u_n + \dots + j_1 u_1 \end{array}$$

$$Z = XY = "\beta_{i_m} \dots \beta_{i_1} \beta_{j_n} \dots \beta_{j_1}"$$

$$\begin{aligned} z &= i_m u_{m+n} + \dots + i_1 u_{1+n} + j_n u_n + \dots + j_1 u_1 \\ &= i_m(u_m u_{n+1} + u_{m-1} u_n) + \dots + i_1(u_1 u_{n+1} + u_0 u_n) + y \\ &= \underbrace{(i_m u_m + \dots + i_1 u_1)}_{x} u_{n+1} + \underbrace{(i_m u_{m-1} + \dots + i_1 u_0)}_{x_1} u_n + y \\ &= x y_3 + x_1 y_2 + y \end{aligned}$$

where

$$y_2 = u_n, \quad y_3 = u_{n+1}$$

From Words to Numbers
(Concatenation cont.)

$$
\begin{array}{rcc@{\qquad}rcc}
X & = & "\beta_{i_m} \dots \beta_{i_1}" & Y & = & "\beta_{j_n} \dots \beta_{j_1}" \\
x & = & i_m u_m + \dots + i_1 u_1 & y & = & j_n u_n + \dots + j_1 u_1 \\
x_1 & = & i_m u_{m-1} + \dots + i_1 u_0 & y_1 & = & j_n u_{n-1} + \dots + j_1 u_0 \\
x_2 & = & u_m & y_2 & = & u_n \\
x_3 & = & u_{m+1} & y_3 & = & u_{n+1}
\end{array}
$$

From Words to Numbers
(Concatenation cont.)

$$
\begin{array}{rcc@{\qquad\qquad}rcc}
X & = & "\beta_{i_m} \dots \beta_{i_1}" & Y & = & "\beta_{j_n} \dots \beta_{j_1}" \\
x & = & i_m u_m + \dots + i_1 u_1 & y & = & j_n u_n + \dots + j_1 u_1 \\
x_1 & = & i_m u_{m-1} + \dots + i_1 u_0 & y_1 & = & j_n u_{n-1} + \dots + j_1 u_0 \\
x_2 & = & u_m & y_2 & = & u_n \\
x_3 & = & u_{m+1} & y_3 & = & u_{n+1}
\end{array}
$$

$$
Z = XY \quad = \quad "\beta_{i_m} \dots \beta_{i_1} \beta_{j_n} \dots \beta_{j_1}"
$$

From Words to Numbers
(Concatenation cont.)

$$
\begin{array}{rcc@{\qquad\qquad}rcc}
X & = & "\beta_{i_m} \dots \beta_{i_1}" & Y & = & "\beta_{j_n} \dots \beta_{j_1}" \\
x & = & i_m u_m + \dots + i_1 u_1 & y & = & j_n u_n + \dots + j_1 u_1 \\
x_1 & = & i_m u_{m-1} + \dots + i_1 u_0 & y_1 & = & j_n u_{n-1} + \dots + j_1 u_0 \\
x_2 & = & u_m & y_2 & = & u_n \\
x_3 & = & u_{m+1} & y_3 & = & u_{n+1}
\end{array}
$$

$$
\begin{aligned}
Z = XY &= "\beta_{i_m} \dots \beta_{i_1} \beta_{j_n} \dots \beta_{j_1}" \\
z &= x_1 y_2 + x y_3 + y
\end{aligned}
$$

From Words to Numbers
(Concatenation cont.)

$$
\begin{array}{rcc@{\qquad\qquad}rcc}
X & = & "\beta_{i_m} \dots \beta_{i_1}" & Y & = & "\beta_{j_n} \dots \beta_{j_1}" \\
x & = & i_m u_m + \dots + i_1 u_1 & y & = & j_n u_n + \dots + j_1 u_1 \\
x_1 & = & i_m u_{m-1} + \dots + i_1 u_0 & y_1 & = & j_n u_{n-1} + \dots + j_1 u_0 \\
x_2 & = & u_m & y_2 & = & u_n \\
x_3 & = & u_{m+1} & y_3 & = & u_{n+1}
\end{array}
$$

$$
\begin{aligned}
Z = XY &= "\beta_{i_m} \dots \beta_{i_1} \beta_{j_n} \dots \beta_{j_1}" \\
z &= x_1 y_2 + x y_3 + y \\
z_1 &= x_1 (y_3 - y_2) + x y_2 + y_1
\end{aligned}
$$

From Words to Numbers
(Concatenation cont.)

$$
\begin{array}{rcc@{\qquad}rcc}
X & = & "\beta_{i_m} \dots \beta_{i_1}" & Y & = & "\beta_{j_n} \dots \beta_{j_1}" \\
x & = & i_m u_m + \dots + i_1 u_1 & y & = & j_n u_n + \dots + j_1 u_1 \\
x_1 & = & i_m u_{m-1} + \dots + i_1 u_0 & y_1 & = & j_n u_{n-1} + \dots + j_1 u_0 \\
x_2 & = & u_m & y_2 & = & u_n \\
x_3 & = & u_{m+1} & y_3 & = & u_{n+1}
\end{array}
$$

$$
\begin{aligned}
Z = XY &= "\beta_{i_m} \dots \beta_{i_1} \beta_{j_n} \dots \beta_{j_1}" \\
z &= x_1 y_2 + x y_3 + y \\
z_1 &= x_1 (y_3 - y_2) + x y_2 + y_1 \\
z_2 &= (x_3 - x_2) y_2 + x_2 y_3
\end{aligned}
$$

From Words to Numbers
(Concatenation cont.)

$$
\begin{array}{rcc@{\qquad}rcc}
X & = & "\beta_{i_m} \dots \beta_{i_1}" & Y & = & "\beta_{j_n} \dots \beta_{j_1}" \\
x & = & i_m u_m + \dots + i_1 u_1 & y & = & j_n u_n + \dots + j_1 u_1 \\
x_1 & = & i_m u_{m-1} + \dots + i_1 u_0 & y_1 & = & j_n u_{n-1} + \dots + j_1 u_0 \\
x_2 & = & u_m & y_2 & = & u_n \\
x_3 & = & u_{m+1} & y_3 & = & u_{n+1}
\end{array}
$$

$$
\begin{aligned}
Z = XY &= "\beta_{i_m} \dots \beta_{i_1} \beta_{j_n} \dots \beta_{j_1}" \\
z &= x_1 y_2 + x y_3 + y \\
z_1 &= x_1 (y_3 - y_2) + x y_2 + y_1 \\
z_2 &= (x_3 - x_2) y_2 + x_2 y_3 \\
z_3 &= x_2 y_2 + x_3 y_3
\end{aligned}
$$

Fibonacci Numbers and Diophantine Equations

Theorem (G. D. Cassini [1680]).

$$u_{m+1}^2 - u_{m+1}u_m - u_m^2 = (-1)^m$$

Fibonacci Numbers and Diophantine Equations

Theorem (G. D. Cassini [1680]).

$$u_{m+1}^2 - u_{m+1}u_m - u_m^2 = (-1)^m$$

Theorem (M. J. Wasteels [1902]). If

$$w^2 - wv - v^2 = \pm 1$$

then

$$w = u_{m+1}, \quad v = u_m$$

for some m.

From Words to Numbers

(Second Numbering cont.)

$$
\begin{aligned}
X &= \text{``}\beta_{i_m} \dots \beta_{i_1}\text{''} \\
x &= i_m u_m + \dots + i_1 u_1 \\
x_1 &= i_m u_{m-1} + \dots + i_1 u_0 \\
x_2 &= u_m \\
x_3 &= u_{m+1}
\end{aligned}
$$

From Words to Numbers

(Second Numbering cont.)

$$
\begin{array}{rcc}
X & = & "\beta_{i_m} \ldots \beta_{i_1}" \\
x & = & i_m u_m + \cdots + i_1 u_1 \\
x_1 & = & i_m u_{m-1} + \cdots + i_1 u_0 \\
x_2 & = & u_m \\
x_3 & = & u_{m+1}
\end{array}
$$

$$(x_3^2 - x_3 x_2 - x_2^2)^2 = 1$$

From Words to Numbers

(Second Numbering cont.)

$$
\begin{array}{rcc}
X & = & "\beta_{i_m} \ldots \beta_{i_1}" \\
x & = & i_m u_m + \cdots + i_1 u_1 \\
x_1 & = & i_m u_{m-1} + \cdots + i_1 u_0 \\
x_2 & = & u_m \\
x_3 & = & u_{m+1}
\end{array}
$$

$$(x_3^2 - x_3 x_2 - x_2^2)^2 = 1$$

$$x_2 \leq x < x_3$$

From Words to Numbers
(Second Numbering cont.)

$$\frac{u_k}{u_{k-1}} \approx \phi = \frac{1+\sqrt{5}}{2}$$

$$\begin{aligned} X &= \text{"}\beta_{i_m} \dots \beta_{i_1}\text{"} \\ x &= i_m u_m + \cdots + i_1 u_1 \\ x_1 &= i_m u_{m-1} + \cdots + i_1 u_0 \\ x_2 &= u_m \\ x_3 &= u_{m+1} \end{aligned}$$

$$(x_3^2 - x_3 x_2 - x_2^2)^2 = 1$$

$$x_2 \leq x < x_3$$

From Words to Numbers
(Second Numbering cont.)

$$\frac{u_k}{u_{k-1}} \approx \phi = \frac{1+\sqrt{5}}{2}$$

$$\begin{aligned} X &= \text{"}\beta_{i_m} \dots \beta_{i_1}\text{"} \\ x &= i_m u_m + \cdots + i_1 u_1 \\ x_1 &= i_m u_{m-1} + \cdots + i_1 u_0 \\ x_2 &= u_m \\ x_3 &= u_{m+1} \end{aligned}$$

$$(x_3^2 - x_3 x_2 - x_2^2)^2 = 1$$

$$x_2 \leq x < x_3$$

$\frac{x}{x_1} \approx \phi$

From Words to Numbers
(Second Numbering cont.)

$$\frac{u_k}{u_{k-1}} \approx \phi = \frac{1+\sqrt{5}}{2}$$

$$\begin{aligned} X &= \text{"}\beta_{i_m} \dots \beta_{i_1}\text{"} \\ x &= i_m u_m + \cdots + i_1 u_1 \\ x_1 &= i_m u_{m-1} + \cdots + i_1 u_0 \\ x_2 &= u_m \\ x_3 &= u_{m+1} \end{aligned}$$

$$(x_3^2 - x_3 x_2 - x_2^2)^2 = 1$$

$$x_2 \le x < x_3$$

$\frac{x}{x_1} \approx \phi$ $\qquad$ $\phi - 2 < x_1 - x/\phi < \phi - 1$

From Words to Numbers

(Length of words)

$$
\begin{array}{rcc|rcc}
X & = & "\beta_{i_m} \dots \beta_{i_1}" & Y & = & "\beta_{j_n} \dots \beta_{j_1}" \\
x & = & i_m u_m + \dots + i_1 u_1 & y & = & j_n u_n + \dots + j_1 u_1 \\
x_1 & = & i_m u_{m-1} + \dots + i_1 u_0 & y_1 & = & j_n u_{n-1} + \dots + j_1 u_0 \\
x_2 & = & u_m & y_2 & = & u_n \\
x_3 & = & u_{m+1} & y_3 & = & u_{n+1}
\end{array}
$$

From Words to Numbers

(Length of words)

$$
\begin{array}{rcc@{\qquad}rcc}
X & = & "\beta_{i_m} \dots \beta_{i_1}" & Y & = & "\beta_{j_n} \dots \beta_{j_1}" \\
x & = & i_m u_m + \dots + i_1 u_1 & y & = & j_n u_n + \dots + j_1 u_1 \\
x_1 & = & i_m u_{m-1} + \dots + i_1 u_0 & y_1 & = & j_n u_{n-1} + \dots + j_1 u_0 \\
x_2 & = & u_m & y_2 & = & u_n \\
x_3 & = & u_{m+1} & y_3 & = & u_{n+1}
\end{array}
$$

$$\text{length}(X) = \text{length}(Y) \quad \Leftrightarrow \quad x_2 = y_2$$

From Words to Numbers

(Length of words)

$$\boxed{\mathrm{GCD}(u_m, u_n) = u_{\mathrm{GCD}(m,n)}}$$

$$\begin{array}{rcc|rcc} X & = & "\beta_{i_m} \dots \beta_{i_1}" & Y & = & "\beta_{j_n} \dots \beta_{j_1}" \\ x & = & i_m u_m + \dots + i_1 u_1 & y & = & j_n u_n + \dots + j_1 u_1 \\ x_1 & = & i_m u_{m-1} + \dots + i_1 u_0 & y_1 & = & j_n u_{n-1} + \dots + j_1 u_0 \\ x_2 & = & u_m & y_2 & = & u_n \\ x_3 & = & u_{m+1} & y_3 & = & u_{n+1} \end{array}$$

$$\mathrm{length}(X) = \mathrm{length}(Y) \quad \Leftrightarrow \quad x_2 = y_2$$

From Words to Numbers

(Length of words)

$$\boxed{\mathrm{GCD}(u_m, u_n) = u_{\mathrm{GCD}(m,n)}}$$

$$\begin{array}{rcc|rcc}
X & = & "\beta_{i_m} \dots \beta_{i_1}" & Y & = & "\beta_{j_n} \dots \beta_{j_1}" \\
x & = & i_m u_m + \dots + i_1 u_1 & y & = & j_n u_n + \dots + j_1 u_1 \\
x_1 & = & i_m u_{m-1} + \dots + i_1 u_0 & y_1 & = & j_n u_{n-1} + \dots + j_1 u_0 \\
x_2 & = & u_m & y_2 & = & u_n \\
x_3 & = & u_{m+1} & y_3 & = & u_{n+1}
\end{array}$$

$$\begin{aligned}
\mathrm{length}(X) = \mathrm{length}(Y) &\Leftrightarrow x_2 = y_2 \\
\mathrm{length}(X) \,\big|\, \mathrm{length}(Y) &\Leftrightarrow x_2(2x_3 - x_3) \,\big|\, y_2(2y_3 - y_2)
\end{aligned}$$

From Words to Numbers

(Length of words)

$$\boxed{\mathrm{GCD}(u_m, u_n) = u_{\mathrm{GCD}(m,n)}}$$

$$\begin{array}{rcc|rcc} X & = & "\beta_{i_m} \dots \beta_{i_1}" & Y & = & "\beta_{j_n} \dots \beta_{j_1}" \\ x & = & i_m u_m + \dots + i_1 u_1 & y & = & j_n u_n + \dots + j_1 u_1 \\ x_1 & = & i_m u_{m-1} + \dots + i_1 u_0 & y_1 & = & j_n u_{n-1} + \dots + j_1 u_0 \\ x_2 & = & u_m & y_2 & = & u_n \\ x_3 & = & u_{m+1} & y_3 & = & u_{n+1} \end{array}$$

$$\begin{aligned} \mathrm{length}(X) = \mathrm{length}(Y) &\Leftrightarrow x_2 = y_2 \\ \mathrm{length}(X) \,\big|\, \mathrm{length}(Y) &\Leftrightarrow x_2(2x_3 - x_3) \,\big|\, y_2(2y_3 - y_2) \\ \mathrm{GCD}(\mathrm{length}(X), \mathrm{length}(Y)) = 1 &\Leftrightarrow z_1 x_2(2x_3 - x_2) - \\ & \qquad z_2 y_2(2y_3 - y_2) = 1 \end{aligned}$$

From Words to Numbers
(Length of words)

$$\boxed{\mathrm{GCD}(u_m, u_n) = u_{\mathrm{GCD}(m,n)}}$$

$$\begin{array}{rcc|rcc} X & = & "\beta_{i_m} \dots \beta_{i_1}" & Y & = & "\beta_{j_n} \dots \beta_{j_1}" \\ x & = & i_m u_m + \dots + i_1 u_1 & y & = & j_n u_n + \dots + j_1 u_1 \\ x_1 & = & i_m u_{m-1} + \dots + i_1 u_0 & y_1 & = & j_n u_{n-1} + \dots + j_1 u_0 \\ x_2 & = & u_m & y_2 & = & u_n \\ x_3 & = & u_{m+1} & y_3 & = & u_{n+1} \end{array}$$

$$\begin{aligned} \mathrm{length}(X) = \mathrm{length}(Y) &\Leftrightarrow x_2 = y_2 \\ \mathrm{length}(X) \,\big|\, \mathrm{length}(Y) &\Leftrightarrow x_2(2x_3 - x_3) \,\big|\, y_2(2y_3 - y_2) \\ \mathrm{GCD}(\mathrm{length}(X), \mathrm{length}(Y)) = 1 &\Leftrightarrow z_1 x_2(2x_3 - x_2) - \\ &\qquad z_2 y_2(2y_3 - y_2) = 1 \end{aligned}$$

Open Problem. Is there an algorithm for deciding whether a system of word equations with additional restrictions on the lengths of the above types has a solution?

From Words to Numbers

(Length of words cont.)

$$"\alpha_{i_k}\alpha_{i_{k-1}}\ldots\alpha_{i_1}"$$

From Words to Numbers

(Length of words cont.)

$$"\alpha_{i_k}\alpha_{i_{k-1}}\ldots\alpha_{i_1}"$$

$$"10^{i_k}10^{i_{k-1}}\ldots10^{i_1}"$$

From Words to Numbers

(Length of words cont.)

$$"\alpha_{i_k}\alpha_{i_{k-1}}\ldots\alpha_{i_1}"$$

$$"10^{i_k}10^{i_{k-1}}\ldots10^{i_1}"$$

$$\text{length}("10^{i_k}10^{i_{k-1}}\ldots10^{i_1}") =$$

From Words to Numbers

(Length of words cont.)

$$"\alpha_{i_k}\alpha_{i_{k-1}}\ldots\alpha_{i_1}"$$

$$"10^{i_k}10^{i_{k-1}}\ldots10^{i_1}"$$

$$\text{length}("10^{i_k}10^{i_{k-1}}\ldots10^{i_1}") = k$$

From Words to Numbers

(Length of words cont.)

$$"\alpha_{i_k}\alpha_{i_{k-1}}\ldots\alpha_{i_1}"$$

$$"10^{i_k}10^{i_{k-1}}\ldots10^{i_1}"$$

$$\text{length}("10^{i_k}10^{i_{k-1}}\ldots10^{i_1}") = k + i_k + i_{k-1} + \cdots + i_1$$

From Words to Numbers

(Fourth Numbering)

$$X \quad = \quad "\beta_{i_m}\beta_{i_{m-1}}\ldots\beta_{i_1}"$$

From Words to Numbers

(Fourth Numbering)

$$\text{"1"} \mapsto \text{"10"}, \ \text{"0"} \mapsto \text{"00"}$$

$$X \quad = \quad \text{"}\beta_{i_m}\beta_{i_{m-1}}\ldots\beta_{i_1}\text{"}$$

From Words to Numbers

"1" $\mapsto$ "10", "0" $\mapsto$ "00"

(Fourth Numbering)

$$
\begin{aligned}
X \quad = \quad & "\beta_{i_m}\beta_{i_{m-1}}\ldots\beta_{i_1}" \\
& "\beta_{i_m}0\beta_{i_{m-1}}0\ldots\beta_{i_1}0"
\end{aligned}
$$

From Words to Numbers

(Fourth Numbering)

$$\text{"}1\text{"} \mapsto \text{"}10\text{"},\ \text{"}0\text{"} \mapsto \text{"}00\text{"}$$

$$\begin{aligned} X &= \text{"}\beta_{i_m}\beta_{i_{m-1}}\ldots\beta_{i_1}\text{"} \\ &\quad\ \text{"}\beta_{i_m}0\beta_{i_{m-1}}0\ldots\beta_{i_1}0\text{"} \\ x &= i_m u_{2m} + i_{m-1}u_{2(m-1)} + \cdots + i_1 u_2 \end{aligned}$$

From Words to Numbers

(Fourth Numbering)

$$\text{"1"} \mapsto \text{"10"}, \quad \text{"0"} \mapsto \text{"00"}$$

$$\begin{aligned} X &= \text{"}\beta_{i_m}\beta_{i_{m-1}}\ldots\beta_{i_1}\text{"} \\ &\quad\ \text{"}\beta_{i_m}0\beta_{i_{m-1}}0\ldots\beta_{i_1}0\text{"} \\ x &= i_m u_{2m} + i_{m-1}u_{2(m-1)} + \cdots + i_1 u_2 \\ x_1 &= i_m u_{2m-1} + i_{m-1}u_{2(m-1)-1} + \cdots + i_1 u_1 \end{aligned}$$

From Words to Numbers

(Fourth Numbering)

$$\text{"1"} \mapsto \text{"10"}, \quad \text{"0"} \mapsto \text{"00"}$$

$$\begin{aligned}
X &= \text{"}\beta_{i_m}\beta_{i_{m-1}}\ldots\beta_{i_1}\text{"} \\
&\quad\ \text{"}\beta_{i_m}0\beta_{i_{m-1}}0\ldots\beta_{i_1}0\text{"} \\
x &= i_m u_{2m} + i_{m-1} u_{2(m-1)} + \cdots + i_1 u_2 \\
x_1 &= i_m u_{2m-1} + i_{m-1} u_{2(m-1)-1} + \cdots + i_1 u_1 \\
x_2 &= u_{2m} \\
x_3 &= u_{2m+1}
\end{aligned}$$

From Words to Numbers

(Fourth Numbering)

$$\boxed{\text{"1"} \mapsto \text{"10"},\ \text{"0"} \mapsto \text{"00"}}$$

$$\begin{aligned}
X &= \text{"}\beta_{i_m}\beta_{i_{m-1}}\ldots\beta_{i_1}\text{"} \\
&\quad\ \text{"}\beta_{i_m}0\beta_{i_{m-1}}0\ldots\beta_{i_1}0\text{"} \\
x &= i_m u_{2m} + i_{m-1} u_{2(m-1)} + \cdots + i_1 u_2 \\
x_1 &= i_m u_{2m-1} + i_{m-1} u_{2(m-1)-1} + \cdots + i_1 u_1 \\
x_2 &= u_{2m} \\
x_3 &= u_{2m+1}
\end{aligned}$$

$$x_3^2 - x_3 x_2 - x_2^2 = 1$$

From Words to Numbers

(Fourth Numbering)

$$\boxed{\text{"1"} \mapsto \text{"10"},\ \text{"0"} \mapsto \text{"00"}}$$

$$\begin{aligned}
X &= \text{"}\beta_{i_m}\beta_{i_{m-1}}\ldots\beta_{i_1}\text{"} \\
&\quad\ \text{"}\beta_{i_m}0\beta_{i_{m-1}}0\ldots\beta_{i_1}0\text{"} \\
x &= i_m u_{2m} + i_{m-1}u_{2(m-1)} + \cdots + i_1 u_2 \\
x_1 &= i_m u_{2m-1} + i_{m-1}u_{2(m-1)-1} + \cdots + i_1 u_1 \\
x_2 &= u_{2m} \\
x_3 &= u_{2m+1}
\end{aligned}$$

$$x_3^2 - x_3x_2 - x_2^2 = 1$$

$$x < x_3$$

From Words to Numbers

(Fourth Numbering)

$$\text{"}1\text{"} \mapsto \text{"}10\text{"},\ \text{"}0\text{"} \mapsto \text{"}00\text{"}$$

$$\begin{aligned} X &= \text{"}\beta_{i_m}\beta_{i_{m-1}}\ldots\beta_{i_1}\text{"} \\ &\quad\ \text{"}\beta_{i_m}0\beta_{i_{m-1}}0\ldots\beta_{i_1}0\text{"} \\ x &= i_m u_{2m} + i_{m-1}u_{2(m-1)} + \cdots + i_1 u_2 \\ x_1 &= i_m u_{2m-1} + i_{m-1}u_{2(m-1)-1} + \cdots + i_1 u_1 \\ x_2 &= u_{2m} \\ x_3 &= u_{2m+1} \end{aligned}$$

$$x_3^2 - x_3x_2 - x_2^2 = 1$$

$$x < x_3$$

$$\phi - 2 < x_1 - x/\phi < \phi - 1$$

$$\text{"}10\text{"} \mapsto \text{"}1\text{"},\ \text{"}00\text{"} \mapsto \text{"}0\text{"},\ \text{"}01\text{"} \mapsto \text{"}1\text{"}$$

From Words to Numbers

(Fourth Numbering)

$$\text{"}1\text{"} \mapsto \text{"}10\text{"},\ \text{"}0\text{"} \mapsto \text{"}00\text{"}$$

$$\begin{aligned} X &= \text{"}\beta_{i_m}\beta_{i_{m-1}}\ldots\beta_{i_1}\text{"} \\ &\quad\ \text{"}\beta_{i_m}0\beta_{i_{m-1}}0\ldots\beta_{i_1}0\text{"} \\ x &= i_m u_{2m} + i_{m-1}u_{2(m-1)} + \cdots + i_1 u_2 \\ x_1 &= i_m u_{2m-1} + i_{m-1}u_{2(m-1)-1} + \cdots + i_1 u_1 \\ x_2 &= u_{2m} \\ x_3 &= u_{2m+1} \end{aligned}$$

$$x_3^2 - x_3x_2 - x_2^2 = 1$$

$$x < x_3$$

$$\phi - 2 < x_1 - x/\phi < \phi - 1$$

$$\text{"}10\text{"} \mapsto \text{"}1\text{"},\ \text{"}00\text{"} \mapsto \text{"}0\text{"},\ \text{"}01\text{"} \mapsto \text{"}1\text{"}$$

From Words to Numbers

(Fourth Numbering)

$$\text{"1"} \mapsto \text{"10"},\ \text{"0"} \mapsto \text{"00"}$$

$$\begin{aligned} X &= \text{"}\beta_{i_m}\beta_{i_{m-1}}\ldots\beta_{i_1}\text{"} \\ &\quad\ \text{"}\beta_{i_m}0\beta_{i_{m-1}}0\ldots\beta_{i_1}0\text{"} \\ x &= i_m u_{2m} + i_{m-1}u_{2(m-1)} + \cdots + i_1 u_2 \\ x_1 &= i_m u_{2m-1} + i_{m-1}u_{2(m-1)-1} + \cdots + i_1 u_1 \\ x_2 &= u_{2m} \\ x_3 &= u_{2m+1} \end{aligned}$$

$$x_3^2 - x_3x_2 - x_2^2 = 1$$

$$x < x_3$$

$$\phi - 2 < x_1 - x/\phi < \phi - 1$$

$$\text{"10"} \mapsto \text{"1"},\ \text{"00"} \mapsto \text{"0"},\ \text{"01"} \mapsto \text{"1"}$$

Open Problem. Is there an algorithm for deciding whether a system of word equations with additional restrictions on the lengths of words has a solution?

Another Reduction of Word Equations

Matiyasevich Yu. V. The connection between Hilbert's Tenth Problem and systems of equations between words and lengths (in Russian). *Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta im. V. A. Steklova AN SSSR*, 8, 132–144, 1968; translated in *Seminars in Mathematics, V. A. Steklov Mathematical Institute*, 8, 61–67, 1970.

Another Reduction of Word Equations

Matiyasevich Yu. V. The connection between Hilbert's Tenth Problem and systems of equations between words and lengths (in Russian). *Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta im. V. A. Steklova AN SSSR*, 8, 132–144, 1968; translated in *Seminars in Mathematics, V. A. Steklov Mathematical Institute*, 8, 61–67, 1970.

Matiyasevich Yu. Word Equations, Fibonacci Numbers, and Hilbert's Tenth Problem
http://logic.pdmi.ras.ru/ yumat/talks/turku2006/turku2006.html

One Step More

J. Robinson. Unsolvable Diophantine problems. *Proceedings of the American Mathematical Society*, 22(2), 534–538, 1969.

One Step More

J. Robinson. Unsolvable Diophantine problems. *Proceedings of the American Mathematical Society*, 22(2), 534–538, 1969.

Реферативный журнал Математика

Russian counterpart to

- *Zentralblatt für Mathematik*
- *Mathematical Reviews*

Pell's equation

New idea of Julia Robinson

$$x^2 - (a^2 - 1)y^2 = 1$$

Pell's equation

New idea of Julia Robinson

$$x^2 - (a^2 - 1)y^2 = 1$$

$$x_0 = 1, y_0 = 0, \quad x_1 = a, y_1 = 1$$

Pell's equation

New idea of Julia Robinson

$$x^2 - (a^2 - 1)y^2 = 1$$

$$x_0 = 1, y_0 = 0, \quad x_1 = a, y_1 = 1$$

$$x_{n+1} = 2ax_n - x_{n-1}, \quad y_{n+1} = 2ay_n - y_{n-1}$$

Pell's equation

New idea of Julia Robinson

$$x^2 - (a^2 - 1)y^2 = 1$$

$$x_0 = 1, y_0 = 0, \quad x_1 = a, y_1 = 1$$

$$x_{n+1} = 2ax_n - x_{n-1}, \quad y_{n+1} = 2ay_n - y_{n-1}$$

$$y_0, y_1, \ldots, y_n, \cdots \equiv 0, 1, \ldots, n, \ldots \pmod{a-1} \qquad (*)$$

Pell's equation

New idea of Julia Robinson

$$x^2 - (a^2 - 1)y^2 = 1$$

$$x_0 = 1, y_0 = 0, \quad x_1 = a, y_1 = 1$$

$$x_{n+1} = 2ax_n - x_{n-1}, \quad y_{n+1} = 2ay_n - y_{n-1}$$

$$y_0, y_1, \ldots, y_n, \cdots \equiv 0, 1, \ldots, n, \ldots \pmod{a-1} \qquad (*)$$

$$x_0 - (a-2)y_0, \ldots, x_n - (a-2)y_n, \cdots \equiv 2^0, \ldots, 2^n, \ldots \pmod{4a-5} \quad (**)$$

Pell's equation

New idea of Julia Robinson

$$x^2 - (a^2 - 1)y^2 = 1$$

$$x_0 = 1, y_0 = 0, \quad x_1 = a, y_1 = 1$$

$$x_{n+1} = 2ax_n - x_{n-1}, \quad y_{n+1} = 2ay_n - y_{n-1}$$

$$y_0, y_1, \ldots, y_n, \cdots \equiv 0, 1, \ldots, n, \ldots \pmod{a-1} \qquad (*)$$

$$x_0 - (a-2)y_0, \ldots, x_n - (a-2)y_n, \cdots \equiv 2^0, \ldots, 2^n, \ldots \pmod{4a-5} \quad (**)$$

New idea of Julia Robinson: *Impose some condition $J(a)$ which would imply that the period of the sequence $(*)$ is a multiple of the period of the sequence $(**)$*

Fibonacci Numbers

Rabbits Strike Again

$$0, 1, 1, 2, 3, 5, 8, \ldots, f_{n+1} = f_n + f_{n-1}, \ldots$$

Fibonacci Numbers

Rabbits Strike Again

$$0, 1, 1, 2, 3, 5, 8, \ldots, f_{n+1} = f_n + f_{n-1}, \ldots$$

$$f^2 - fg - g^2 = \pm 1$$

Fibonacci Numbers

Rabbits Strike Again

$$0, 1, 1, 2, 3, 5, 8, \ldots, f_{n+1} = f_n + f_{n-1}, \ldots$$

$$f^2 - fg - g^2 = \pm 1$$

$$f_{2(n+1)} = 3f_{2n} - f_{2(n-1)}$$

Fibonacci Numbers

Rabbits Strike Again

$$0, 1, 1, 2, 3, 5, 8, \ldots, f_{n+1} = f_n + f_{n-1}, \ldots$$

$$f^2 - fg - g^2 = \pm 1$$

$$f_{2(n+1)} = 3f_{2n} - f_{2(n-1)}$$

$$y_0, y_1, \ldots, y_n, \cdots \equiv 0, 1, ..., n, \ldots \pmod{a-1} \qquad (*)$$

Fibonacci Numbers

Rabbits Strike Again

$$0, 1, 1, 2, 3, 5, 8, \ldots, f_{n+1} = f_n + f_{n-1}, \ldots$$

$$f^2 - fg - g^2 = \pm 1$$

$$f_{2(n+1)} = 3f_{2n} - f_{2(n-1)}$$

$$y_0, y_1, \ldots, y_n, \cdots \equiv 0, 1, ..., n, \ldots \pmod{a-1} \qquad (*)$$

$$y_0, y_1, \ldots, y_n, \cdots \equiv f_0, f_2, \ldots, f_{2n}, \ldots \pmod{a-3} \qquad (**)$$

Fibonacci Numbers

Rabbits Strike Again

$$0, 1, 1, 2, 3, 5, 8, \ldots, f_{n+1} = f_n + f_{n-1}, \ldots$$

$$f^2 - fg - g^2 = \pm 1$$

$$f_{2(n+1)} = 3f_{2n} - f_{2(n-1)}$$

$$y_0, y_1, \ldots, y_n, \cdots \equiv 0, 1, ..., n, \ldots \pmod{a-1} \qquad (*)$$

$$y_0, y_1, \ldots, y_n, \cdots \equiv f_0, f_2, \ldots, f_{2n}, \ldots \pmod{a-3} \qquad (**)$$

If $a = f_{2k} + f_{2k+2} + 3$, then the period of $(**)$ is exactly

$$0, 1, 3, \ldots, f_{2k}, -f_{2k}, \ldots, -3, -1$$

Fibonacci Numbers

Rabbits Strike Again

$$0, 1, 1, 2, 3, 5, 8, \ldots, f_{n+1} = f_n + f_{n-1}, \ldots$$

$$f^2 - fg - g^2 = \pm 1$$

$$f_{2(n+1)} = 3f_{2n} - f_{2(n-1)}$$

$$y_0, y_1, \ldots, y_n, \cdots \equiv 0, 1, ..., n, \ldots \pmod{a-1} \qquad (*)$$

$$y_0, y_1, \ldots, y_n, \cdots \equiv f_0, f_2, \ldots, f_{2n}, \ldots \pmod{a-3} \qquad (**)$$

If $a = f_{2k} + f_{2k+2} + 3$, then the period of $(**)$ is exactly

$$0, 1, 3, \ldots, f_{2k}, -f_{2k}, \ldots, -3, -1$$

$$f_{2k} + f_{2k+2} + 2, \qquad 2k + 1$$

Missing Link

Syncronization done

N. N. Vorob'ev, *Fibonacci Numbers*, Moscow, Nauka Publishing House

- 2nd ed., 1964
- 3rd ed., 1969

Missing Link

Syncronization done

N. N. Vorob'ev, *Fibonacci Numbers*, Moscow, Nauka Publishing House

- 2nd ed., 1964
- 3rd ed., 1969

$$f_n^2 \mid f_m \Rightarrow f_n \mid m$$

Missing Link

Syncronization done

N. N. Vorob'ev, *Fibonacci Numbers*, Moscow, Nauka Publishing House

- 2nd ed., 1964
- 3rd ed., 1969

$$f_n^2 \mid f_m \Rightarrow f_n \mid m$$

$$y_0, y_1, \ldots, y_n, \cdots \equiv 0, 1, ..., n, \ldots \pmod{a-1} \qquad (*)$$

$$y_0, y_1, \ldots, y_n, \ldots \equiv f_0, f_2, \ldots, f_{2n}, \ldots \pmod{a-3} \qquad (**)$$

Missing Link

Syncronization done

N. N. Vorob'ev, *Fibonacci Numbers*, Moscow, Nauka Publishing House

- 2nd ed., 1964
- 3rd ed., 1969

$$f_n^2 \mid f_m \Rightarrow f_n \mid m$$

$$y_0, y_1, \ldots, y_n, \cdots \equiv 0, 1, ..., n, \ldots \pmod{a-1} \qquad (*)$$

$$y_0, y_1, \ldots, y_n, \ldots \equiv f_0, f_2, \ldots, f_{2n}, \ldots \pmod{a-3} \qquad (**)$$

Julia Robinson: *Impose some condition $J(a)$ which would imply that the period of $(*)$ is a multiple of the period of $(**)$*

Missing Link

Syncronization done

N. N. Vorob'ev, *Fibonacci Numbers*, Moscow, Nauka Publishing House

- 2nd ed., 1964
- 3rd ed., 1969

$$f_n^2 \mid f_m \Rightarrow f_n \mid m$$

$$y_0, y_1, \ldots, y_n, \cdots \equiv 0, 1, ..., n, \ldots \pmod{a-1} \qquad (*)$$

$$y_0, y_1, \ldots, y_n, \ldots \equiv f_0, f_2, \ldots, f_{2n}, \ldots \pmod{a-3} \qquad (**)$$

Julia Robinson: *Impose some condition $J(a)$ which would imply that the period of $(*)$ is a multiple of the period of $(**)$*

My syncronization: *A condition $M(a)$ which implies that the period of $(**)$ is a multiple of the period of $(*)$*

DPRM-Theorem

Davis' Conjecture Proved

Theorem Every listable set $\mathfrak{M}$ has an Diophantine representation.

Current Records

Solving an arbitrary parametric Diophantine equation can be reduced to solving another Diophantine equation (with the same parameters) of degree D in M unknowns where $\langle D, M \rangle$ is any of the following pairs:

$$\langle 4, 58 \rangle, \langle 8, 38 \rangle, \langle 12, 32 \rangle, \langle 16, 29 \rangle, \langle 20, 28 \rangle, \langle 24, 26 \rangle, \langle 28, 25 \rangle,$$
$$\langle 36, 24 \rangle, \langle 96, 21 \rangle, \langle 2668, 19 \rangle, \langle 2 \times 10^5, 14 \rangle, \langle 6.6 \times 10^{43}, 13 \rangle,$$
$$\langle 1.3 \times 10^{44}, 12 \rangle, \langle 4.6 \times 10^{44}, 11 \rangle, \langle 8.6 \times 10^{44}, 10 \rangle, \langle 1.6 \times 10^{45}, 9 \rangle.$$

Davis's Conjecture Proved:

Effectively enumerable Sets are effectively Diophantine

DPRM-theorem. The notions of a Diophantine set and the notion of an effectively enumerable set coincide.

Davis's Conjecture Proved:

Effectively enumerable Sets are effectively Diophantine

DPRM-theorem. The notions of a Diophantine set and the notion of an effectively enumerable set coincide.

Given an arbitrary effectively enumerable set $\mathfrak{M}$ presented in any standard form one can construct corresponding polynomial giving Diophantine representation of the set.

Davis's Conjecture Proved:

Effectively enumerable Sets are effectively Diophantine

DPRM-theorem. The notions of a Diophantine set and the notion of an effectively enumerable set coincide.

Given an arbitrary effectively enumerable set $\mathfrak{M}$ presented in any standard form one can construct corresponding polynomial giving Diophantine representation of the set.

1. Construction of an arithmetical formula with many bounded universal quantifiers;

Davis's Conjecture Proved:

Effectively enumerable Sets are effectively Diophantine

DPRM-theorem. The notions of a Diophantine set and the notion of an effectively enumerable set coincide.

Given an arbitrary effectively enumerable set $\mathfrak{M}$ presented in any standard form one can construct corresponding polynomial giving Diophantine representation of the set.

1. Construction of an arithmetical formula with many bounded universal quantifiers;
2. Transformation of this formula into Davis normal form with single bounded universal quantifier;

Davis's Conjecture Proved:

Effectively enumerable Sets are effectively Diophantine

DPRM-theorem. The notions of a Diophantine set and the notion of an effectively enumerable set coincide.

Given an arbitrary effectively enumerable set $\mathfrak{M}$ presented in any standard form one can construct corresponding polynomial giving Diophantine representation of the set.

1. Construction of an arithmetical formula with many bounded universal quantifiers;
2. Transformation of this formula into Davis normal form with single bounded universal quantifier;
3. Elimination of the single bounded universal quantifier at the cost of passing to exponential Diophantine equations;

Davis's Conjecture Proved:

Effectively enumerable Sets are effectively Diophantine

DPRM-theorem. The notions of a Diophantine set and the notion of an effectively enumerable set coincide.

Given an arbitrary effectively enumerable set $\mathfrak{M}$ presented in any standard form one can construct corresponding polynomial giving Diophantine representation of the set.

1. Construction of an arithmetical formula with many bounded universal quantifiers;
2. Transformation of this formula into Davis normal form with single bounded universal quantifier;
3. Elimination of the single bounded universal quantifier at the cost of passing to exponential Diophantine equations;
4. Elimination of the exponentiation.

Davis's normal form: Original Proof

Formal reductions of the general combinatorial decision problem. *Amer. J. Math.*, v. 65 (1943), 197-215; reprinted in: *The Collected Works of E. L. Post*, Davis, M. (ed), Birkhäuser, Boston, 1994.

Emil L. Post
1897–1954

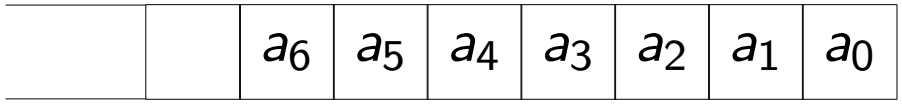
Davis's normal form: Original Proof

Formal reductions of the general combinatorial decision problem. *Amer. J. Math.*, v. 65 (1943), 197-215; reprinted in: *The Collected Works of E. L. Post*, Davis, M. (ed), Birkhäuser, Boston, 1994.

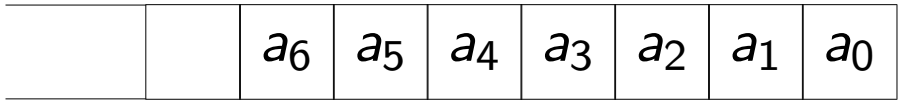
$$AX \mapsto XB$$

Emil L. Post
1897–1954

Existential Arithmetization I: Turing Machines

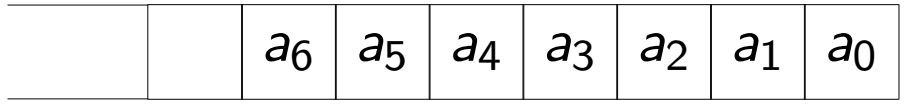


Existential Arithmetization I: Turing Machines



$$\sum_{k=0}^{\infty} a_k p^k$$

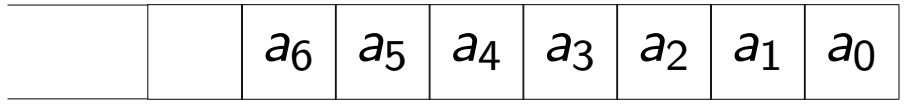
Existential Arithmetization I: Turing Machines



$$\sum_{k=0}^{\infty} a_k p^k$$

$$\binom{a+b}{b} = \frac{(a+b)!}{a!\,b!} = 2^{\beta_2}\,3^{\beta_3}\,5^{\beta_5}\,\ldots$$

Existential Arithmetization I: Turing Machines



$$\sum_{k=0}^{\infty} a_k p^k$$

$$\left(\begin{array}{c} a+b \\ b \end{array} \right) = \frac{(a+b)!}{a!\, b!} = 2^{\beta_2}\, 3^{\beta_3}\, 5^{\beta_5} \ldots$$

Theorem (E.Kummer [1852]) In order to calculate β_p: *write a and b in base-p notation and add them; the number of carries from digit to digit performed during this addition is exactly β_p.*

Existential Arithmetization II: Register Machines

A register machine has a finite number of *registers* R1, . . . ,Rn each of which is capable of containing an arbitrarily large natural number. The machine performs a *program* consisting of finitely many *instructions* labeled by S1, . . . ,Sm.

I. Sk: R$l++$; goto Si

II. Sk: if R$l > 0$ then R$l--$; goto Si else goto Sj

III. Sk: STOP

Existential Arithmetization II: Register Machines

A register machine has a finite number of *registers* R1, . . . ,Rn each of which is capable of containing an arbitrarily large natural number. The machine performs a *program* consisting of finitely many *instructions* labeled by S1, . . . ,Sm.

I. Sk: R$l++$; goto Si

II. Sk: if R$l > 0$ then R$l--$; goto Si else goto Sj

III. Sk: STOP

Introduced by J. Lambek [1961], Z. A. Melzak [1961], M. L. Minsky [1961, 1967], J. C. Shepherdson and H. E. Sturgis [1963]

Existential Arithmetization III: Partial Recursive Functions

$$\begin{aligned} f(0,c) &= g(c), \\ f(a+1,c) &= h(a,f(a),c) \end{aligned}$$

Existential Arithmetization III: Partial Recursive Functions

$$\begin{aligned} f(0,c) &= g(c), \\ f(a+1,c) &= h(a, f(a), c) \end{aligned}$$

$$\begin{bmatrix} f(0,c) \\ f(1,c) \\ \vdots \\ f(a,c) \\ f(a+1,c) \end{bmatrix} = \begin{bmatrix} g(c) \\ \\ h\left(\begin{bmatrix} 0 \\ \vdots \\ a-1 \\ a \end{bmatrix}, \begin{bmatrix} f(0,c) \\ \vdots \\ f(a-1,c) \\ f(a,c) \end{bmatrix}, \begin{bmatrix} c \\ \vdots \\ c \\ c \end{bmatrix}\right) \end{bmatrix}$$

Existential Arithmetization III: Partial Recursive Functions

$$\begin{bmatrix} X \\ \\ \\ x \end{bmatrix} = \begin{bmatrix} g(c) \\ \\ h\left(\begin{bmatrix} 0 \\ \vdots \\ a \end{bmatrix}, X, \begin{bmatrix} c \\ \vdots \\ c \end{bmatrix}\right) \end{bmatrix}$$

Existential Arithmetization III: Partial Recursive Functions

$$\begin{bmatrix} X \\ \\ \\ x \end{bmatrix} = \begin{bmatrix} g(c) \\ \\ h\left(\begin{bmatrix} 0 \\ \vdots \\ a \end{bmatrix}, X, \begin{bmatrix} c \\ \vdots \\ c \end{bmatrix}\right) \end{bmatrix}$$

$$X = f\left(\begin{bmatrix} 0 \\ \vdots \\ a \end{bmatrix}, \begin{bmatrix} c \\ \vdots \\ c \end{bmatrix}\right) = \begin{bmatrix} f(0,c) \\ \vdots \\ f(a,c) \end{bmatrix}, \quad x = f(a+1,c)$$

Existential Arithmetization III: Partial Recursive Functions

$$f\left(\begin{bmatrix} a_{1,1} \\ \vdots \\ a_{l,1} \end{bmatrix}, \ldots, \begin{bmatrix} a_{1,n} \\ \vdots \\ a_{l,n} \end{bmatrix}\right) = \begin{bmatrix} f(a_{1,1}, \ldots, a_{1,n}) \\ \ldots \\ f(a_{l,1}, \ldots, a_{l,n}) \end{bmatrix}$$

$$f(A_1, \ldots, A_n) = B \iff \exists x_1 \ldots x_m [F(\bar{A}_1, \ldots, \bar{A}_n, \bar{B}, x_1, \ldots, x_m) = 0]$$

Speeding up Diophantine Equations

Theorem (M.Davis [1973] after M.Blum [1967]).

Speeding up Diophantine Equations

Theorem (M.Davis [1973] after M.Blum [1967]). *For every total computable function* $\alpha(a, x)$ *one can construct two one-parameter Diophantine equations*

$$P_1(a, x_1, \ldots, x_k) = 0, \qquad P_2(a, x_1, \ldots, x_k) = 0 \tag{$*$}$$

such that

Speeding up Diophantine Equations

Theorem (M.Davis [1973] after M.Blum [1967]). *For every total computable function* $\alpha(a, x)$ *one can construct two one-parameter Diophantine equations*

$$P_1(a, x_1, \ldots, x_k) = 0, \qquad P_2(a, x_1, \ldots, x_k) = 0 \tag{$*$}$$

such that

(i) *for every value of the parameter a exactly one of these two equations has a solution;*

Speeding up Diophantine Equations

Theorem (M.Davis [1973] after M.Blum [1967]). *For every total computable function* $\alpha(a, x)$ *one can construct two one-parameter Diophantine equations*

$$P_1(a, x_1, \ldots, x_k) = 0, \qquad P_2(a, x_1, \ldots, x_k) = 0 \tag{$*$}$$

such that

(i) *for every value of the parameter a exactly one of these two equations has a solution;*

(ii) *if Diophantine equations*

$$Q_1(a, y_1, \ldots, y_l) = 0, \qquad Q_2(a, y_1, \ldots, y_l) = 0 \tag{$**$}$$

are solvable for the same values of the parameter a as, respectively, equations $(*)$,

Speeding up Diophantine Equations

Theorem (M.Davis [1973] after M.Blum [1967]). *For every total computable function* $\alpha(a, x)$ *one can construct two one-parameter Diophantine equations*

$$P_1(a, x_1, \ldots, x_k) = 0, \qquad P_2(a, x_1, \ldots, x_k) = 0 \tag{$*$}$$

such that

(i) *for every value of the parameter a exactly one of these two equations has a solution;*

(ii) *if Diophantine equations*

$$Q_1(a, y_1, \ldots, y_l) = 0, \qquad Q_2(a, y_1, \ldots, y_l) = 0 \tag{$**$}$$

are solvable for the same values of the parameter a as, respectively, equations $(*)$*, then one can construct a third pair of Diophantine equations*

$$R_1(a, z_1, \ldots, z_m) = 0, \qquad R_2(a, z_1, \ldots, z_m) = 0 \tag{$***$}$$

such that

Speeding up Diophantine Equations

Theorem (M.Davis [1973] after M.Blum [1967]). *For every total computable function* $\alpha(a, x)$ *one can construct two one-parameter Diophantine equations*

$$P_1(a, x_1, \ldots, x_k) = 0, \qquad P_2(a, x_1, \ldots, x_k) = 0 \tag{$*$}$$

such that

(i) *for every value of the parameter a exactly one of these two equations has a solution;*

(ii) *if Diophantine equations*

$$Q_1(a, y_1, \ldots, y_l) = 0, \qquad Q_2(a, y_1, \ldots, y_l) = 0 \tag{$**$}$$

are solvable for the same values of the parameter a as, respectively, equations $(*)$*, then one can construct a third pair of Diophantine equations*

$$R_1(a, z_1, \ldots, z_m) = 0, \qquad R_2(a, z_1, \ldots, z_m) = 0 \tag{$***$}$$

such that

- *these equations are again solvable for the same values of the parameter a as, respectively, equations* $(*)$*;*

Speeding up Diophantine Equations

Theorem (M.Davis [1973] after M.Blum [1967]). *For every total computable function* $\alpha(a, x)$ *one can construct two one-parameter Diophantine equations*

$$P_1(a, x_1, \ldots, x_k) = 0, \qquad P_2(a, x_1, \ldots, x_k) = 0 \tag{$*$}$$

such that

(i) *for every value of the parameter a exactly one of these two equations has a solution;*

(ii) *if Diophantine equations*

$$Q_1(a, y_1, \ldots, y_l) = 0, \qquad Q_2(a, y_1, \ldots, y_l) = 0 \tag{$**$}$$

are solvable for the same values of the parameter a as, respectively, equations $(*)$*, then one can construct a third pair of Diophantine equations*

$$R_1(a, z_1, \ldots, z_m) = 0, \qquad R_2(a, z_1, \ldots, z_m) = 0 \tag{$***$}$$

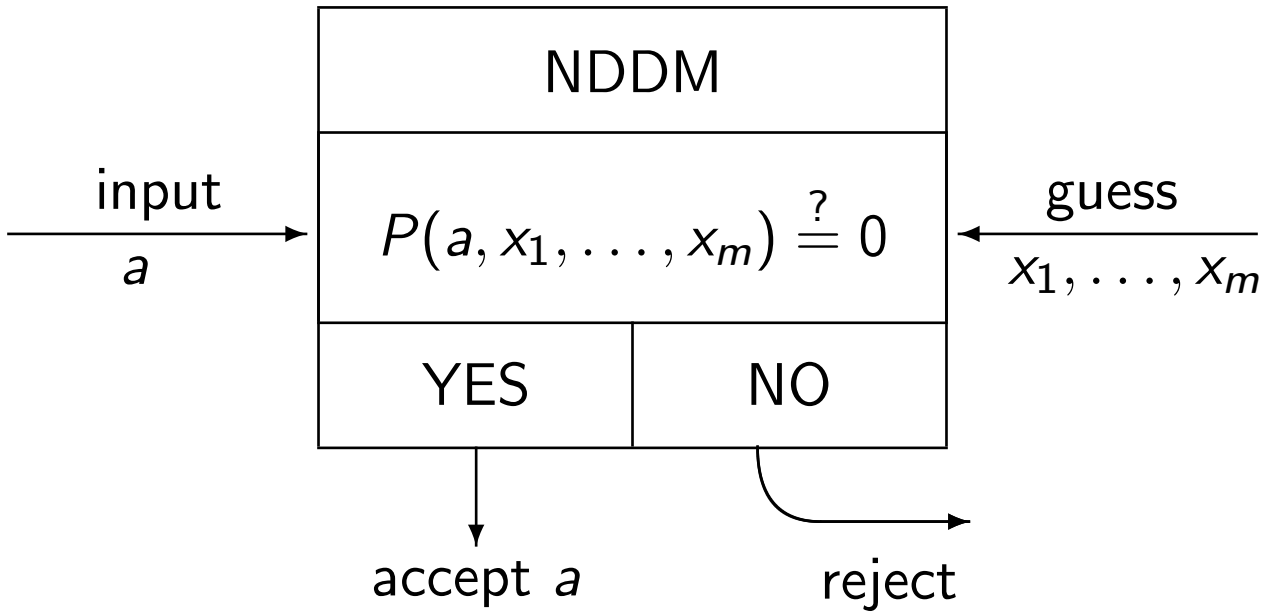
such that

- *these equations are again solvable for the same values of the parameter a as, respectively, equations* $(*)$*;*
- *for all sufficiently large values of the parameter a for every solution* $y_1, \ldots, y_l$ *of one of the equations* $(**)$ *there exists a solution* $z_1, \ldots, z_m$ *of the corresponding equation* $(***)$ *such that*

$$y_1 + \cdots + y_l > \alpha(a, z_1 + \cdots + z_m).$$

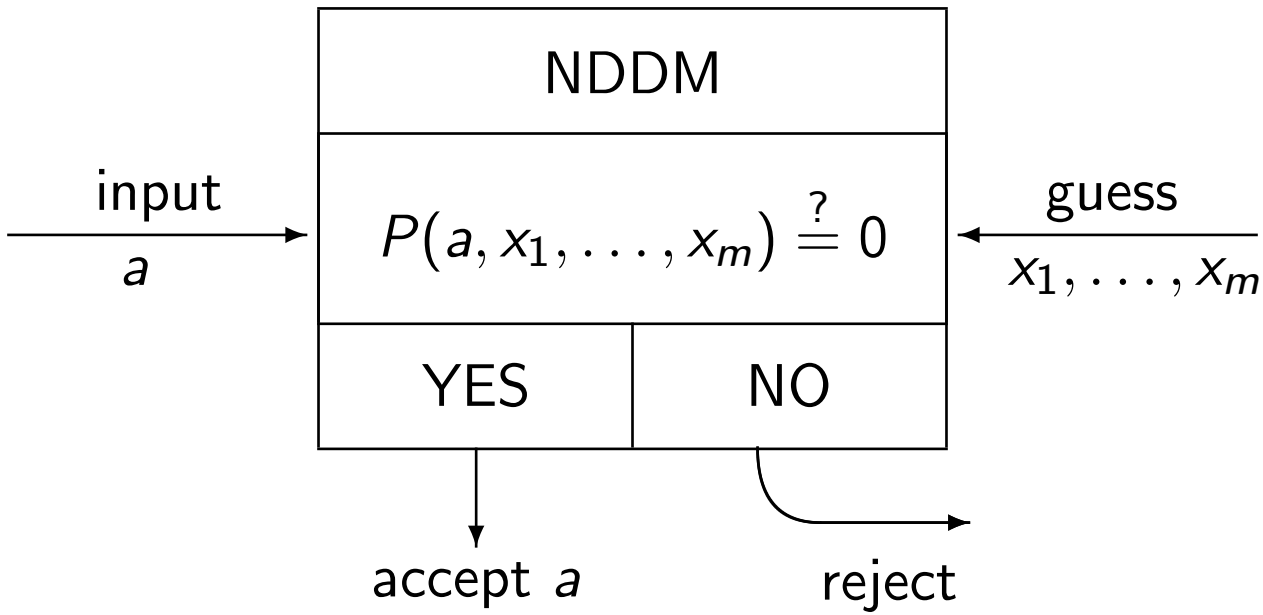
Diophantine Machines: Capturing Nondeterminism

Leonard Adleman and Kenneth Manders [1976] introduced the notion of *Non-Deterministic Diophantine Machine*, NDDM for short.



Diophantine Machines: Capturing Nondeterminism

Leonard Adleman and Kenneth Manders [1976] introduced the notion of *Non-Deterministic Diophantine Machine*, NDDM for short.



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*.

Unambiguity: Equations with Unique Solution

Definition. A purely existential representation

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

is called *single-fold* if for given value of the parameter a there exists at most one choice of the values of $x_1, \ldots, x_m$.

Unambiguity: Equations with Unique Solution

Definition. A purely existential representation

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

is called *single-fold* if for given value of the parameter a there exists at most one choice of the values of $x_1, \ldots, x_m$.

Theorem (Yu.Matiyasevich [1974] as an improvement of DPR[1961]). Every effectively enumerable set $\mathfrak{M}$ has a single-fold exponential Diophantine representation

$$a \in \mathfrak{M} \Longleftrightarrow \exists x_1 \ldots x_m [E(a, x_1, x_2, \ldots, x_m) = 0]$$

where E is an exponential polynomial.

Unambiguity: Equations with Unique Solution

Definition. A purely existential representation

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

is called *single-fold* if for given value of the parameter a there exists at most one choice of the values of $x_1, \ldots, x_m$.

Theorem (Yu.Matiyasevich [1974] as an improvement of DPR[1961]). Every effectively enumerable set $\mathfrak{M}$ has a single-fold exponential Diophantine representation

$$a \in \mathfrak{M} \Longleftrightarrow \exists x_1 \ldots x_m [E(a, x_1, x_2, \ldots, x_m) = 0]$$

where E is an exponential polynomial.

Open Problem. Does every effectively enumerable set $\mathfrak{M}$ have a single-fold Diophantine representation

$$a \in \mathfrak{M} \Longleftrightarrow \exists x_1 \ldots x_m [P(a, x_1, x_2, \ldots, x_m) = 0]$$

where P is a polynomial?

Unambiguity: Equations with Unique Solution

Open Problem. Does every effectively enumerable set $\mathfrak{M}$ have a single-fold Diophantine representation

$$a \in \mathfrak{M} \Longleftrightarrow \exists x_1 \ldots x_m [P(a, x_1, x_2, \ldots, x_m) = 0]$$

where P is a polynomial?

Unambiguity: Equations with Unique Solution

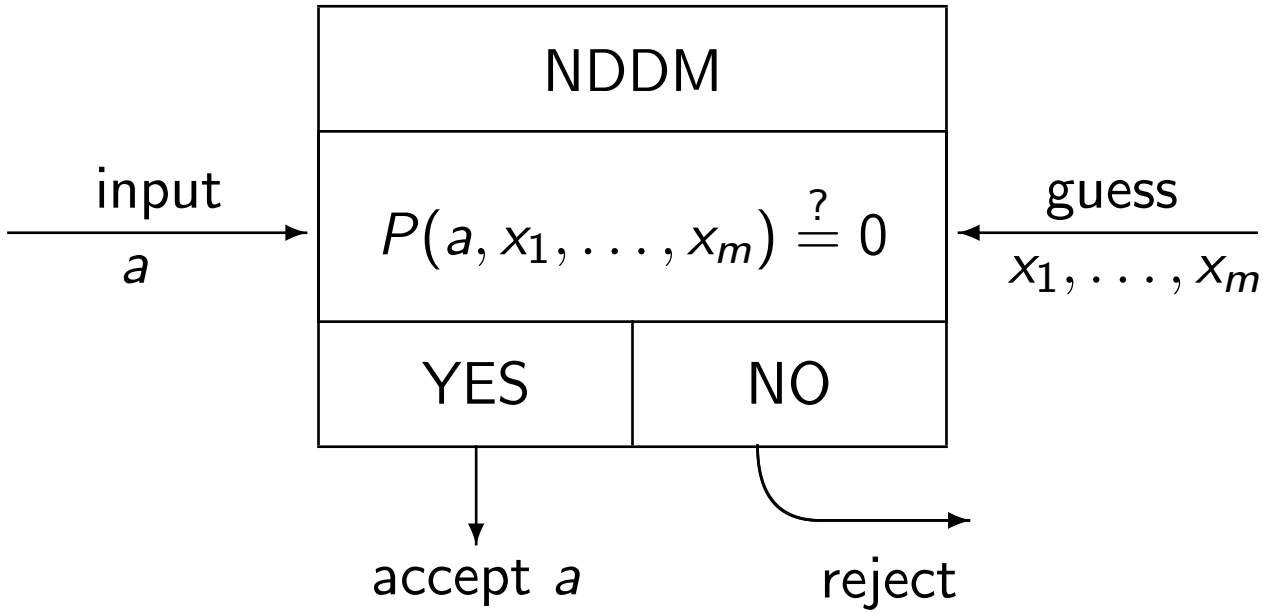
Open Problem. Does every effectively enumerable set $\mathfrak{M}$ have a single-fold Diophantine representation

$$a \in \mathfrak{M} \Longleftrightarrow \exists x_1 \ldots x_m [P(a, x_1, x_2, \ldots, x_m) = 0]$$

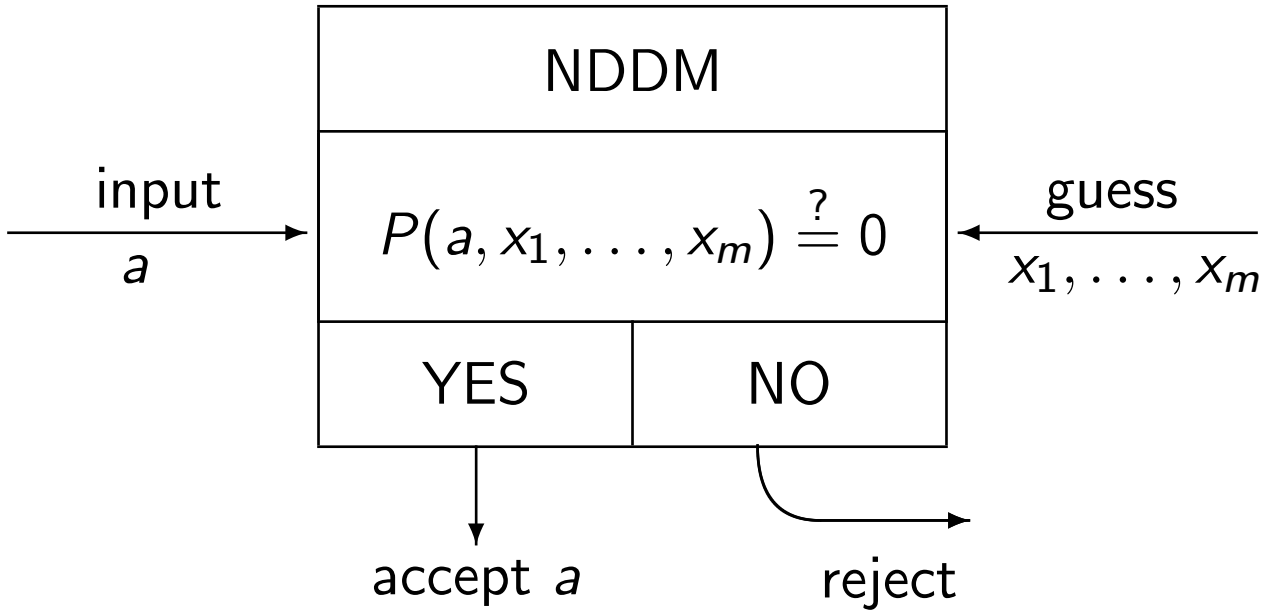
where P is a polynomial?

Open Problem (reformulation) Are unambiguous NDDMs are as powerful as (deterministic) Turing machines?

Diophantine Complexity: Time and Space vs Size



Diophantine Complexity: Time and Space vs Size



SIZE(a)=the minimal possible value of $|x_1| + \cdots + |x_m|$ where $|x|$ denotes the binary length of x.

Diophantine Complexity: D vs NP

Leonard Adleman and Kenneth Manders [1975] introduced the class **D** consisting of all sets $\mathfrak{M}$ having representations of the form

$$a \in \mathfrak{M} \quad \Longleftrightarrow \quad \exists x_1 \ldots x_m \left[P(a, x_1, \ldots, x_m) = 0 \,\&\, |x_1| + \cdots + |x_m| \leq |a|^k \right]$$

where $|x|$ denotes the binary length of x.

Diophantine Complexity: D vs NP

Leonard Adleman and Kenneth Manders [1975] introduced the class **D** consisting of all sets $\mathfrak{M}$ having representations of the form

$$a \in \mathfrak{M} \quad \Longleftrightarrow \quad \exists x_1 \ldots x_m \big[P(a, x_1, \ldots, x_m) = 0 \,\&\, |x_1| + \cdots + |x_m| \leq |a|^k \big]$$

where $|x|$ denotes the binary length of x.

Open question. D $\stackrel{?}{=}$ NP.

Diophantine Complexity: D vs NP

Leonard Adleman and Kenneth Manders [1975] introduced the class **D** consisting of all sets $\mathfrak{M}$ having representations of the form

$$a \in \mathfrak{M} \iff \exists x_1 \ldots x_m \left[P(a, x_1, \ldots, x_m) = 0 \,\&\, |x_1| + \cdots + |x_m| \leq |a|^k \right]$$

where $|x|$ denotes the binary length of x.

Open question. $\mathbf{D} \stackrel{?}{=} \mathbf{NP}$.

Theorem (Chris Pollett [2003]).

$$\mathbf{D} \subseteq \mathbf{co{-}NLOGTIME} \Longrightarrow \mathbf{D} = \mathbf{NP}$$

Diophantine Complexity: D vs NP

Leonard Adleman and Kenneth Manders [1975] introduced the class **D** consisting of all sets $\mathfrak{M}$ having representations of the form

$$a \in \mathfrak{M} \iff \exists x_1 \ldots x_m \left[P(a, x_1, \ldots, x_m) = 0 \,\&\, |x_1| + \cdots + |x_m| \leq |a|^k \right]$$

where $|x|$ denotes the binary length of x.

Open question. $\mathbf{D} \stackrel{?}{=} \mathbf{NP}$.

Theorem (Chris Pollett [2003]).

$$\mathbf{D} \subseteq \mathbf{co{-}NLOGTIME} \Longrightarrow \mathbf{D} = \mathbf{NP}$$

Helger Lipmaa [2003] introduced **PD**, the "deterministic part" of the class **D**.

Above Hilbert's Tenth Problem: Computational Chaos

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

Above Hilbert's Tenth Problem: Computational Chaos

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

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

Above Hilbert's Tenth Problem: Computational Chaos

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

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

The set $\mathfrak{M}_n$ can be effectively calculated from $\|\mathfrak{M}_n\|$, the cardinality of $\mathfrak{M}_n$.

Above Hilbert's Tenth Problem: Computational Chaos

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

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

The set $\mathfrak{M}_n$ can be effectively calculated from $\|\mathfrak{M}_n\|$, the cardinality of $\mathfrak{M}_n$.

The *descriptive* or *Kolmogorov* complexity of $\mathfrak{M}_n$ is at most $\log(n)$.

Above Hilbert's Tenth Problem: Computational Chaos

Gregory Chaitin [1987] 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:

$$a \in \mathfrak{M} \Longleftrightarrow \exists^{\infty} x_1 \ldots x_m [E(a, x_1, x_2, \ldots, x_m) = 0]$$

He proved that so called *prefix-free* Kolmogorov complexity of the initial segment

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

is equal to n (up to an additive constant).

Above Hilbert's Tenth Problem: Computational Chaos

Gregory Chaitin [1987] 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:

$$a \in \mathfrak{M} \Longleftrightarrow \exists^{\infty} x_1 \ldots x_m [E(a, x_1, x_2, \ldots, x_m) = 0]$$

He proved that so called *prefix-free* Kolmogorov complexity of the initial segment

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

is equal to n (up to an additive constant).

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