Undecidability everywhere

Bjorn Poonen

Rademacher Lecture 3
November 8, 2017

Undecidability of a single question?

So far, we've been considering families of questions with YES/NO answers, and we wanted to know if there is a computer program that gets the right answer on all of them.

Question

Can a single question be undecidable?

Example

Could the Riemann hypothesis be undecidable?

Undecidability of a single question?

So far, we've been considering families of questions with YES/NO answers, and we wanted to know if there is a computer program that gets the right answer on all of them.

Question

Can a single question be undecidable?

Example

Could the Riemann hypothesis be undecidable?

Answer: Not in the sense we've been considering, because there *is* a computer program that correctly answers the question

Is the Riemann hypothesis true?

Undecidability of a single question?

So far, we've been considering families of questions with YES/NO answers, and we wanted to know if there is a computer program that gets the right answer on all of them.

Question

Can a single question be undecidable?

Example

Could the Riemann hypothesis be undecidable?

Answer: Not in the sense we've been considering, because there *is* a computer program that correctly answers the question

Is the Riemann hypothesis true?

Program 1: PRINT "YES"

Program 2: PRINT "NO"

Independence

But it could be that

neither the Riemann hypothesis nor its negation is *provable* (within the ZFC axiom system, say).

In that case, one would say

"The Riemann hypothesis is independent of ZFC."

Example

The continuum hypothesis, that there is no set S such that

$$\#\mathbb{N} < \#S < \#\mathbb{R},$$

is independent of ZFC (Gödel 1940, Cohen 1963).
(The fine print: we're assuming that ZFC is consistent.)

Undecidability vs. independence

If a family of problems is undecidable, at least one instance is independent of ZFC. For example,

Theorem

There exists a polynomial p such that the statement

$$\exists x_1, \ldots, x_n \in \mathbb{Z} \text{ such that } p(x_1, \ldots, x_n) = 0$$

is independent of ZFC, neither provable nor disprovable.
(The fine print: we're assuming that ZFC is consistent and that ZFC theorems about integers are true.)

Proof.

Suppose that each such statement were either provable or disprovable. Then Hilbert's tenth problem is solvable: search for a proof by day, and for a disproof by night; stop when one or the other is found! □

There is a different proof that is *constructive*—one can write down a *specific* polynomial with this property! (Post 1944)

Integration

Question

Can a computer, given an explicit function $f(x)$,

1. *decide whether there is a formula for $\int f(x)\,dx$,*
2. *and if so, find it?*

Integration

Question

Can a computer, given an explicit function $f(x)$,

1. *decide whether there is a formula for $\int f(x)\,dx$,*
2. *and if so, find it?*

Theorem (Risch)

YES.

Integration

Question

Can a computer, given an explicit function $f(x)$,

1. *decide whether there is a formula for $\int f(x)\,dx$,*
2. *and if so, find it?*

Theorem (Risch)

YES.

Theorem (Richardson)

NO.

Integration

Question

Can a computer, given an explicit function $f(x)$,

1. *decide whether there is a formula for $\int f(x)\,dx$,*
2. *and if so, find it?*

Theorem (Risch)

YES.

Theorem (Richardson)

NO.

Another answer: MAYBE; it's not known yet.

Integration

Question

Can a computer, given an explicit function $f(x)$,

1. *decide whether there is a formula for $\int f(x)\,dx$,*
2. *and if so, find it?*

Theorem (Risch)

YES.

Theorem (Richardson)

NO.

Another answer: MAYBE; it's not known yet.

All of these answers are correct!

Elementary functions

Warmup question

Does $\int e^{x^2}\,dx$ *exist?*

Yes, but Liouville proved in 1835 that it cannot be represented by an elementary formula.

What does elementary mean?

Example

$$\sqrt[3]{\frac{x^3+\log\sqrt{x^2+2e^x}}{x+\sqrt{e^x+\log x}}} \text{ is elementary.}$$

In general: any function that can be built up from constants and x by arithmetic operations, adjoining roots of polynomials whose coefficients are previously constructed functions, and adjoining e^f or $\log f$ for previously constructed functions f.

YES: Risch's algorithm for integration

Question

Can a computer decide, given an elementary function f, whether it has an elementary antiderivative?

MAYBE: This runs into sticky questions about *constants*:
e.g., is $\int \left(e^{e^{3/2}} + e^{5/3} - \frac{13396}{143} \right) e^{x^2} \, dx$ elementary?

Theorem (Risch)

Let K be a field of functions built up from constants whose algebraic relations are known by adjoining x, by making finite extensions, and by adjoining functions e^f and $\log f$ such that the field of constants does not grow.
Then a computer can decide, given $f \in K$, whether $\int f$ is elementary (and can compute it if so).

NO: Undecidability of integration

Theorem (Richardson)

If one enlarges the class of elementary functions by including $|\ |$ among the building blocks, then there is no algorithm for deciding whether an elementary function has an elementary antiderivative.

Sketch of proof.

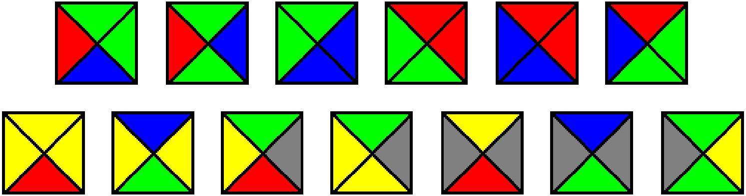
Using undecidability of trigonometric inequalities, and using $|\ |$, build a function $g(x)$ that is either 0 everywhere, or that is 1 on some interval, but such that we can't tell which. Then it is impossible to decide whether

$$\int g(x)e^{x^2}\,dx$$

is elementary. $\square$

Wang tiles

Can you tile the entire plane with copies of the following?



Rules:

- Tiles may not be rotated or reflected.
- Two tiles may share an edge only if the colors match.

Conjecture (Wang 1961)

If a finite set of tiles can tile the plane,
then there exists a periodic tiling.

Assuming this, Wang gave an algorithm for deciding whether a finite set of tiles can tile the plane.

But. . .

Conjecture (Wang 1961)

If a finite set of tiles can tile the plane,
then there exists a periodic tiling.

Assuming this, Wang gave an algorithm for deciding whether a finite set of tiles can tile the plane.

But...

Theorem (Berger 1967)

1. *Wang's conjecture is wrong!*
   Some tile sets can tile the plane only aperiodically.
2. *The problem of deciding whether a given tile set can tile the plane is undecidable.*

The mortal matrix problem

Consider the four matrices

$$A = \begin{pmatrix} 1 & 5 \\ 0 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$$

$$C = \begin{pmatrix} 6 & 2 \\ 3 & 1 \end{pmatrix} \qquad D = \begin{pmatrix} 1 & -7 \\ 0 & 1 \end{pmatrix}$$

Question

Can one multiply copies of these in some order

$$(\text{e.g., } ABCABC \text{ or } CBAADACCB)$$

to get the zero matrix?

The mortal matrix problem

Consider the four matrices

$$A = \begin{pmatrix} 1 & 5 \\ 0 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$$

$$C = \begin{pmatrix} 6 & 2 \\ 3 & 1 \end{pmatrix} \qquad D = \begin{pmatrix} 1 & -7 \\ 0 & 1 \end{pmatrix}$$

Question

Can one multiply copies of these in some order

(e.g., $ABCABC$ or $CBAADACCB$)

to get the zero matrix?

YES!

The mortal matrix problem

Consider the four matrices

$$A = \begin{pmatrix} 1 & 5 \\ 0 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$$

$$C = \begin{pmatrix} 6 & 2 \\ 3 & 1 \end{pmatrix} \qquad D = \begin{pmatrix} 1 & -7 \\ 0 & 1 \end{pmatrix}$$

Question

Can one multiply copies of these in some order

(e.g., $ABCABC$ or $CBAADACCB$)

to get the zero matrix?

YES!

What if we increase the number of matrices, or their size?

Undecidability of the mortal matrix problem

In 1970, Paterson proved that the general problem of this type is undecidable. Here are samples of what is now known:

Theorem

1. *There is no algorithm that takes as input eight 3×3 integer matrices and decides whether copies of them can be multiplied to give* $\mathbf{0}$.
2. *There is no algorithm that takes as input two 24×24 integer matrices and decides whether copies of them can be multiplied to give* $\mathbf{0}$.

Question

Is there an algorithm for any set of 2×2 integer matrices?

Powers of a single matrix

Given an $n \times n$ integer matrix A, it is easy to decide whether there exists $m \geq 0$ such that $A^m = \mathbf{0}$: just check whether the characteristic polynomial $\det(xI - A)$ equals x^n.

Question

Is there an algorithm with

input: *an integer square matrix A*

output: *YES or NO, according to whether there exists $m \geq 0$ such that the upper right corner of A^m is 0?*

The answer is not known.

This question is equivalent to a question about linear recursive sequences. . .

Linear recursive sequences

Example

$F_0 = 0, \quad F_1 = 1, \quad F_{n+2} = F_{n+1} + F_n$

$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots$

Example

$b_0 = 0, \quad b_1 = 1, \quad b_{n+2} = b_{n+1} - b_n$

$0, 1, 1, 0, -1, -1, 0, 1, 1, 0, -1, -1, 0, 1, 1, 0, -1, -1, \ldots$

Example

$a_0 = 1, \quad a_1 = 1, \quad a_2 = 1, \quad a_{n+3} = -a_{n+1} - a_n$

$1, 1, 1, -2, -2, 1, 4, 1, -5, -5, 4, 10, 1, -14, -11, 13, 25, -2, \ldots$

Zeros in a linear recursive sequence

Theorem (Skolem 1934)

For any linear recursive sequence $(a_n)_{n \geq 0}$ of integers, the set $\{n : a_n = 0\}$ is a union of a finite set and finitely many arithmetic progressions.

Question

Is there an algorithm with

input: *the specification of a linear recursive sequence*

output: *YES or NO, according to whether 0 appears in the sequence?*

The answer is not known.

Collatz $3x + 1$ problem

Start with a positive integer x.

- If x is even, replace x by $x/2$.
- If x is odd, replace x by $3x + 1$.

Repeat.

Example

Starting at 13 gives the sequence

$$13, 40, 20, 10, 5, 16, 8, 4, 2, 1.$$

Conjecture (Collatz)

For any starting value, the sequence always reaches 1*.*

Generalized Collatz problem

The original Collatz conjecture involved

$$f(x) := \begin{cases} x/2, & \text{if } x \equiv 0 \pmod 2 \\ 3x+1, & \text{if } x \equiv 1 \pmod 2. \end{cases}$$

More generally,
given $m \geq 1$ and $a_0, \ldots, a_{m-1}, b_0, \ldots, b_{m-1} \in \mathbb{Q}$,
define f by $f(x) = a_i x + b_i$ for $x \bmod m = i$.

Question

Can a computer decide, given m and the a_i and b_i such that f maps $\mathbb{N}$ to $\mathbb{N}$, whether every starting value leads to 1?

Answer: NO (Conway 1972; Kurtz & Simon 2007; Endrullis, Grabmayer, & Hendriks 2009).

Varieties

A variety is (essentially) the set of solutions to a system of multivariable polynomial equations.

Example

The variety

$$x^2 + y^2 - 1 = 0$$

is isomorphic to the variety

$$t^2 + u^2 - 5 = 0$$

via the polynomial map $(x, y) \mapsto (2x + y, x - 2y)$.
These are varieties over $\mathbb{Q}$ because they are defined by polynomials whose coefficients are rational numbers.

Isomorphism problem for varieties

Question

Is there an algorithm for deciding whether two varieties over $\mathbb{Q}$ are isomorphic?

No one has succeeded in finding such an algorithm.
Burt Totaro has asked whether it might be undecidable.

Automorphisms of varieties

Question

Is there an algorithm that given a variety over $\mathbb{Q}$, decides whether it has a nontrivial automorphism?

Not known.

Theorem (P. 2011)

There is no algorithm with

input: *a variety X, a point $x \in X$, and a subvariety $Z \subset X$ (all over $\mathbb{Q}$, say),*

output: *YES or NO, according to whether exists an automorphism of X mapping x into Z.*

Finitely generated algebras

Definition

A finitely generated commutative algebra over a field k is a k-algebra of the form $k[x_1, \dots, x_n]/(f_1, \dots, f_m)$ for some $f_1, \cdots, f_m \in k[x_1, \dots, x_n]$.

Example

The algebras $\mathbb{Q}[x, y]/(x^2 + y^2 - 1)$ and $\mathbb{Q}[t, u]/(t^2 + u^2 - 5)$ are isomorphic.

Question

Is there an algorithm for deciding whether two finitely generated commutative algebras over $\mathbb{Q}$ are isomorphic?

Question

What if $\mathbb{Q}$ is replaced by $\mathbb{Z}$?

Finitely generated fields

Definition

If A is an integral domain that is a finitely generated $\mathbb{Q}$-algebra, then the fraction field of A is called a finitely generated field extension of $\mathbb{Q}$.

Question

Is there an algorithm for deciding whether two finitely generated field extensions of $\mathbb{Q}$ are isomorphic?

All of these questions are unanswered.

Noncommutative algebra

Question

Can one decide whether two noncommutative rings are isomorphic?

The rings we consider are the (possibly noncommutative) f.p. $\mathbb{Z}$-algebras: $\mathbb{Z}\langle x_1, \ldots, x_n \rangle / (f_1, \ldots, f_m)$.

Noncommutative algebra

Question

Can one decide whether two noncommutative rings are isomorphic?

The rings we consider are the (possibly noncommutative) f.p. $\mathbb{Z}$-algebras: $\mathbb{Z}\langle x_1, \ldots, x_n\rangle/(f_1, \ldots, f_m)$.

Theorem

There is no algorithm for deciding whether two such rings are isomorphic.

Proof.

For an f.p. group G, the group ring $\mathbb{Z}G$ is an f.p. $\mathbb{Z}$-algebra, and $\mathbb{Z}G \simeq \mathbb{Z}$ if and only if $G \simeq \{1\}$ (which is undecidable). □

Games

Given a computable function $W\colon \mathbb{N}^m \to \{\mathrm{A}, \mathrm{B}\}$, players A and B play a game as follows:

- A chooses $x_1 \in \mathbb{N}$, B chooses x_2, A chooses x_3, ... until x_m has been chosen;
- then the winner is $W(x_1, x_2, \ldots, x_m)$.

Exactly one of the players has a winning strategy (Zermelo, König, Kalmár 1928). But...

Games

Given a computable function $W\colon \mathbb{N}^m \to \{A, B\}$, players A and B play a game as follows:

- A chooses $x_1 \in \mathbb{N}$, B chooses x_2, A chooses x_3, ... until x_m has been chosen;
- then the winner is $W(x_1, x_2, \ldots, x_m)$.

Exactly one of the players has a winning strategy (Zermelo, König, Kalmár 1928). But...

Theorem

It is impossible to decide, given W, which player has a winning strategy.

Proof.

Given a program p, consider the one-move game in which A chooses a positive integer x_1 and wins if p halts within the first x_1 steps. Player A has a winning strategy if and only if p halts, which is undecidable. □

Winning strategy vs. computable winning strategy

Theorem (Rabin 1957)

There is a three-move game in which B has a winning strategy, but not a computable winning strategy (i.e., there is no computable function of x_1 that is a winning move x_2 for B).

The proof uses Post's notion of a simple set (a listable set whose complement is infinite but contains no infinite listable set).

Infinite chess

Question (Stanley)

Given finitely many chess pieces on a $\mathbb{Z} \times \mathbb{Z}$ chessboard, can White force mate?

Not known.

Infinite chess

Question (Stanley)

Given finitely many chess pieces on a $\mathbb{Z} \times \mathbb{Z}$ chessboard, can White force mate?

Not known.

Theorem (Brumleve, Hamkins, Schlicht 2012)

One can decide, given finitely many chess pieces on a $\mathbb{Z} \times \mathbb{Z}$ chessboard and $n \geq 1$, whether White can mate in n moves.

Sketch of proof.

Each instance is a first-order sentence in $(\mathbb{N}; 0, 1, +)$.
The truth of any such sentence is decidable (Presburger 1929). $\square$

For more details

Search the web for my survey article

Undecidable problems: a sampler.

Thank you for your attention!