What WE CAN do with Diophantine problems and what WE CANNOT do

Yu. V. Matiyasevich

Steklov Institute of Mathematics at St.Petersburg, Russia

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

Hilbert's 10th Problem

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 10th Problem

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]

Terminology–what are Diophantine equations?

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*.

Terminology–what are Diophantine equations?

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 the present talk, a Diophantine equation is an equation of the form

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

where P is a polynomial with integer coefficients.

Terminology–what is a process?

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*.

Terminology–what is a process?

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.

Terminology–what is a process?

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.

Terminology–what is a process?

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.

Range of the 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*.

Range of the 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*.

$$x^3 + y^3 = z^3$$

Range of the 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*.

$$x^3 + y^3 = z^3$$

Has this equation solutions in integers?

Range of the 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*.

$$x^3 + y^3 = z^3$$

Has this equation solutions in integers?
Yes

Range of the 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*.

$$x^3 + y^3 = z^3$$

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

Range of the 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*.

$$x^3 + y^3 = z^3$$

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

Has this equation solutions in natural numbers?

Range of the 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*.

$$x^3 + y^3 = z^3$$

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

Has this equation solutions in natural numbers?
No

Range of the 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*.

$$x^3 + y^3 = z^3$$

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

Has this equation solutions in natural numbers?
No, and this isn't trivial.

From All Integers to Natural Numbers

An equation

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

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

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

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

From All Integers to Natural Numbers

An equation

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

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

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

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

Thus WE CAN *reduce* solving an arbitrary Diophantine equations in integers to solving another Diophantine equations in natural numbers.

From All Integers to Natural Numbers

An equation

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

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

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

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

Thus WE CAN *reduce* solving an arbitrary Diophantine equations in integers to solving another Diophantine equations in natural numbers.

So WE CAN *reduce* the decision problem of recognizing solvability of Diophantine equations in integers to the similar decision problem of recognizing the solvability of Diophantine equations in natural numbers.

From Non-negative Integers to All Integers

An equation

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

has a solution in natural numbers if and only if system

$$\begin{aligned} P(p_1, \ldots, p_m) &= 0 \\ p_1 &= w_1^2 + x_1^2 + y_1^2 + z_1^2 + 1 \\ &\vdots \\ p_m &= w_m^2 + x_m^2 + y_m^2 + z_m^2 + 1 \end{aligned}$$

has a solution in integers.

From Non-negative Integers to All Integers

An equation

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

has a solution in natural numbers if and only if system

$$\begin{aligned} P(p_1, \ldots, p_m) &= 0 \\ p_1 &= w_1^2 + x_1^2 + y_1^2 + z_1^2 + 1 \\ &\vdots \\ p_m &= w_m^2 + x_m^2 + y_m^2 + z_m^2 + 1 \end{aligned}$$

has a solution in integers.

Thus WE CAN *reduce* the decision problem of recognizing solvability of Diophantine equations in natural numbers to the decision problem of recognizing the solvability of Diophantine equations in integers.

Natural Numbers vs All Integers

For a particular Diophantine equation the question whether it has a solution in integers and the question whether it has a solution in natural numbers are, in general, two different questions.

Natural Numbers vs All Integers

For a particular Diophantine equation the question whether it has a solution in integers and the question whether it has a solution in natural numbers are, in general, two different questions.

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

The Undecidability of Hilbert's Tenth Problem

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

The Undecidability of Hilbert's Tenth Problem

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

Theorem (Undecidability of Hilbert's tenth problem)
WE CANNOT algorithmically decide, given an arbitrary Diophantine equation, whether it has a solution or not.

The Undecidability of Hilbert's Tenth Problem

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

Theorem (Undecidability of Hilbert's tenth problem)
WE CANNOT algorithmically decide, given an arbitrary Diophantine equation, whether it has a solution or not.

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

The Effective Undecidability of Hilbert's Tenth Problem

Given any algorithm supposedly solving Hilbert's 10th problem in the positive sense WE CAN effectively construct a Diophantine equation

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

for which this algorithm gives, if any, an incorrect answer.

The Effective Undecidability of Hilbert's Tenth Problem

Given any algorithm supposedly solving Hilbert's 10th problem in the positive sense WE CAN effectively construct a Diophantine equation

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

for which this algorithm gives, if any, an incorrect answer.

However, WE CANNOT in general decide whether this equation has a solution or not.

A Generalization of the 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*.

A Generalization of the 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*.

Let $\#(P(x_1, \ldots, x_m) = 0)$ denote the number of solutions of the equation

A Generalization of the 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*.

Let $\#(P(x_1, \ldots, x_m) = 0)$ denote the number of solutions of the equation, $\#(P(x_1, \ldots, x_m) = 0) \in \mathfrak{N} = \{0, 1, \ldots, \aleph_0\}$.

A Generalization of the 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*.

Let $\#(P(x_1, \ldots, x_m) = 0)$ denote the number of solutions of the equation, $\#(P(x_1, \ldots, x_m) = 0) \in \mathfrak{N} = \{0, 1, \ldots, \aleph_0\}$.

For what subset $\mathfrak{M} \subset \mathfrak{N}$ CAN WE algorithmically decide, given an arbitrary Diophantine equation $P(x_1, \ldots, x_m)$, whether

$$\#(P(x_1, \ldots, x_m) = 0) \in \mathfrak{M}?$$

A Generalization of the 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*.

Let $\#(P(x_1, \ldots, x_m) = 0)$ denote the number of solutions of the equation, $\#(P(x_1, \ldots, x_m) = 0) \in \mathfrak{N} = \{0, 1, \ldots, \aleph_0\}$.

For what subset $\mathfrak{M} \subset \mathfrak{N}$ CAN WE algorithmically decide, given an arbitrary Diophantine equation $P(x_1, \ldots, x_m)$, whether

$$\#(P(x_1, \ldots, x_m) = 0) \in \mathfrak{M}?$$

Hilbert's 10th Problem is the cases $\mathfrak{M} = \{0\}$ and its complement $\mathfrak{M} = \{1, 2, \ldots, \aleph_0\}$.

A Generalization of the Problem

Theorem (Martin Davis [1972]). WE CANNOT algorithmically decide, given an arbitrary Diophantine equation $P(x_1, \ldots, x_m) = 0$, whether

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

unless $\mathfrak{M} = \emptyset$ or $\mathfrak{M} = \mathfrak{N}$.

A Generalization of the Problem

Theorem (Martin Davis [1972]). WE CANNOT algorithmically decide, given an arbitrary Diophantine equation $P(x_1, \ldots, x_m) = 0$, whether

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

unless $\mathfrak{M} = \emptyset$ or $\mathfrak{M} = \mathfrak{N}$.

Main Lemma. If $\mathfrak{M} \subset \mathfrak{N}$ and neither $\mathfrak{M} = \emptyset$ nor $\mathfrak{M} = \mathfrak{N}$ then given an arbitrary Diophantine equation $P(x_1, \ldots, x_m) = 0$ WE CAN construct another equation $Q(x_1, \ldots, x_m) = 0$ and reduce the question

$$\#(P(x_1, \ldots, x_m) = 0) \stackrel{?}{=} 0$$

to the question

$$\#(P(x_1, \ldots, x_m) = 0) \stackrel{?}{\in} \mathfrak{M}.$$

Back to Diophantus

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.*

Back to Diophantus

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 rational numbers.*

From Rational Numbers to Integers

An equation

$$P(\chi_1, \ldots, \chi_m) = 0$$

has a solution in rational numbers $\chi_1, \ldots, \chi_m$ if and only if the equation

$$P\left(\frac{x_1}{v_1^2 + w_1^2 + y_1^2 + z_1^2 + 1}, \ldots, \frac{x_m}{v_m^2 + w_m^2 + y_m^2 + z_m^2 + 1}\right) = 0$$

has a solution in integers $v_1, \ldots, v_m$, $w_1, \ldots, w_m$, $x_1, \ldots, x_m$, $y_1, \ldots, y_m$, $z_1, \ldots, z_m$.

From Rational Numbers to Integers

An equation

$$P(\chi_1, \ldots, \chi_m) = 0$$

has a solution in rational numbers $\chi_1, \ldots, \chi_m$ if and only if the equation

$$P\left(\frac{x_1}{v_1^2 + w_1^2 + y_1^2 + z_1^2 + 1}, \ldots, \frac{x_m}{v_m^2 + w_m^2 + y_m^2 + z_m^2 + 1}\right) = 0$$

has a solution in integers $v_1, \ldots, v_m$, $w_1, \ldots, w_m$, $x_1, \ldots, x_m$, $y_1, \ldots, y_m$, $z_1, \ldots, z_m$.

Thus WE CAN reduce the decision problem of recognizing solvability of Diophantine equations in rational numbers to the decision problem of recognizing the solvability of Diophantine equations in integers.

From Integers to Rational Numbers?

CAN WE reduce the decision problem of recognizing solvability of Diophantine equations in integers to the decision problem of recognizing the solvability of Diophantine equations in rational numbers?

From Integers to Rational Numbers?

CAN WE reduce the decision problem of recognizing solvability of Diophantine equations in integers to the decision problem of recognizing the solvability of Diophantine equations in rational numbers?

Hypothetical Theorem. *An equation*

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

has a solution in integers if and only if system

$$\begin{aligned} P(p_1, \ldots, p_m) &= 0 \\ R(p_1, \ldots) &= 0 \\ &\vdots \\ R(p_m, \ldots) &= 0 \end{aligned}$$

has a solution in rational numbers.

From Integers to Rational Numbers?

Hypothetical Main Lemma. There is a polynomial $R(x, y_1, \ldots, y_n)$ with rational integer coefficients such that

- in every solution of equation

$$R(x, y_1, \ldots, y_n) = 0 \qquad (*)$$

  in rational numbers $x, y_1, \ldots, y_n$ the value of x is an integer;
- for every integer x there are rational numbers $y_1, \ldots, y_n$ satisfying $(*)$.

Barry Mazur [1992,1994] put forward a number of conjectures which imply the impossibility to construct such a polynomial $R(x, y_1, \ldots, y_n)$.

Open Problem

CAN WE algorithmically decide, given an arbitrary Diophantine equation, whether it has a solution in rational number?

Open Problem

CAN WE algorithmically decide, given an arbitrary Diophantine equation, whether it has a solution in rational number?

An Equivalent Question:

CAN WE algorithmically decide, given an arbitrary homogeneous Diophantine equation, whether it has a solution in integers?

Another Variation of the 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* .

Another Variation of the 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*~~ *in algebraic integers*.

A specialization:

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 Gaussian integers*.

From Gaussian Integers to Rational Integers

An equation

$$P(\chi_1, \ldots, \chi_m) = 0$$

has a solution in Gaussian integers if and only if the equation

$$P(x_1 + y_1\mathrm{i}, \ldots, x_m + y_m\mathrm{i}) = 0$$

has a solution in *rational integers*.

From Gaussian Integers to Rational Integers

An equation

$$P(\chi_1, \ldots, \chi_m) = 0$$

has a solution in Gaussian integers if and only if the equation

$$P(x_1 + y_1\mathrm{i}, \ldots, x_m + y_m\mathrm{i}) = 0$$

has a solution in *rational integers*.

Thus WE CAN reduce the decision problem of recognizing solvability of Diophantine equations in Gaussian integers to the decision problem of recognizing the solvability of Diophantine equations in rational integers.

From Rational Integers to Gaussian Integers?

CAN WE reduce the decision problem of recognizing solvability of Diophantine equations in rational numbers to the decision problem of recognizing the solvability of Diophantine equations in Gaussian integers?

From Rational Integers to Gaussian Integers?

CAN WE reduce the decision problem of recognizing solvability of Diophantine equations in rational numbers to the decision problem of recognizing the solvability of Diophantine equations in Gaussian integers?

Theorem (Jan Denef [1975]). WE CAN find a polynomial $D(x, y_1, \ldots, y_n)$ with rational integer coefficients such that

- in every solution of equation

$$D(x, y_1, \ldots, y_n) = 0 \qquad (*)$$

  in Gaussian integers $x, y_1, \ldots, y_n$ the value of x is a rational integer;

- for every rational integer x there are Gaussian integers $y_1, \ldots, y_n$ satisfying $(*)$.

Corollaries

An equation

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

has a solution in rational integers if and only if system

$$\begin{aligned} P(x_1, \ldots, x_m) &= 0 \\ D(x_1, y_{1,1}, \ldots, y_{1,n}) &= 0 \\ &\vdots \\ D(x_m, y_{m,1}, \ldots, y_{m,n}) &= 0 \end{aligned}$$

has a solution in Gaussian integers.

Corollaries

An equation

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

has a solution in rational integers if and only if system

$$\begin{aligned} P(x_1, \ldots, x_m) &= 0 \\ D(x_1, y_{1,1}, \ldots, y_{1,n}) &= 0 \\ &\vdots \\ D(x_m, y_{m,1}, \ldots, y_{m,n}) &= 0 \end{aligned}$$

has a solution in Gaussian integers.

WE CAN reduce the decision problem of solvability of Diophantine equations in rational integers to the decision problem of solvability of Diophantine equations in Gaussian integers.

Corollaries

An equation

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

has a solution in rational integers if and only if system

$$\begin{aligned} P(x_1, \ldots, x_m) &= 0 \\ D(x_1, y_{1,1}, \ldots, y_{1,n}) &= 0 \\ &\vdots \\ D(x_m, y_{m,1}, \ldots, y_{m,n}) &= 0 \end{aligned}$$

has a solution in Gaussian integers.

WE CAN reduce the decision problem of solvability of Diophantine equations in rational integers to the decision problem of solvability of Diophantine equations in Gaussian integers.

WE CANNOT decide, given an arbitrary Diophantine equation, whether it has a solution in Gaussian integers.

Another Variation of the Problem (cont.)

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 algebraic integers*.

Another Variation of the Problem (cont.)

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 algebraic integers*.

Specialization 1:

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 algebraic integers from a fixed finite extension of rational numbers.*

Decidable case

Specialization 2:

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 arbitrary algebraic integers.*

Decidable case

Specialization 2:

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 arbitrary algebraic integers.*

Theorem (Robert S. Roumely [1986]). WE CAN algorithmically decide, given an arbitrary Diophantine equation, whether it has a solution in arbitrary algebraic integers.

Diophantine Sets

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*.

Diophantine Sets

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*.

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

P is a polynomial with integer coefficients

Diophantine Sets

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*.

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

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

Diophantine Sets

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*.

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

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

the parameters $a_1, \ldots, a_n$

Diophantine Sets

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*.

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

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

the parameters $a_1, \ldots, a_n$ and the unknowns $x_1, \ldots, x_m$.

Diophantine Sets

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*.

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

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

the parameters $a_1, \ldots, a_n$ and the unknowns $x_1, \ldots, x_m$.

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

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

Diophantine Sets

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*.

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

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

the parameters $a_1, \ldots, a_n$ and 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

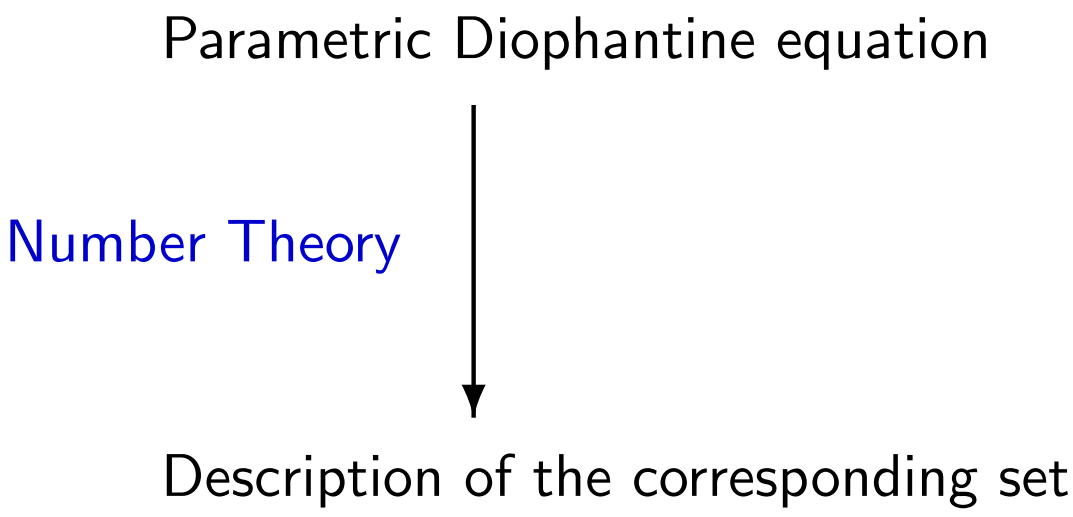
$$a - (2x_1 + 3)(x_2 + 1) = 0.$$

Martin Davis' Conjecture

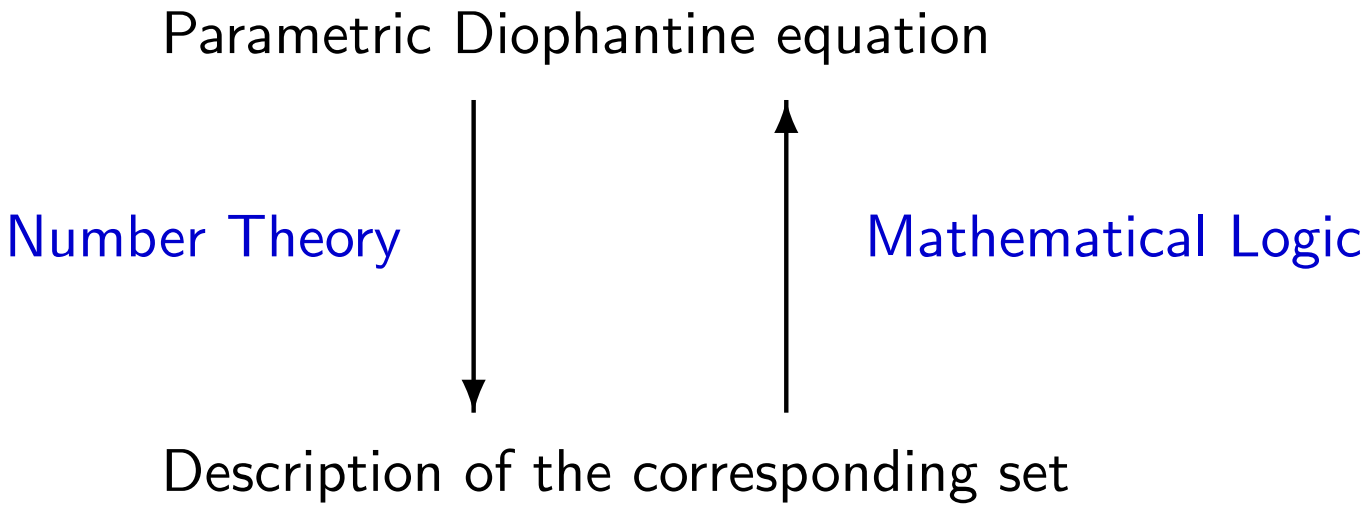
Martin Davis' Conjecture

Parametric Diophantine equation

Martin Davis' Conjecture



Martin Davis' Conjecture



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 (=effectively enumerable = semidecidable) if there is an algorithm which would print in some order, possibly with repetitions, all elements of the set $\mathfrak{M}$.

Martin Davis' Conjecture

Evident fact. *Every Diophantine set is listable.*

Martin Davis' Conjecture

Evident fact. *Every Diophantine set is listable.*

Martin Davis' Conjecture (1950's) *Every listable set is Diophantine.*

Martin Davis' Conjecture

Evident fact. *Every Diophantine set is listable.*

Martin Davis' Conjecture (1950's) *Every listable set is Diophantine.*

DPRM Theorem [1970]. *Every listable set is Diophantine*

Martin Davis' Conjecture

Evident fact. *Every Diophantine set is listable.*

Martin Davis' Conjecture (1950's) *Every listable set is Diophantine.*

DPRM Theorem [1970]. *Every listable set is Diophantine, and given any standard representaion of a listable set, WE CAN construct corresponding Diophantine equation.*

Martin Davis' Conjecture

Evident fact. *Every Diophantine set is listable.*

Martin Davis' Conjecture (1950's) *Every listable set is Diophantine.*

DPRM Theorem [1970]. *Every listable set is Diophantine, and given any standard representaion of a listable set, WE CAN construct corresponding Diophantine equation.*

DPRM after Davis–Putnam–Robinson–Matiyasevich

Corollary of DPRM Theorem

Theorem. *Hilbert's tenth problem is undecidable.*

Corollary of DPRM Theorem

Theorem. *Hilbert's tenth problem is undecidable.*

Proof. Take an listable set $\mathfrak{M}$ of natural numbers which is undecidable and consider its Diophantine representation:

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

WE CANNOT, given a value of a, algorithmically decide whether equation

$$P_{\mathfrak{M}}(a, x_1, \ldots, x_m) = 0$$

has a solution.

Listing Diophantine Equations

WE CAN list all n-parametric Diophantine equations:

$$P_1(a_1, \ldots, a_n, x_1, \ldots) = 0, \ldots, P_k(a_1, \ldots, a_n, x_1, \ldots) = 0, \ldots$$

Listing Diophantine Equations

WE CAN list all n-parametric Diophantine equations:

$$P_1(a_1, \ldots, a_n, x_1, \ldots) = 0, \ldots, P_k(a_1, \ldots, a_n, x_1, \ldots) = 0, \ldots$$

$$\langle a_1, \ldots, a_n, k \rangle \in \mathfrak{U}_n \Leftrightarrow \exists x_1 \ldots \{P_k(a_1, \ldots, a_n, x_1, \ldots) = 0\}$$

Listing Diophantine Equations

WE CAN list all n-parametric Diophantine equations:

$$P_1(a_1, \ldots, a_n, x_1, \ldots) = 0, \ldots, P_k(a_1, \ldots, a_n, x_1, \ldots) = 0, \ldots$$

$$\langle a_1, \ldots, a_n, k \rangle \in \mathfrak{U}_n \Leftrightarrow \exists x_1 \ldots \{P_k(a_1, \ldots, a_n, x_1, \ldots) = 0\}$$

$$\langle a_1, \ldots, a_n, k \rangle \in \mathfrak{U} \Leftrightarrow \exists y_1 \ldots y_n \{U_n(a_1, \ldots, a_n, k, y_1, \ldots, y_{M_n}) = 0\}$$

Listing Diophantine Equations

WE CAN list all n-parametric Diophantine equations:

$$P_1(a_1, \ldots, a_n, x_1, \ldots) = 0, \ldots, P_k(a_1, \ldots, a_n, x_1, \ldots) = 0, \ldots$$

$$\langle a_1, \ldots, a_n, k \rangle \in \mathfrak{U}_n \Leftrightarrow \exists x_1 \ldots \{P_k(a_1, \ldots, a_n, x_1, \ldots) = 0\}$$

$$\langle a_1, \ldots, a_n, k \rangle \in \mathfrak{U} \Leftrightarrow \exists y_1 \ldots y_n \{U_n(a_1, \ldots, a_n, k, y_1, \ldots, y_{M_n}) = 0\}$$

$$\exists x_1 \ldots \{P_k(a_1, \ldots, a_n, x_1, \ldots) = 0\} \Leftrightarrow \exists y_1 \ldots y_n \{U_n(a_1, \ldots, a_n, k, y_1, \ldots, y_{M_n}) = 0\}$$

Universal Diophantine Equations

For every n WE CAN construct an equation

$$U_n(a_1, \ldots, a_n, k, y_1, \ldots, y_{M_n}) = 0$$

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

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

WE 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

$$U_n(a_1, \ldots, a_n, k_P, y_1, \ldots, y_{M_n}) = 0$$

has a solution in $y_1, \ldots, y_{M_n}$.

Universal Diophantine Equations

For every n WE CAN construct an equation

$$U_n(a_1, \ldots, a_n, k, y_1, \ldots, y_{M_n}) = 0$$

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

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

WE 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

$$U_n(a_1, \ldots, a_n, k_P, y_1, \ldots, y_{M_n}) = 0$$

has a solution in $y_1, \ldots, y_{M_n}$.

Thus the traditional classifications of difficulties of Diophantine equations ("equations of degree 1", "equations of degree 2", ..., and "equations in 1 unknown", "equations in 2 unknowns", ...) collapse from some point on.

Current Records

WE CAN reduce solving an arbitrary parametric Diophantine equation to solving another Diophantine equation (with the same parameters) of degree D in M unknowns (ranging over natural numbers) where $\langle D, M \rangle$ is any of the following pairs:

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

Current Records

WE CAN reduce solving an arbitrary parametric Diophantine equation to solving another Diophantine equation (with the same parameters) of degree D in M unknowns (ranging over natural numbers) where $\langle D, M\rangle$ is any of the following pairs:

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

The above bounds are uniform with respect to the number of parameters provided that D is the degree with respect to unknonws only.

Current Records

WE CAN reduce solving an arbitrary parametric Diophantine equation to solving another Diophantine equation (with the same parameters) of degree D in M unknowns (ranging over natural numbers) where $\langle D, M\rangle$ is any of the following pairs:

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

The above bounds are uniform with respect to the number of parameters provided that D is the degree with respect to unknonws only.

Open Problem. *Are there similar uniform bounds with respect to the total (both in the parameters and unknonws) degree?*

Systems of Equations in 4 Unknowns

Theorem (Matiyasevich [1972]) *Given any Diophantine equation* $P(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$ *WE CAN construct an equivalent system of Diophantine equations of the form*

$$\begin{aligned} Q_1(a_1, \ldots, a_m, w, x_1, y_1) &= z_1 \\ &\vdots \\ Q_M(a_1, \ldots, a_m, w, x_M, y_M) &= z_M \end{aligned}$$

with $w, x_1, y_1, z_1, \ldots, x_M, y_M, z_m$ ranging over natural numbers.

Systems of Equations in 4 Unknowns

Theorem (Matiyasevich [1972]) *Given any Diophantine equation* $P(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$ *WE CAN construct an equivalent system of Diophantine equations of the form*

$$\begin{aligned} Q_1(a_1, \ldots, a_m, w, x_1, y_1) &= z_1 \\ &\vdots \\ Q_M(a_1, \ldots, a_m, w, x_M, y_M) &= z_M \end{aligned}$$

with $w, x_1, y_1, z_1, \ldots, x_M, y_M, z_m$ ranging over natural numbers.

Corollary. WE CANNOT algorithmically decide whether given system of Diophantine equations of the form

$$\begin{aligned} Q_1(w, x_1, y_1) &= z_1 \\ &\vdots \\ Q_M(w, x_M, y_M) &= z_M \end{aligned}$$

has a solution in natural numbers.

Decidable cases

WE CAN algorithmically decide whether a Diophantine equation in 1 unknown has a solution in integers or in natural numbers or in rational numbers.

Decidable cases

WE CAN algorithmically decide whether a Diophantine equation in 1 unknown has a solution in integers or in natural numbers or in rational numbers.

WE CAN algorithmically decide whether a Diophantine equation of degree 1 has a solution in integers or in natural numbers or in rational numbers.

Decidable cases

WE CAN algorithmically decide whether a Diophantine equation in 1 unknown has a solution in integers or in natural numbers or in rational numbers.

WE CAN algorithmically decide whether a Diophantine equation of degree 1 has a solution in integers or in natural numbers or in rational numbers.

Theorem (Carl Ludwig Siegel [1972]). WE CAN algorithmically decide whether a Diophantine equation of degree 2 has a solution in integers.

Decidable cases

WE CAN algorithmically decide whether a Diophantine equation in 1 unknown has a solution in integers or in natural numbers or in rational numbers.

WE CAN algorithmically decide whether a Diophantine equation of degree 1 has a solution in integers or in natural numbers or in rational numbers.

Theorem (Carl Ludwig Siegel [1972]). WE CAN algorithmically decide whether a Diophantine equation of degree 2 has a solution in integers.

Theorem (Fritz Grunewald and Daniel Segal [2004]).
WE CAN algorithmically decide whether a Diophantine equation of degree 2 has a solution in natural numbers.

$1 000 000 Diophantine Equation

A "Millenium Problem" (Clay Mathematics Institute) $\mathrm{P} \stackrel{?}{=} \mathrm{NP}$

$1 000 000 Diophantine Equation

A "Millenium Problem" (Clay Mathematics Institute) $\mathrm{P} \stackrel{?}{=} \mathrm{NP}$

Computational Problem

- INPUT: Natural numbers $a,\ b,\ c$.
- QUESTION: Has equation $ax^2 + by = c$ solutions in integers x and y?

$1 000 000 Diophantine Equation

A "Millenium Problem" (Clay Mathematics Institute) $\mathrm{P} \stackrel{?}{=} \mathrm{NP}$

Computational Problem

- INPUT: Natural numbers $a,\ b,\ c$.
- QUESTION: Has equation $ax^2 + by = c$ solutions in integers x and y?

Theorem (Leonard M. Adleman and Kenneth Manders [1976]) *The above problem is NP-complete.*

$1 000 000 Diophantine Equation

A "Millenium Problem" (Clay Mathematics Institute) $\mathrm{P} \stackrel{?}{=} \mathrm{NP}$

Computational Problem

- INPUT: Natural numbers $a,\ b,\ c$.
- QUESTION: Has equation $ax^2 + by = c$ solutions in integers x and y?

Theorem (Leonard M. Adleman and Kenneth Manders [1976]) *The above problem is NP-complete.*

$\mathbf{P} \stackrel{?}{=} \mathbf{NP}$: *CAN WE answer the above QUESTION in a fast way, namely by performing $O(\log(a+b+c)^m)$ elementary operations for some fixed value of m?*

$1 000 000 Diophantine Equation

A "Millenium Problem" (Clay Mathematics Institute) $\mathrm{P} \stackrel{?}{=} \mathrm{NP}$

Computational Problem

- INPUT: Natural numbers $a,\ b,\ c$.
- QUESTION: Has equation $ax^2 + by = c$ solutions in integers x and y?

Theorem (Leonard M. Adleman and Kenneth Manders [1976]) *The above problem is NP-complete.*

$\mathrm{P} \stackrel{?}{=} \mathrm{NP}$: *CAN WE answer the above QUESTION in a fast way, namely by performing $O(\log(a+b+c)^m)$ elementary operations for some fixed value of m?*

ONE CAN earn $1 000 000 either by finding such an algorithm or by proving that such an algorithm is impossible.

The Set of All Primes

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*

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

Goldbach's conjecture

Every even integer greater than 2 is the sum of two prime numbers.

Goldbach's conjecture

Every even integer greater than 2 is the sum of two prime numbers.

The set $\mathfrak{M}$ of *counterexamples* to Goldbach's conjecture (i.e., even numbers greater than 2 not being the sum of two primes) is listable

Goldbach's conjecture

Every even integer greater than 2 is the sum of two prime numbers.

The set $\mathfrak{M}$ of *counterexamples* to Goldbach's conjecture (i.e., even numbers greater than 2 not being the sum of two primes) is listable and hence WE CAN construct its Diophantine representation

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

Goldbach's conjecture

Every even integer greater than 2 is the sum of two prime numbers.

The set $\mathfrak{M}$ of *counterexamples* to Goldbach's conjecture (i.e., even numbers greater than 2 not being the sum of two primes) is listable and hence WE CAN construct its Diophantine representation

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

Thus, Goldbach's conjecture is equivalent to the statement that the Diophantine equation

$$G(x_0, x_1, \ldots, x_m) = 0$$

has no solution.

Goldbach's conjecture

Every even integer greater than 2 is the sum of two prime numbers.

The set $\mathfrak{M}$ of *counterexamples* to Goldbach's conjecture (i.e., even numbers greater than 2 not being the sum of two primes) is listable and hence WE CAN construct its Diophantine representation

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

Thus, Goldbach's conjecture is equivalent to the statement that the Diophantine equation

$$G(x_0, x_1, \ldots, x_m) = 0$$

has no solution.

So, a positive solution of Hilbert's 10th problem in it original form would allow us to know whether Goldbach's conjecture is true or not.

Another $1 000 000 Diophantine Equation

A "Millenium Problem": The Riemann hypothesis

Another $1 000 000 Diophantine Equation

A "Millenium Problem": The Riemann hypothesis

WE CAN construct a particular Diophantine equation

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

which has no solution if and only if the Riemann hypothesis is true.

Another $1 000 000 Diophantine Equation

A "Millenium Problem": The Riemann hypothesis

WE CAN construct a particular Diophantine equation

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

which has no solution if and only if the Riemann hypothesis is true.

ONE CAN earn $1 000 000 by proving that the above equation has no solution.

Another $1 000 000 Diophantine Equation

A "Millenium Problem": The Riemann hypothesis

WE CAN construct a particular Diophantine equation

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

which has no solution if and only if the Riemann hypothesis is true.

ONE CAN earn $1 000 000 by proving that the above equation has no solution.

ATTENTION! No prize is promised for refuting the Riemann hypothesis, that is, for finding a solution of the above equation.

Exponential Diophantine representations

DPRM Theorem [1970]. *For every listable set is Diophantine*
WE CAN construct its Diophantine representation.

Exponential Diophantine representations

DPRM Theorem [1970]. *For every listable set is Diophantine WE CAN construct its Diophantine representation.*

DPR Theorem [1961]. For every listable set is Diophantine WE CAN construct an exponential Diophantine repesentation, 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.

The Number of Unknowns

Theorem (James Jones and Yuri Matiyasevich [1982]).
WE CAN reduce solving an arbitrary parametric exponential Diophantine equation to solving an exponential Diophantine equation (with the same parameters) of the form

$$E_{\mathrm{L}}(a_1, \ldots, a_n, x, y, z) \;=\; E_{\mathrm{R}}(a_1, \ldots, a_n, x, y, z)$$

where E_{L} and E_{R} are expression constructed by traditional rules from the variables and particular positive integers by addition, multiplication and unary exponentiation 2^w.

The Number of Unknowns

Theorem (James Jones and Yuri Matiyasevich [1982]).
WE CAN reduce solving an arbitrary parametric exponential Diophantine equation to solving an exponential Diophantine equation (with the same parameters) of the form

$$E_{\mathrm{L}}(a_1, \ldots, a_n, x, y, z) \;=\; E_{\mathrm{R}}(a_1, \ldots, a_n, x, y, z)$$

where E_{L} and E_{R} are expression constructed by traditional rules from the variables and particular positive integers by addition, multiplication and unary exponentiation 2^w.

Thus WE CANNOT algorithmically decide whether an arbitrary unary (base 2) exponential Diophantine equation with 3 unknowns $E_{\mathrm{L}}(x, y, z) \;=\; E_{\mathrm{R}}(x, y, z)$ has solution.

The Number of Unknowns

Theorem (James Jones and Yuri Matiyasevich [1982]). WE CAN reduce solving an arbitrary parametric exponential Diophantine equation to solving an exponential Diophantine equation (with the same parameters) of the form

$$E_{\mathrm{L}}(a_1, \ldots, a_n, x, y, z) \;=\; E_{\mathrm{R}}(a_1, \ldots, a_n, x, y, z)$$

where E_{L} and E_{R} are expression constructed by traditional rules from the variables and particular positive integers by addition, multiplication and unary exponentiation 2^w.

Thus WE CANNOT algorithmically decide whether an arbitrary unary (base 2) exponential Diophantine equation with 3 unknowns $E_{\mathrm{L}}(x, y, z) \;=\; E_{\mathrm{R}}(x, y, z)$ has solution.

Theorem (Hilbert Levitz [1985]). WE CAN algorithmically decide whether an arbitrary unary (base 2) exponential Diophantine equation with 1 unknown $E_{\mathrm{L}}(x) \;=\; E_{\mathrm{R}}(x)$ has solution.

Single- and finite-fold representations

An existential representation of a set

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

is called single-fold if for every n-tuple $\langle a_1, \ldots, a_n \rangle$ there is at most one m-tuple $\langle x_1, \ldots, x_m \rangle$ giving a solution of the equation.

Single- and finite-fold representations

An existential representation of a set

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

is called single-fold if for every n-tuple $\langle a_1, \ldots, a_n \rangle$ there is at most one m-tuple $\langle x_1, \ldots, x_m \rangle$ giving a solution of the equation.

Respectively, a representation is called finite-fold if there only finitely many m-tuples $\langle x_1, \ldots, x_m \rangle$ giving solutions of the equation.

Another Open Problem

DPRM-theorem [1970]. For every listable set WE CAN construct a Diophantine representation.

DPR-theorem [1961]. For every listable set WE CAN construct an exponential Diophantine repesentation

Another Open Problem

DPRM-theorem [1970]. For every listable set WE CAN construct a Diophantine representation.

Matiyasevich [1974]. For every listable set WE CAN construct a single-fold exponential Diophantine representation.

DPR-theorem [1961]. For every listable set WE CAN construct an exponential Diophantine repesentation

Another Open Problem

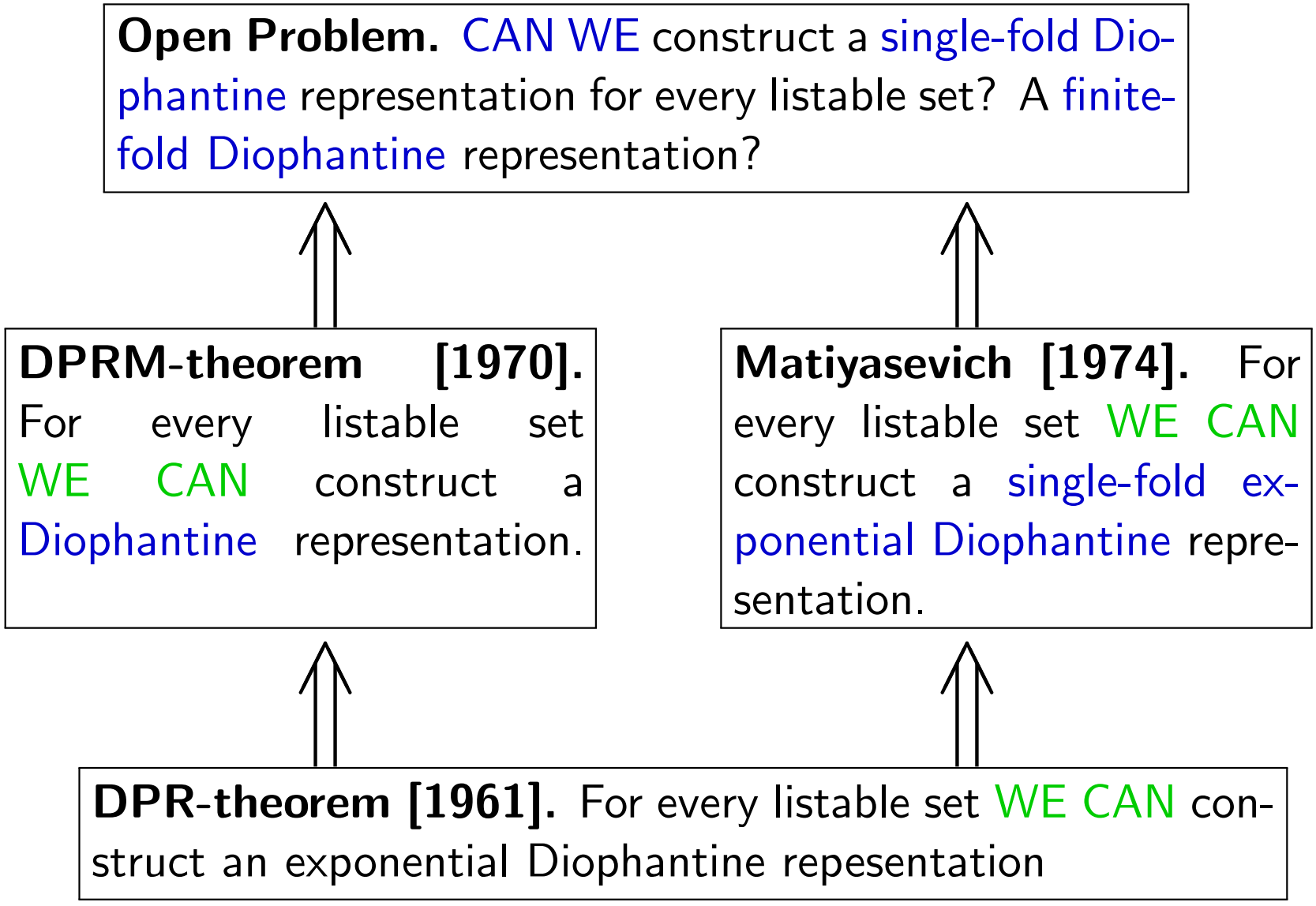
Open Problem. CAN WE construct a single-fold Diophantine representation for every listable set?

DPRM-theorem [1970]. For every listable set WE CAN construct a Diophantine representation.

Matiyasevich [1974]. For every listable set WE CAN construct a single-fold exponential Diophantine representation.

DPR-theorem [1961]. For every listable set WE CAN construct an exponential Diophantine repesentation

Another Open Problem



Restriction of the Usage of Exponentiation

Theorem (Yuri Matiyasevich [1974]). For every listable set $\mathfrak{M}$ WE CAN construct a single-fold exponential Diophantine representation of the form

$$\langle a_1, \ldots, a_n \rangle \in \mathfrak{M} \Longleftrightarrow$$
$$\exists x_1 \ldots x_m \{ P(a_1, \ldots, a_n, x_1, \ldots, x_m) = y + 4^y \}$$

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

Impossibility of Effectivization

Let

$$E_{\mathrm{L}}(a, x, y, z) \;=\; E_{\mathrm{R}}(a, x, y, z)$$

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

Impossibility of Effectivization

Let

$$E_{\mathrm{L}}(a, x, y, z) \;=\; E_{\mathrm{R}}(a, x, y, z)$$

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

- WE CAN bound the number of solutions for any value of the parameter a

Impossibility of Effectivization

Let

$$E_{\mathrm{L}}(a, x, y, z) \;=\; E_{\mathrm{R}}(a, x, y, z)$$

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

- WE CAN bound the number of solutions for any value of the parameter a by 1;

Impossibility of Effectivization

Let

$$E_{\mathrm{L}}(a, x, y, z) \;=\; E_{\mathrm{R}}(a, x, y, z)$$

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

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

Impossibility of Effectivization

Let

$$E_{\mathrm{L}}(a, x, y, z) \;=\; E_{\mathrm{R}}(a, x, y, z)$$

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

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

The above equation is non-effectivizable in priciple.

Impossibility of Effectivization

Let

$$E_{\mathrm{L}}(a, x, y, z) \;=\; E_{\mathrm{R}}(a, x, y, z)$$

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

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

The above equation is non-effectivizable in priciple.

Open problem. *CAN WE construct non-effectivizable genuine Diophantine equation?*

Archiving Diophantine Sets

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

Archiving Diophantine Sets

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

$$B = b_1 \ldots b_k \ldots \qquad b_k = \begin{cases} 1, & \text{if } k \in \mathfrak{M} \\ 0 & \text{otherwise} \end{cases}$$

Archiving Diophantine Sets

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

$$B = b_1 \ldots b_k \ldots \qquad b_k = \begin{cases} 1, & \text{if } k \in \mathfrak{M} \\ 0 & \text{otherwise} \end{cases}$$

$$B_n = b_1 \ldots b_k \ldots b_n$$

Archiving Diophantine Sets

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

$$B = b_1 \ldots b_k \ldots \qquad b_k = \begin{cases} 1, & \text{if } k \in \mathfrak{M} \\ 0 & \text{otherwise} \end{cases}$$

$$B_n = b_1 \ldots b_k \ldots b_n$$

Archiving Diophantine Sets

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

$$B = b_1 \ldots b_k \ldots \qquad b_k = \begin{cases} 1, & \text{if } k \in \mathfrak{M} \\ 0 & \text{otherwise} \end{cases}$$

$$B_n = b_1 \ldots b_k \ldots b_n$$

Alice Bob

Archiving Diophantine Sets

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

$$B = b_1 \ldots b_k \ldots \qquad b_k = \begin{cases} 1, & \text{if } k \in \mathfrak{M} \\ 0 & \text{otherwise} \end{cases}$$

$$B_n = b_1 \ldots b_k \ldots b_n$$

Alice

B_n

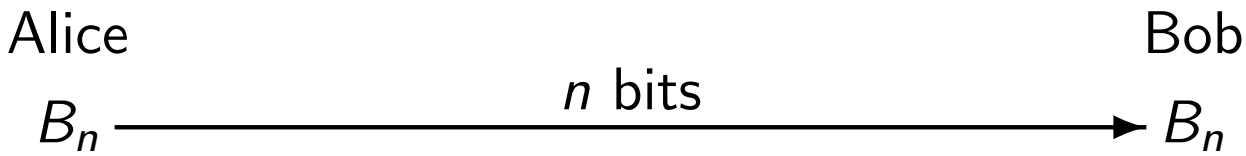
Bob

Archiving Diophantine Sets

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

$$B = b_1 \ldots b_k \ldots \qquad b_k = \begin{cases} 1, & \text{if } k \in \mathfrak{M} \\ 0 & \text{otherwise} \end{cases}$$

$$B_n = b_1 \ldots b_k \ldots b_n$$

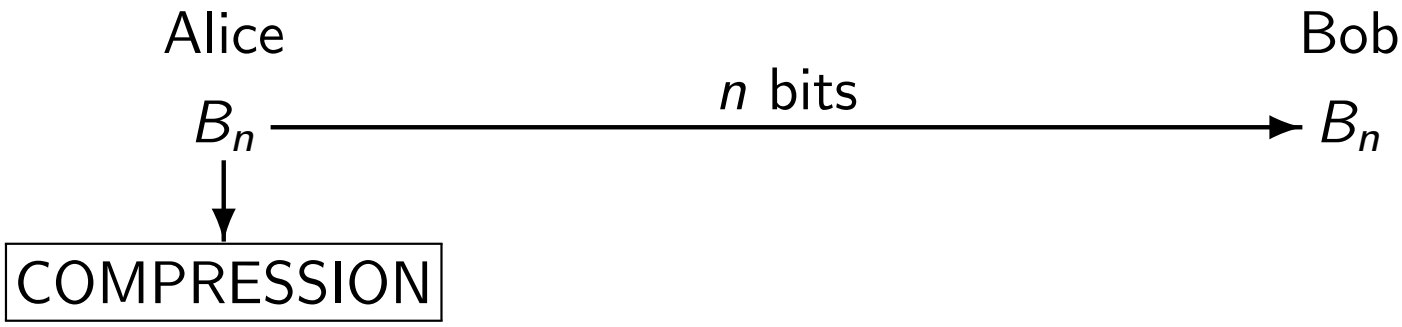


Archiving Diophantine Sets

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

$$B = b_1 \ldots b_k \ldots \qquad b_k = \begin{cases} 1, & \text{if } k \in \mathfrak{M} \\ 0 & \text{otherwise} \end{cases}$$

$$B_n = b_1 \ldots b_k \ldots b_n$$

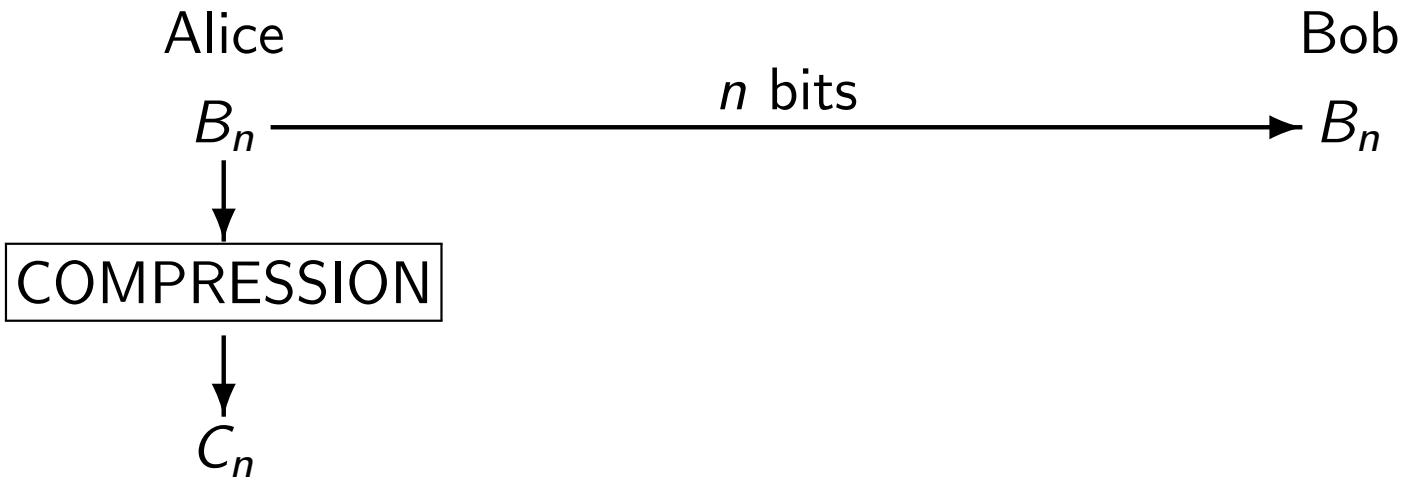


Archiving Diophantine Sets

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

$$B = b_1 \ldots b_k \ldots \qquad b_k = \begin{cases} 1, & \text{if } k \in \mathfrak{M} \\ 0 & \text{otherwise} \end{cases}$$

$$B_n = b_1 \ldots b_k \ldots b_n$$

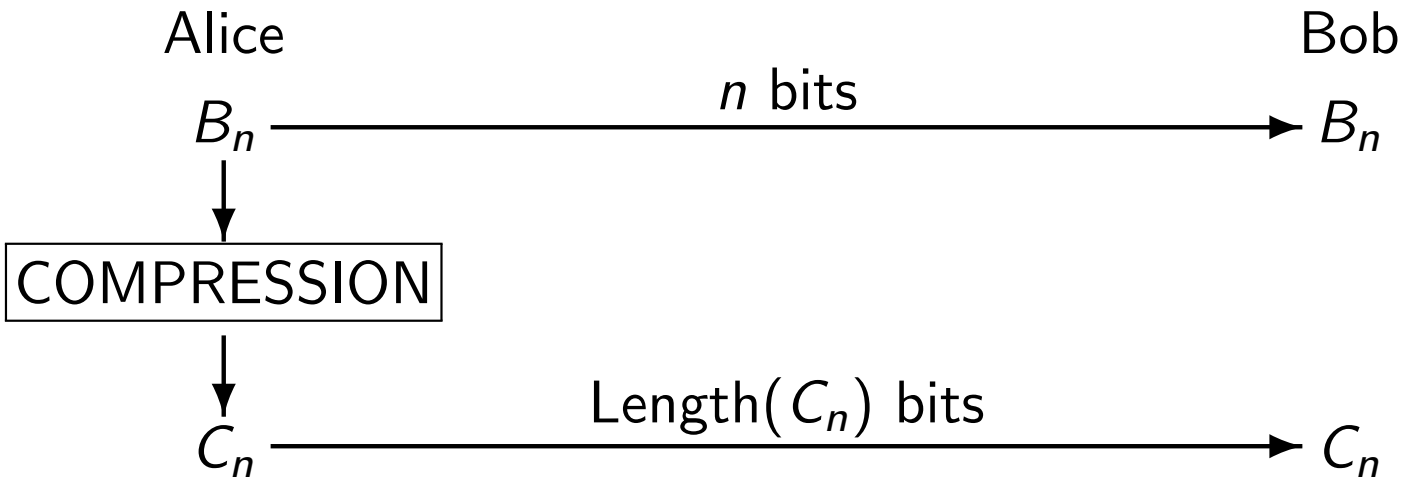


Archiving Diophantine Sets

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

$$B = b_1 \ldots b_k \ldots \qquad b_k = \begin{cases} 1, & \text{if } k \in \mathfrak{M} \\ 0 & \text{otherwise} \end{cases}$$

$$B_n = b_1 \ldots b_k \ldots b_n$$

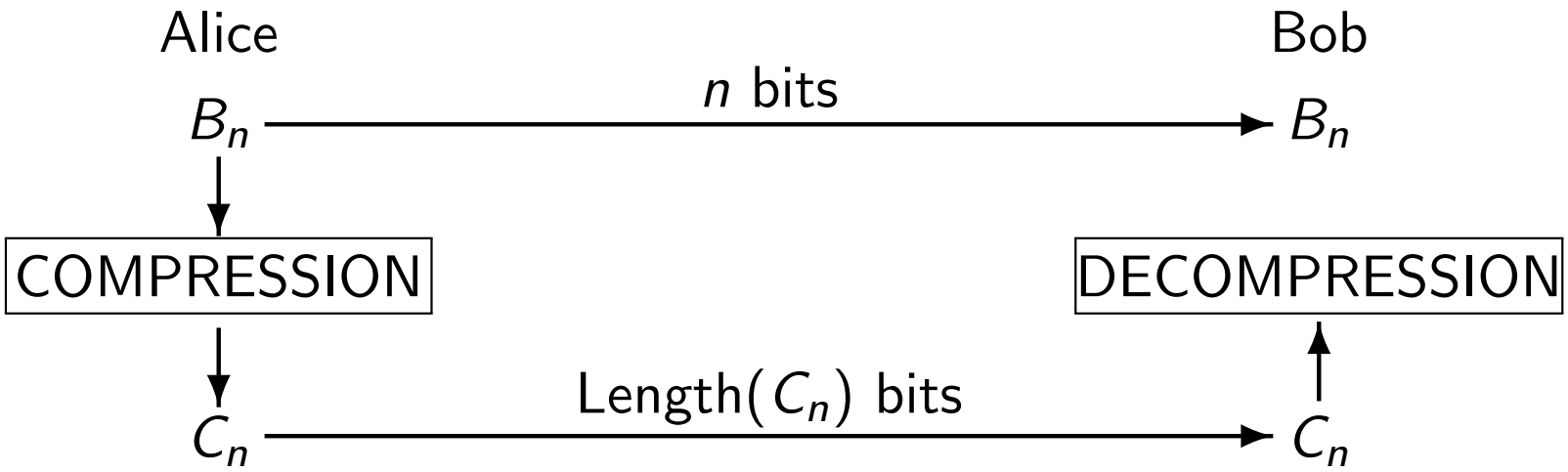


Archiving Diophantine Sets

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

$$B = b_1 \ldots b_k \ldots \qquad b_k = \begin{cases} 1, & \text{if } k \in \mathfrak{M} \\ 0 & \text{otherwise} \end{cases}$$

$$B_n = b_1 \ldots b_k \ldots b_n$$

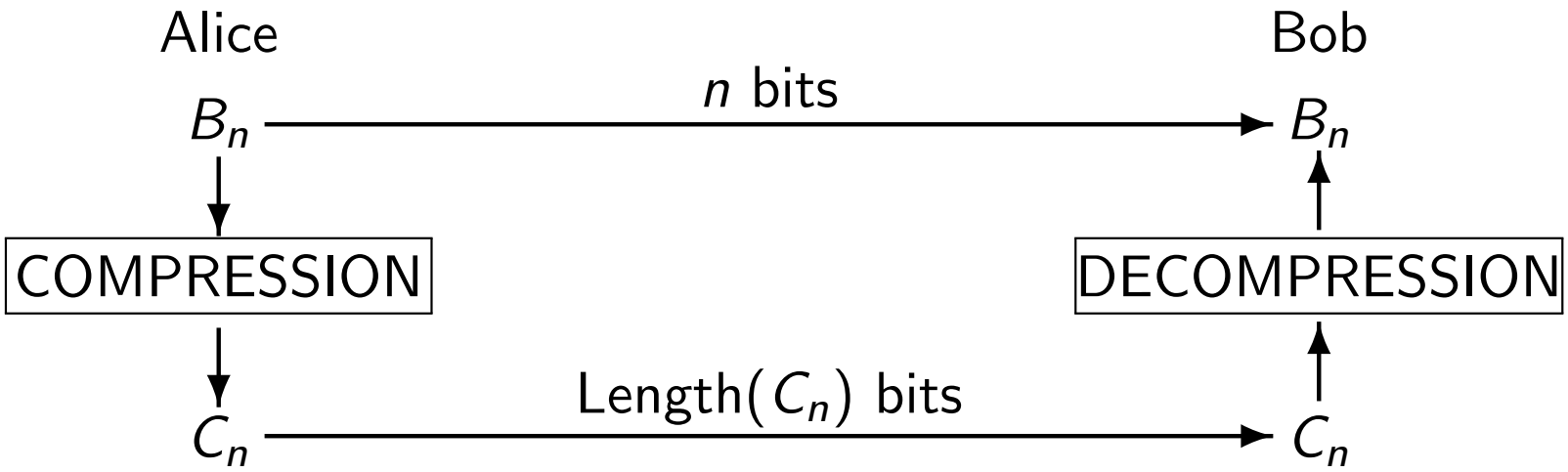


Archiving Diophantine Sets

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

$$B = b_1 \ldots b_k \ldots \qquad b_k = \begin{cases} 1, & \text{if } k \in \mathfrak{M} \\ 0 & \text{otherwise} \end{cases}$$

$$B_n = b_1 \ldots b_k \ldots b_n$$

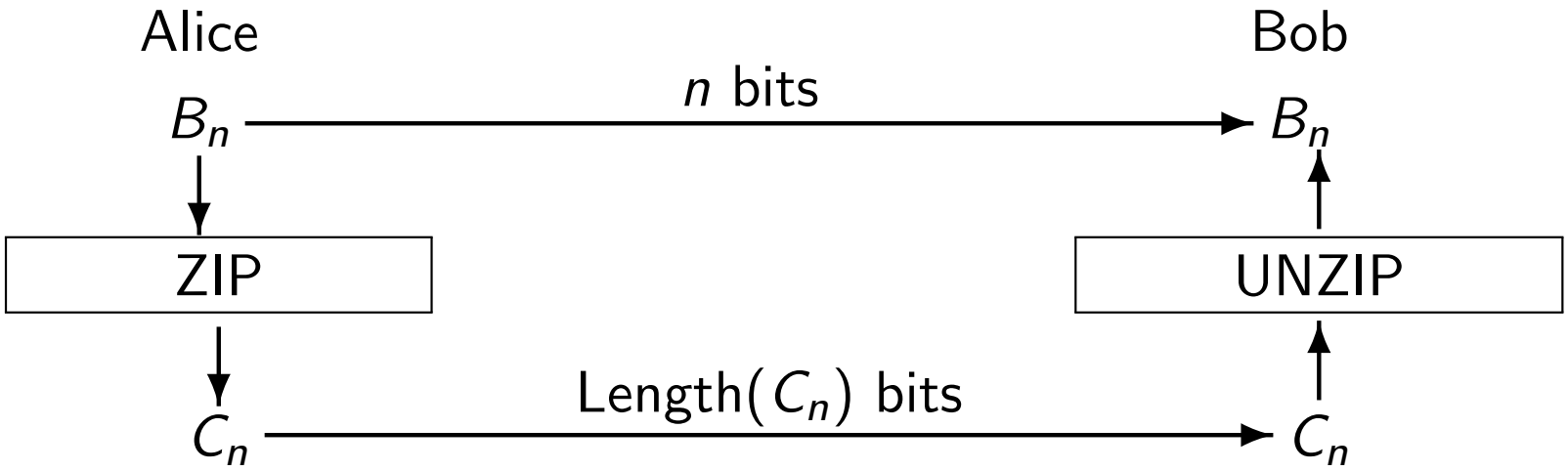


Archiving Diophantine Sets

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

$$B = b_1 \ldots b_k \ldots \qquad b_k = \begin{cases} 1, & \text{if } k \in \mathfrak{M} \\ 0 & \text{otherwise} \end{cases}$$

$$B_n = b_1 \ldots b_k \ldots b_n$$

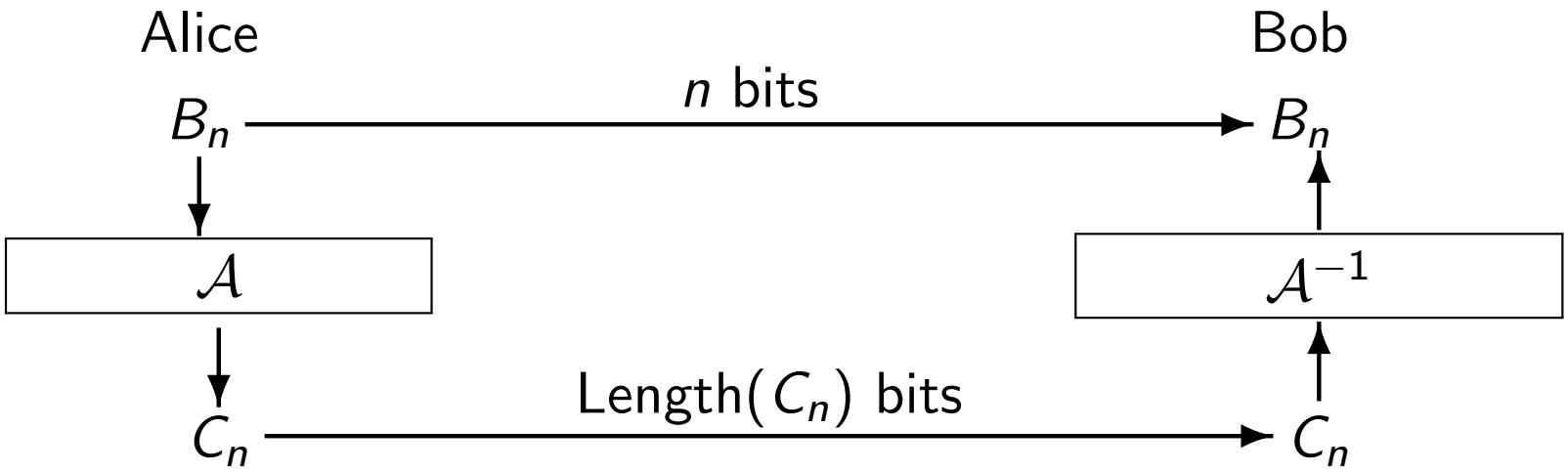


Archiving Diophantine Sets

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

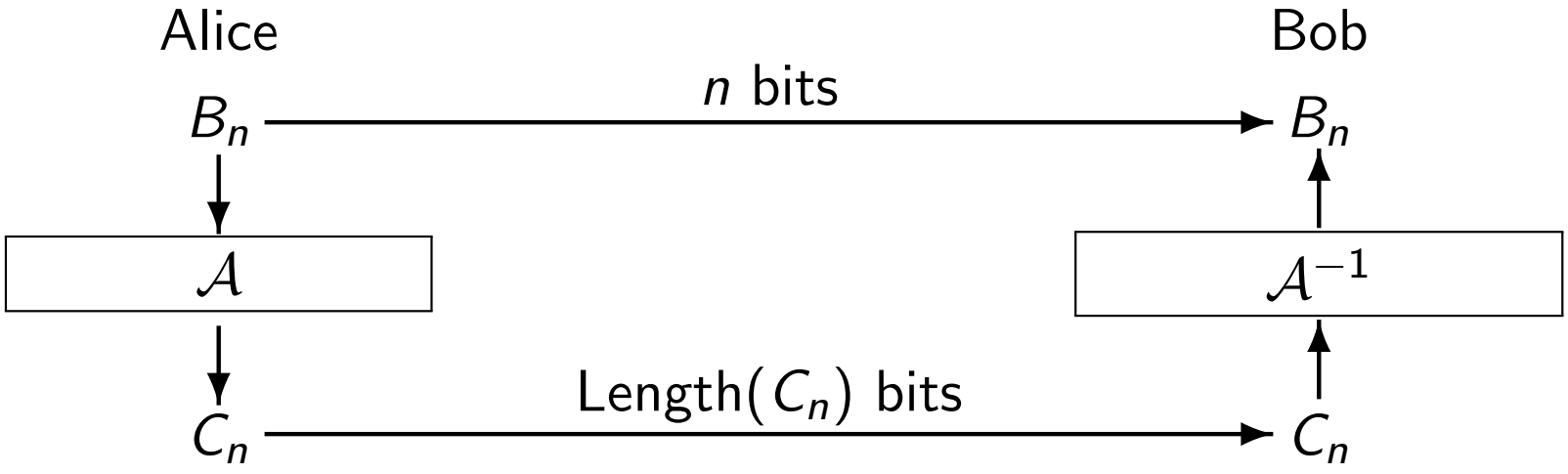
$$B = b_1 \ldots b_k \ldots \qquad b_k = \begin{cases} 1, & \text{if } k \in \mathfrak{M} \\ 0 & \text{otherwise} \end{cases}$$

$$B_n = b_1 \ldots b_k \ldots b_n$$



Saving Constant Number of Bits

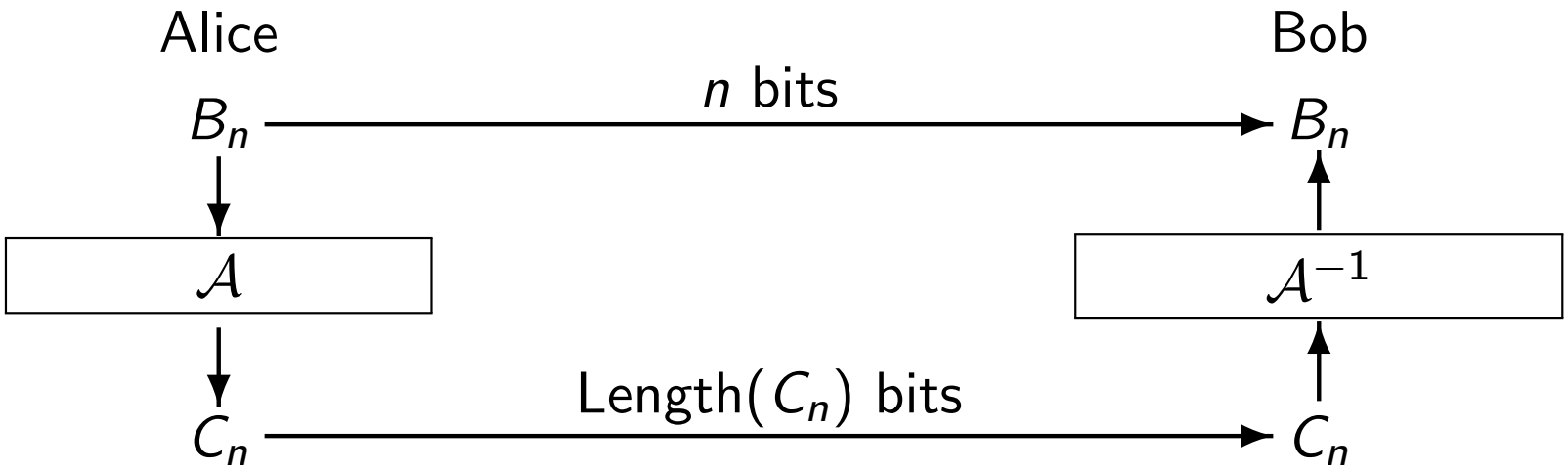
$$B = b_1 \ldots b_k \ldots$$



Saving Constant Number of Bits

$$B = b_1 \dots b_k \dots$$

WE CAN always save any constant number k of bits (for $n > k$):

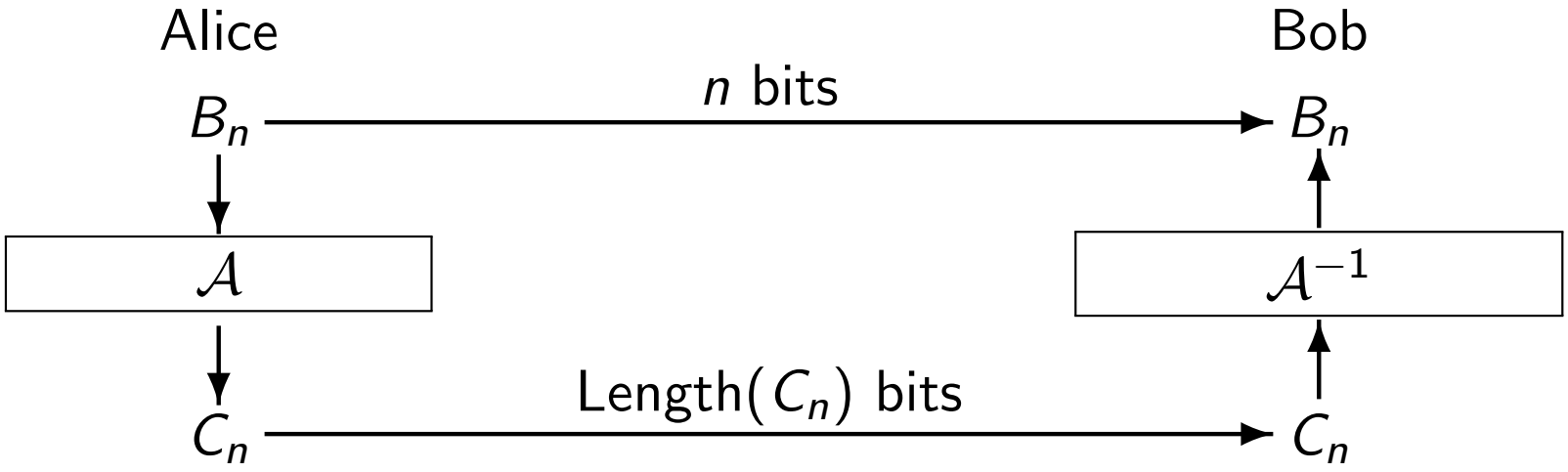


Saving Constant Number of Bits

$$B = b_1 \dots b_k \dots$$

WE CAN always save any constant number k of bits (for $n > k$):

$$C_n = \mathcal{A}(B_n)$$

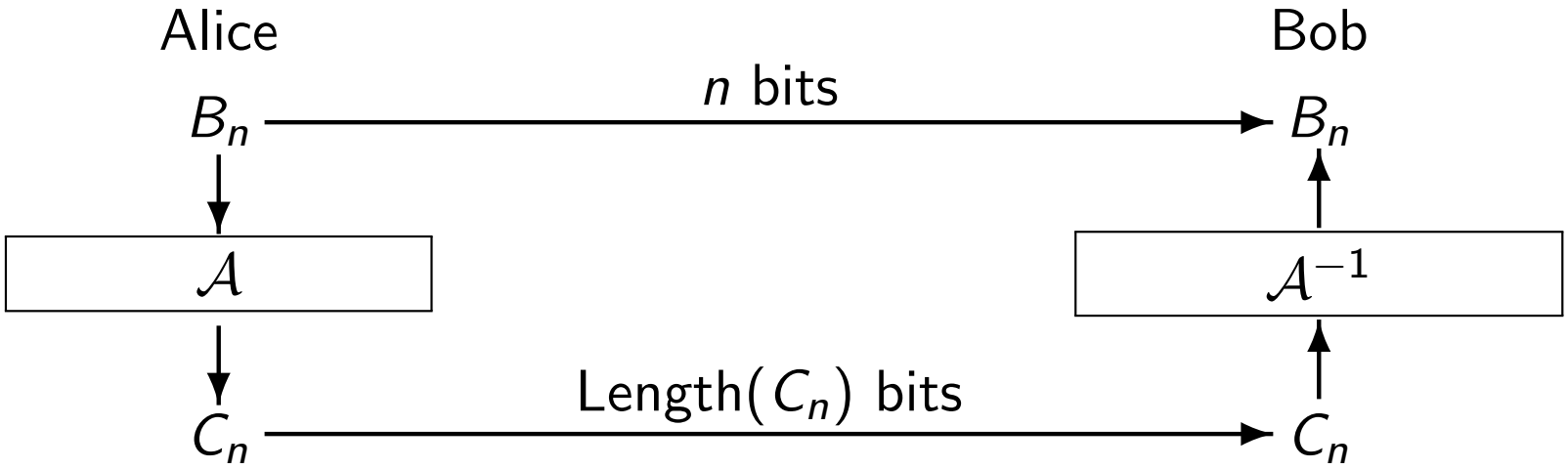


Saving Constant Number of Bits

$$B = b_1 \dots b_k \dots$$

WE CAN always save any constant number k of bits (for $n > k$):

$$C_n = \mathcal{A}(B_n) \quad = \quad \begin{cases} & \text{if } n \leq k+1 \\ & \text{otherwise} \end{cases}$$

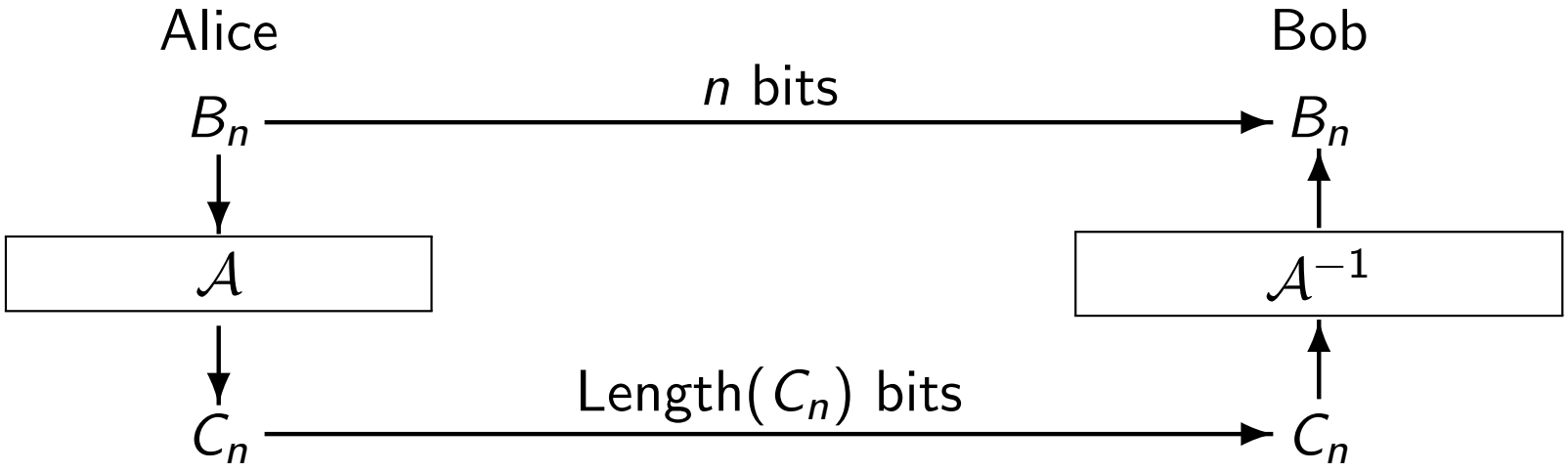


Saving Constant Number of Bits

$$B = b_1 \dots b_k \dots$$

WE CAN always save any constant number k of bits (for $n > k$):

$$C_n = \mathcal{A}(B_n) \quad = \quad \begin{cases} 0B_n & \text{if } n \leq k+1 \\ & \text{otherwise} \end{cases}$$

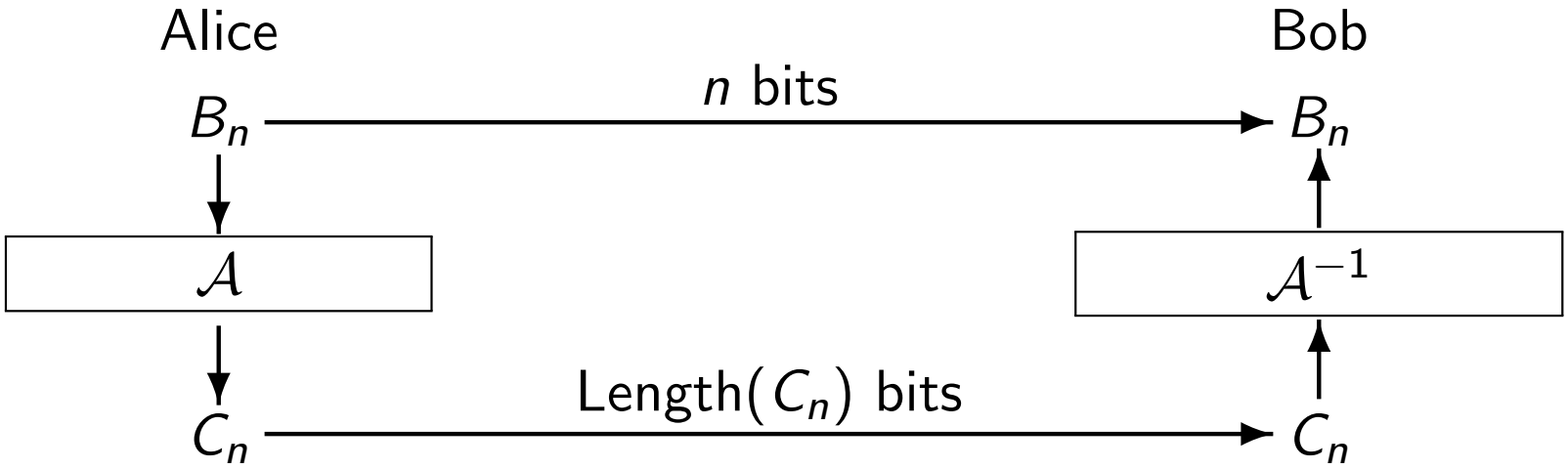


Saving Constant Number of Bits

$$B = b_1 \dots b_k \dots$$

WE CAN always save any constant number k of bits (for $n > k$):

$$C_n = \mathcal{A}(B_n) \quad = \quad \begin{cases} 0B_n & \text{if } n \leq k+1 \\ 1b_{k+2}b_{k+3}\dots b_n & \text{otherwise} \end{cases}$$



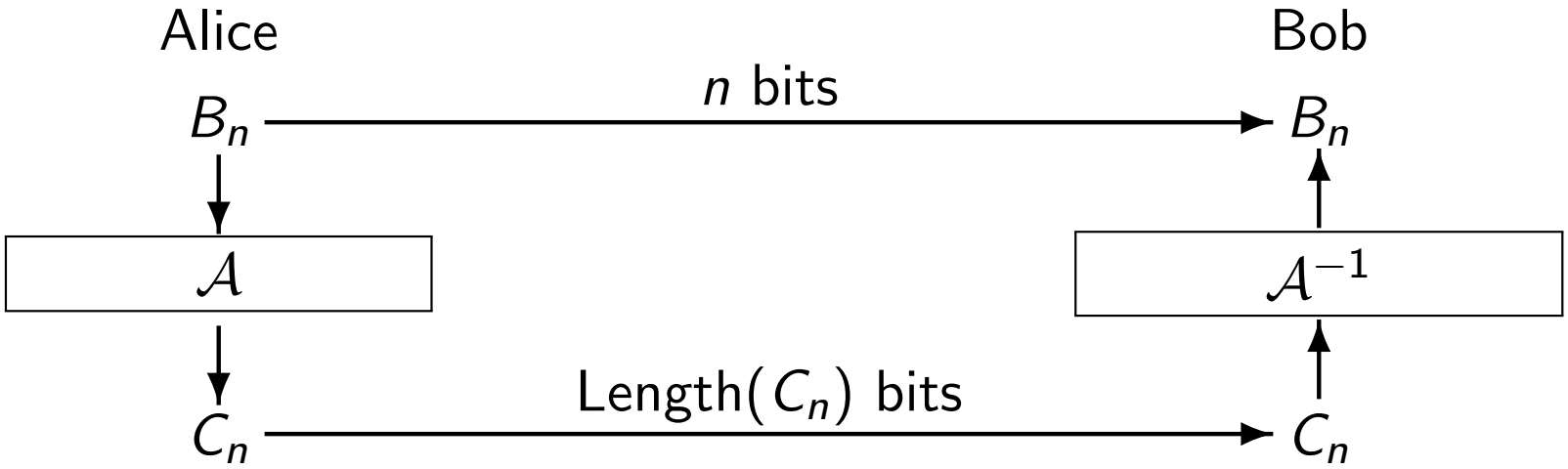
Saving Constant Number of Bits

$$B = b_1 \dots b_k \dots$$

WE CAN always save any constant number k of bits (for $n > k$):

$$C_n = \mathcal{A}(B_n) = \begin{cases} 0B_n & \text{if } n \leq k+1 \\ 1b_{k+2}b_{k+3}\dots b_n & \text{otherwise} \end{cases}$$

$$\mathcal{A}^{-1}(0C) = C$$



Saving Constant Number of Bits

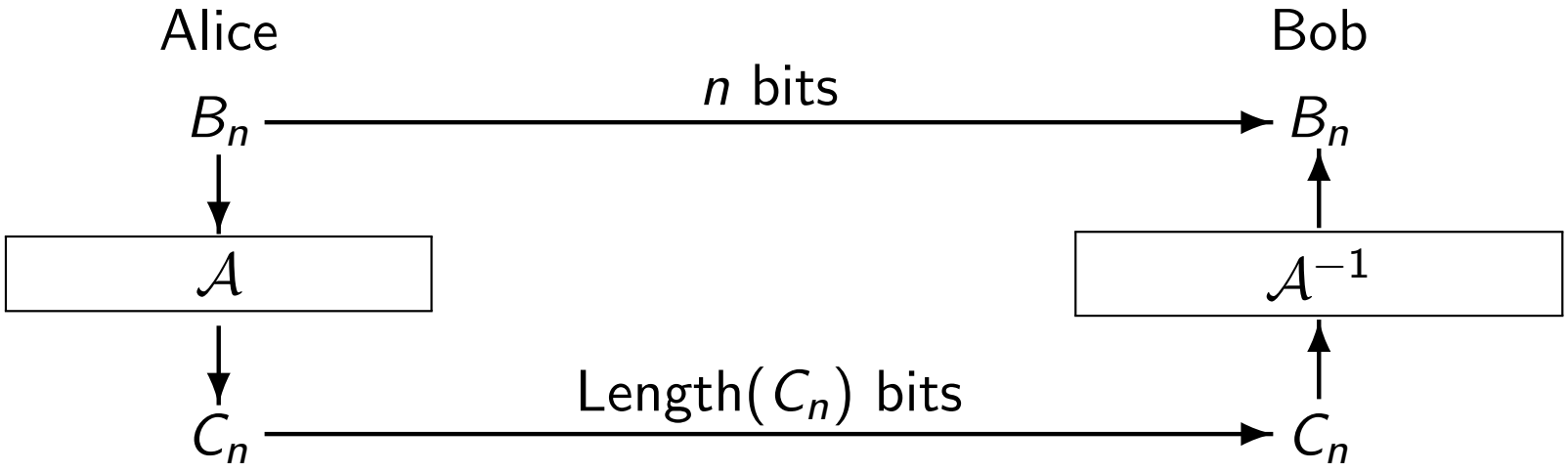
$$B = b_1 \dots b_k \dots$$

WE CAN always save any constant number k of bits (for $n > k$):

$$C_n = \mathcal{A}(B_n) = \begin{cases} 0B_n & \text{if } n \leq k+1 \\ 1b_{k+2}b_{k+3}\dots b_n & \text{otherwise} \end{cases}$$

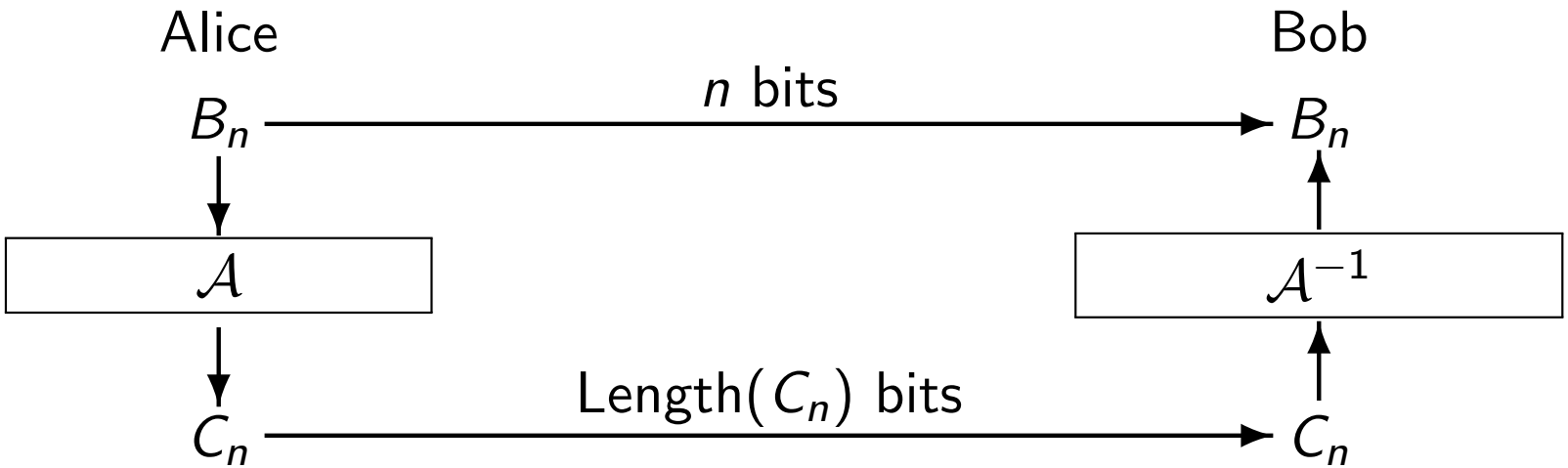
$$\mathcal{A}^{-1}(0C) = C$$

$$\mathcal{A}^{-1}(1C) = b_1 \dots b_{k+1} C$$



Case of Decidable $\mathfrak{M}$

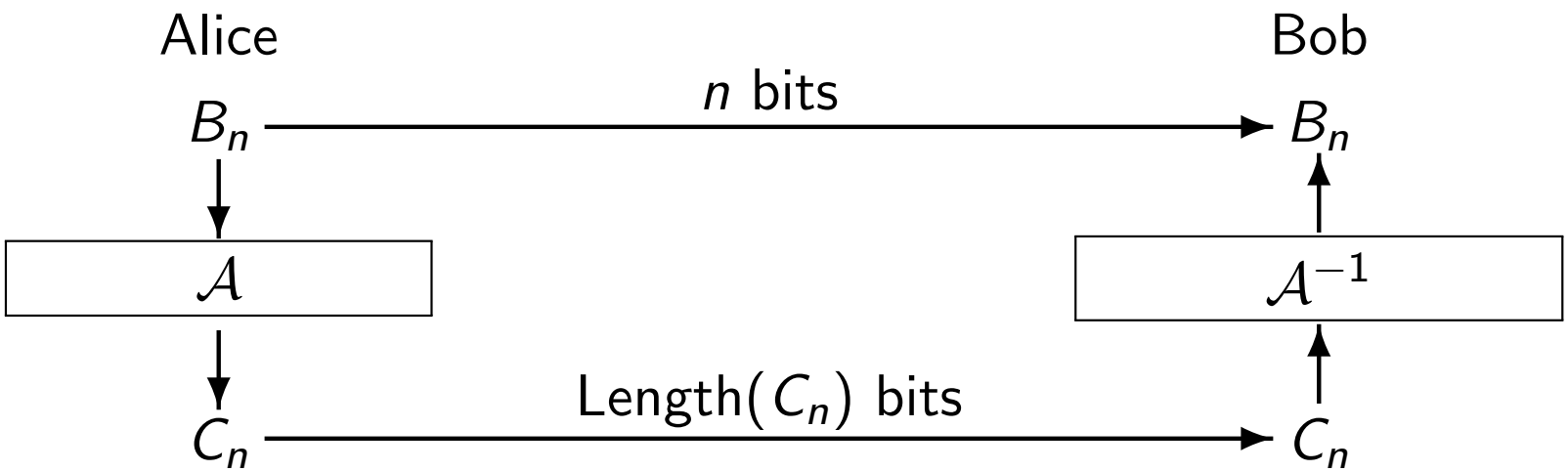
$$B_n = b_1 b_2 \ldots b_k \ldots b_n \qquad b_k = \begin{cases} 1, & \text{if } k \in \mathfrak{M} \\ 0 & \text{otherwise} \end{cases}$$



Case of Decidable $\mathfrak{M}$

$$B_n = b_1 b_2 \ldots b_k \ldots b_n \qquad b_k = \begin{cases} 1, & \text{if } k \in \mathfrak{M} \\ 0 & \text{otherwise} \end{cases}$$

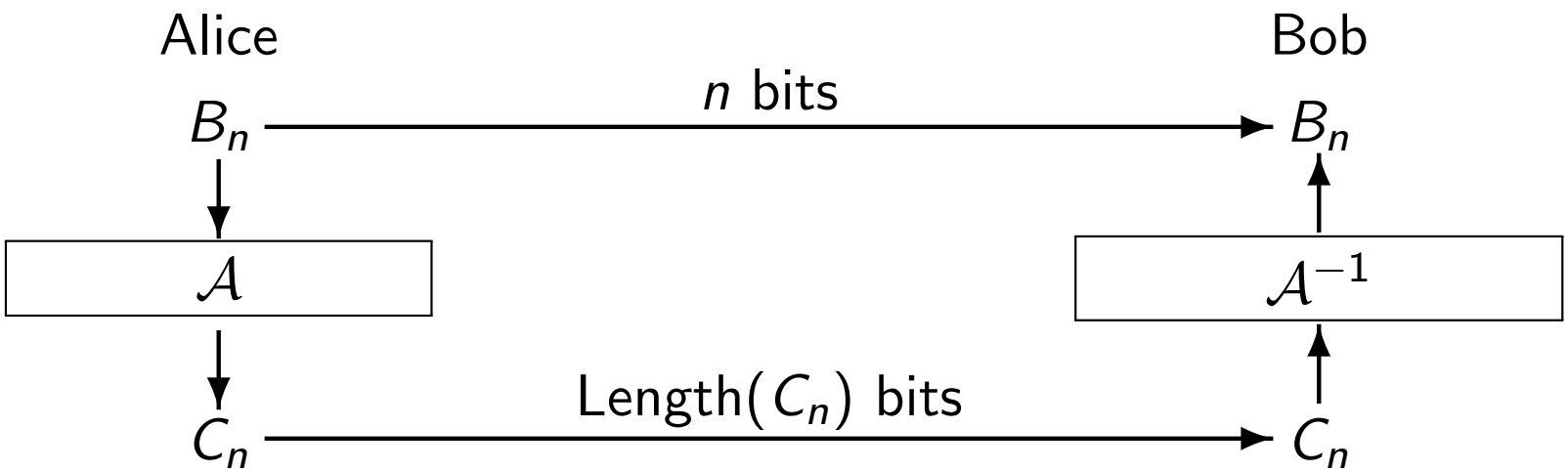
$$C_n = \mathcal{A}(B_n)$$



Case of Decidable $\mathfrak{M}$

$$B_n = b_1 b_2 \ldots b_k \ldots b_n \qquad b_k = \begin{cases} 1, & \text{if } k \in \mathfrak{M} \\ 0 & \text{otherwise} \end{cases}$$

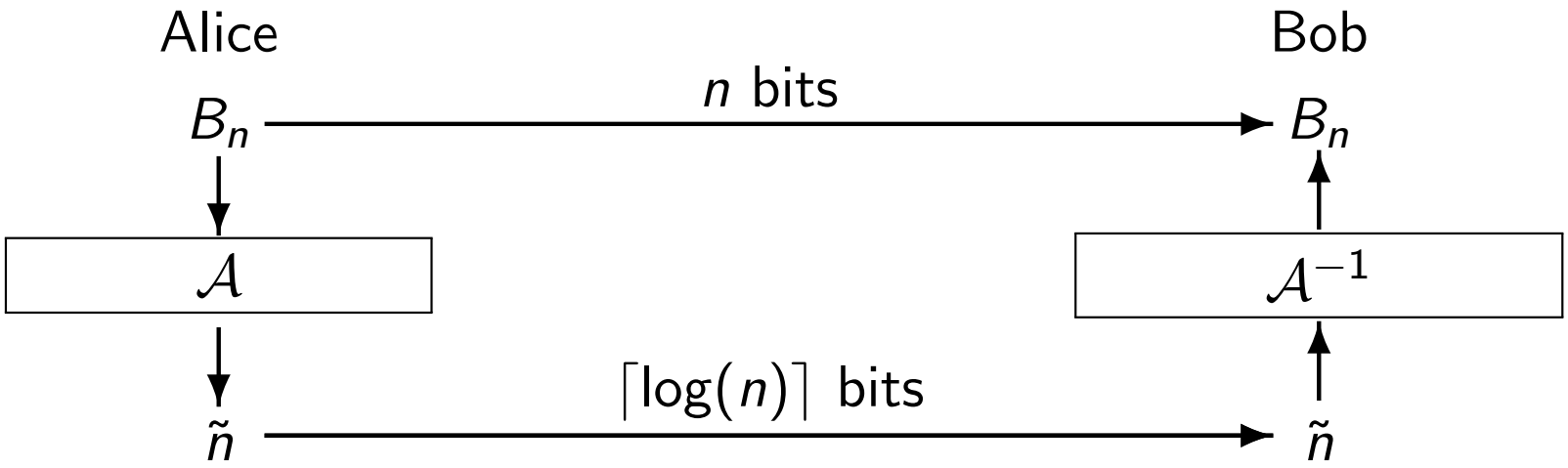
$$C_n = \mathcal{A}(B_n) \quad = \tilde{n} = \text{binary notation of } n$$



Case of Decidable $\mathfrak{M}$

$$B_n = b_1 b_2 \ldots b_k \ldots b_n \qquad b_k = \begin{cases} 1, & \text{if } k \in \mathfrak{M} \\ 0 & \text{otherwise} \end{cases}$$

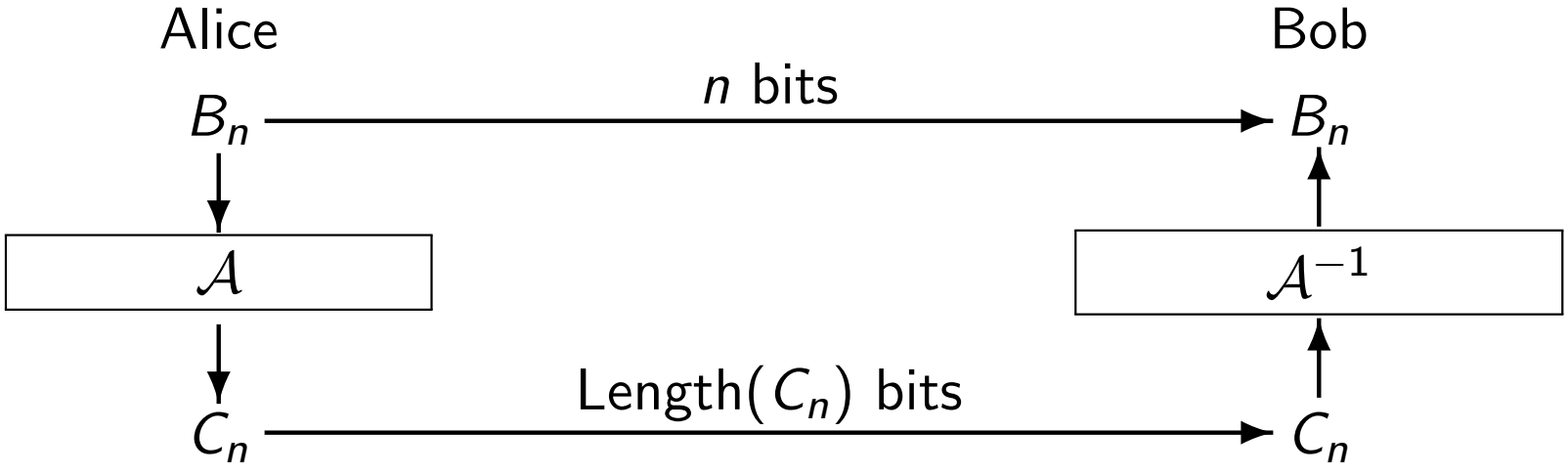
$$C_n = \mathcal{A}(B_n) \quad = \tilde{n} = \text{binary notation of } n$$



Case of Diophantine $\mathfrak{M}$

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

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

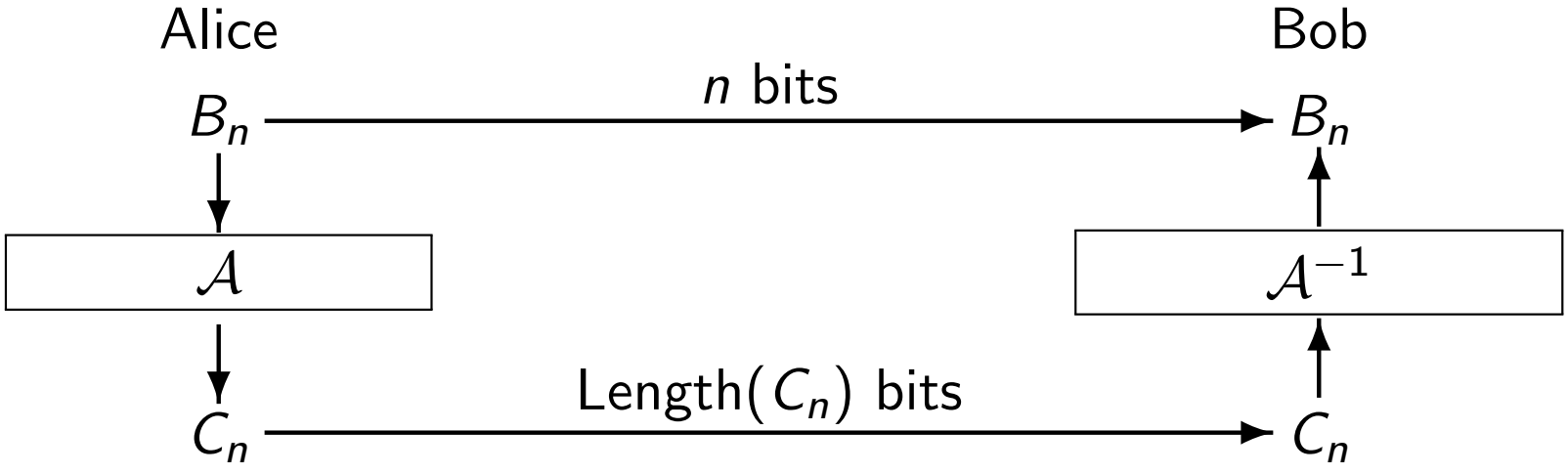


Case of Diophantine $\mathfrak{M}$

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

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

$$C_n = \mathcal{A}(B_n)$$



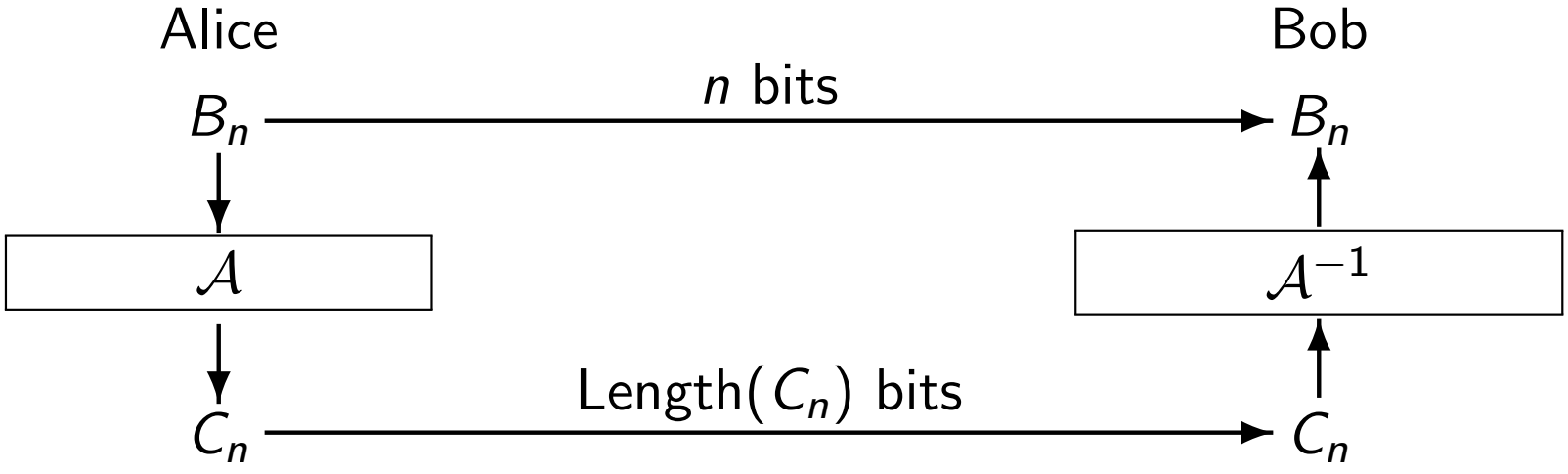
Case of Diophantine $\mathfrak{M}$

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

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

$$C_n = \mathcal{A}(B_n) \quad = \tilde{n}\widetilde{q_n}$$

where q_n is the number of "1" in B_n and $\widetilde{q_n}$ is the binary notation of q_n padded by leading zeros to the length of n.



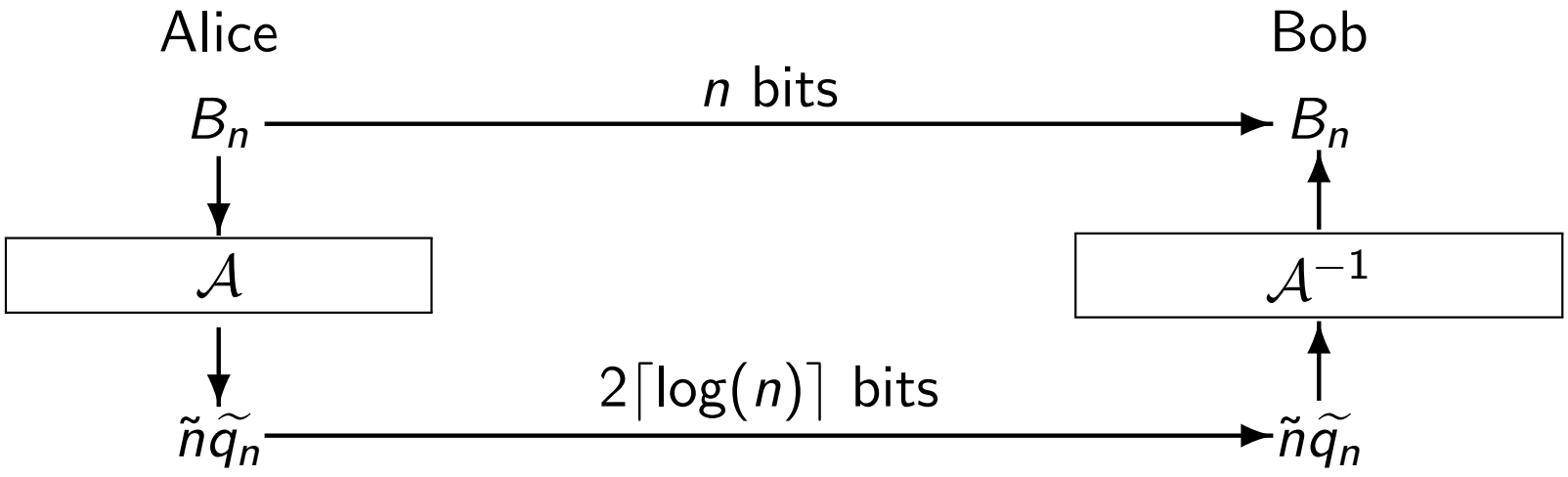
Case of Diophantine $\mathfrak{M}$

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

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

$$C_n = \mathcal{A}(B_n) \quad = \tilde{n}\widetilde{q_n}$$

where q_n is the number of "1" in B_n and $\widetilde{q_n}$ is the binary notation of q_n padded by leading zeros to the length of n.



Computational Chaos in Number Theory

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:

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

Computational Chaos in Number Theory

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 (defined up to an additive constant) of this set is equal to n.

Computational Chaos in Number Theory

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 (defined up to an additive constant) of this set is equal to n.

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

More Computational Chaos in Number Theory

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

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

More Computational Chaos in Number Theory

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

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

They proved that the prefix-free Kolmogorov complexity of this set is also equal to n (up to an additive constant).

Even More Computational Chaos in Number Theory

Theorem (Matiyasevich [2006]). *Let $\mathfrak{U}$ be a decidable infinite set with infinite complement. WE CAN construct an exponential Diophantine equation which for every value of the parameter has only finitely many solutions and such that the prefix-free Kolmogorov complexity of the set*

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

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

Diophantine Games

Diophantine Games

Diophantine Games

James Jones [1974], based on ideas of Michael O. Rabin [1957], introduced Diophantine games.

Diophantine Games

James Jones [1974], based on ideas of Michael O. Rabin [1957], introduced Diophantine games.

$$G(a_1, \ldots, a_m, x_1, \ldots, x_m) = 0$$

Diophantine Games

James Jones [1974], based on ideas of Michael O. Rabin [1957], introduced Diophantine games.

$$G(a_1, \ldots, a_m, x_1, \ldots, x_m) = 0$$

Peter selects the values of the parameters $a_1, \ldots, a_m$.

Diophantine Games

James Jones [1974], based on ideas of Michael O. Rabin [1957], introduced Diophantine games.

$$G(a_1, \ldots, a_m, x_1, \ldots, x_m) = 0$$

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

Diophantine Games

James Jones [1974], based on ideas of Michael O. Rabin [1957], introduced Diophantine games.

$$G(a_1, \ldots, a_m, x_1, \ldots, x_m) = 0$$

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

- Peter selects a_1

Diophantine Games

James Jones [1974], based on ideas of Michael O. Rabin [1957], introduced Diophantine games.

$$G(a_1, \ldots, a_m, x_1, \ldots, x_m) = 0$$

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

- Peter selects a_1
- Ursula selects x_1

Diophantine Games

James Jones [1974], based on ideas of Michael O. Rabin [1957], introduced Diophantine games.

$$G(a_1, \ldots, a_m, x_1, \ldots, x_m) = 0$$

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

- Peter selects a_1
- Ursula selects x_1
- Peter selects a_2

Diophantine Games

James Jones [1974], based on ideas of Michael O. Rabin [1957], introduced Diophantine games.

$$G(a_1, \ldots, a_m, x_1, \ldots, x_m) = 0$$

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

- Peter selects a_1
- Ursula selects x_1
- Peter selects a_2
- Ursula selects x_2

Diophantine Games

James Jones [1974], based on ideas of Michael O. Rabin [1957], introduced Diophantine games.

$$G(a_1, \ldots, a_m, x_1, \ldots, x_m) = 0$$

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

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

Diophantine Games

James Jones [1974], based on ideas of Michael O. Rabin [1957], introduced Diophantine games.

$$G(a_1, \ldots, a_m, x_1, \ldots, x_m) = 0$$

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

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

Diophantine Games

James Jones [1974], based on ideas of Michael O. Rabin [1957], introduced Diophantine games.

$$G(a_1, \ldots, a_m, x_1, \ldots, x_m) = 0$$

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

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

Diophantine Games

James Jones [1974], based on ideas of Michael O. Rabin [1957], introduced Diophantine games.

$$G(a_1, \ldots, a_m, x_1, \ldots, x_m) = 0$$

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

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

Ursula is the *winner* if and only if the value of the polynomial turns out to be equal to 0.

A Quiz

Question: *Who has the winning strategy in the following game:*

$$(x_1 + a_2)^2 + 1 - (x_2 + 2)(x_3 + 3) = 0$$

A Quiz

Question: *Who has the winning strategy in the following game:*

$$(x_1 + a_2)^2 + 1 - (x_2 + 2)(x_3 + 3) = 0$$

Hint: Peter is the winner if and only if there are infinitely many primes of the form $n^2 + 1$.

Theorem (James Jones[1982]) *In the Diophantine game*

$$\Big\{\{a_1+a_6+1-x_4\}^2\cdot\Big\{\big\langle(a_6+a_7)^2+3a_7+a_6-2x_4\big\rangle^2$$
$$+\Big\langle\big[(x_9-a_7)^2+(x_{10}-a_9)^2\big]\big[(x_9-a_6)^2+(x_{10}-a_8)^2((x_4-a_1)^2$$
$$+(x_{10}-a_9-x_1)^2)\big]\big[(x_9-3x_4)^2+(x_{10}-a_8-a_9)^2\big]\big[(x_9-3x_4-1)^2$$
$$+(x_{10}-a_8a_9)^2\big]-a_{12}-1\Big\rangle^2+\big\langle[x_{10}+a_{12}+a_{12}x_9a_4-a_3]^2$$
$$+[x_5+a_{13}-x_9a_4]^2\big\rangle\Big\}-x_{13}-1\Big\}\{a_1+x_5+1-a_5\}\Big\{\big\langle(x_5-x_6)^2$$
$$+3x_6+x_5-2a_5\big\rangle^2+\Big\langle\big[(a_{10}-x_6)^2+(a_{11}-x_8)^2\big]\big[(a_{10}-x_5)^2$$
$$+(a_{11}-x_7)^2((a_5-a_1)^2+(a_{11}-x_8-a_2)^2)\big]\big[(a_{10}-3a_5)^2$$
$$+(a_{11}-x_7-x_8)^2\big]\big[(a_{10}-3a_5-1)^2+(a_{11}-x_7x_8)^2\big]-x_{11}-1\Big\rangle^2$$
$$+\big\langle[a_{11}+x_{11}+x_{11}a_{10}x_3-x_2]^2+[a_{11}+x_{12}-a_{10}x_3]^2\big\rangle\Big\}=0$$

Ursula has a winning strategy but no computable winning strategy.