Undecidability in group theory, topology, and analysis

Bjorn Poonen

Rademacher Lecture 2
November 7, 2017

Group theory

Question

Can a computer decide whether
two given elements of a group are equal?

Group theory

Question

Can a computer decide whether
~~two given elements of a group are equal~~
a given element of a group equals the identity?

Group theory

Question

Can a computer decide whether
~~*two given elements of a group are equal*~~
a given element of a group equals the identity?

To make sense of this question, we must specify

1. how the group is described
2. how the element is described

The descriptions should be suitable for input into a Turing machine.

Group theory

Question

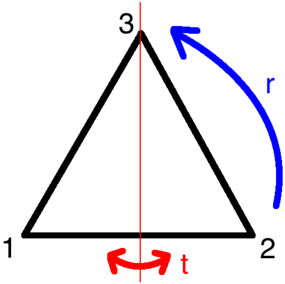
Can a computer decide whether
~~*two given elements of a group are equal*~~
a given element of a group equals the identity?

To make sense of this question, we must specify

1. how the group is described: f.p. group
2. how the element is described: word

The descriptions should be suitable for input into a Turing machine.

Example: The symmetric group S_3



In cycle notation, $r = (123)$ and $t = (12)$. These satisfy

$$r^3 = 1, \quad t^2 = 1, \quad trt^{-1} = r^{-1}$$

It turns out that r and t generate S_3, and every relation involving them is a consequence of the relations above:

$$S_3 = \langle r, t \mid r^3 = 1, t^2 = 1, trt^{-1} = r^{-1} \rangle.$$

Finitely presented groups

Definition

An f.p. group is a group specified by finitely many generators and finitely many relations.

Example

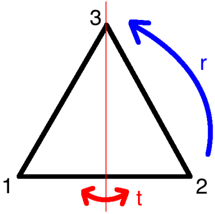
$$\mathbb{Z} \times \mathbb{Z} = \langle a, b \mid ab = ba \rangle$$

Example

The free group on 2 (noncommuting) generators is

$$F_2 := \langle a, b \mid \rangle$$

Representing elements of an f.p. group: words



$$S_3 = \langle r, t \mid r^3 = 1, t^2 = 1, trt^{-1} = r^{-1} \rangle.$$

Definition

A word is a sequence of the generator symbols and their inverses, such as

$$tr^{-1}ttrt^{-1}rrr.$$

Since r and t generate S_3, every element of S_3 is represented by a word, but not necessarily in a unique way.

Example

The words tr and $r^{-1}t$ both represent (23).

The word problem

Given an f.p. group G, we have

Word problem for G

Find an algorithm with

input: *a word w in the generators of G*
output: *YES or NO, according to whether $w = 1$ in G.*

Harder problem:

Uniform word problem

Find an algorithm with

input: *an f.p. group G, and a word w in the generators of G*
output: *YES or NO, according to whether $w = 1$ in G.*

Word problem for F_n

Theorem

The word problem for the free group F_n is decidable.

Algorithm to decide whether a given word w represents 1:

1. Repeatedly cancel adjacent inverses until there is nothing left to cancel.
2. Check if the end result is the empty word.

Example

In the free group $F_2 = \langle a, b \rangle$, given the word

$$aba^{-1}bb^{-1}abb,$$

cancellation leads to

$$abbb,$$

which is not the empty word,
so $aba^{-1}bb^{-1}abb$ does not represent the identity.

Undecidability of the word problem

Theorem (P. S. Novikov and Boone, independently in the 1950s)

There exists an f.p. group G such that the word problem for G is undecidable.

The strategy of the proof, as for Hilbert's tenth problem, is to build a group G such that solving the word problem for G is at least as hard as solving the halting problem.

Corollary

The uniform word problem is undecidable.

Markov properties

Definition

A property of f.p. groups is called a Markov property if

1. there exists an f.p. group G_1 with the property, and
2. there exists an f.p. group G_2 that cannot be embedded in any f.p. group with the property.

Example

The property of being *finite* is a Markov property, because

1. There exists a finite group!
2. $\mathbb{Z}$ cannot be embedded in any finite group.

Other Markov properties: trivial, abelian, free, ...

Theorem (Adian & Rabin 1955–1958)

For each Markov property $\mathcal{P}$, the problem of deciding whether an arbitrary f.p. group has $\mathcal{P}$ is undecidable.

Sketch of proof.

Embed the uniform word problem in this $\mathcal{P}$ problem: Given an f.p. group G and a word w in its generators, build another f.p. group K such that

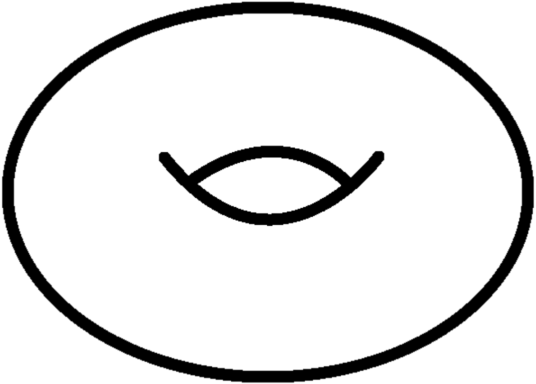
$$K \text{ has } \mathcal{P} \iff w = 1 \text{ in } G. \qquad \square$$

Example

There is no algorithm to decide whether an f.p. group is trivial.

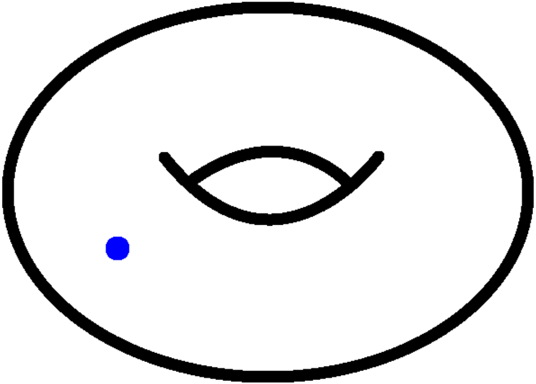
Fundamental group

Fix a manifold M.



Fundamental group

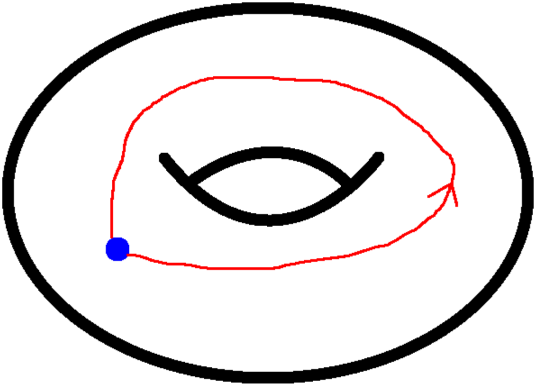
Fix a manifold M and a point p.



Fundamental group

Fix a manifold M and a point p.

Consider paths in M that start and end at p.

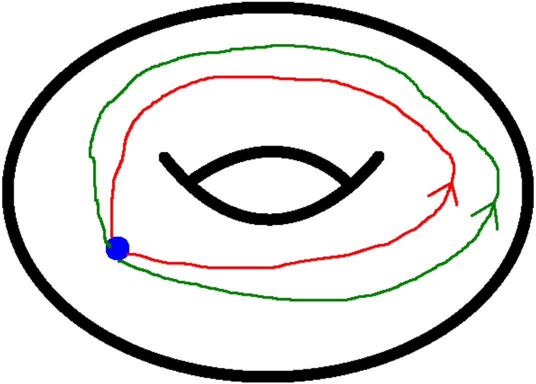


Fundamental group

Fix a manifold M and a point p.

Consider paths in M that start and end at p.

Paths are homotopic if one can be deformed to the other.



Fundamental group

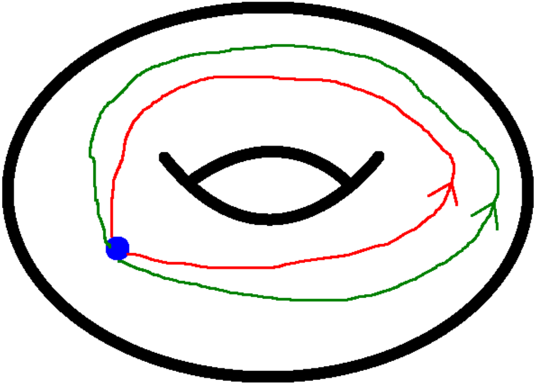
Fix a manifold M and a point p.

Consider paths in M that start and end at p.

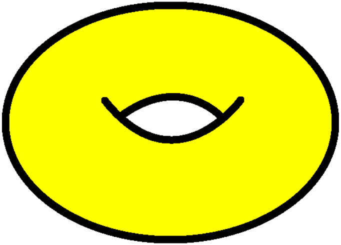
Paths are homotopic if one can be deformed to the other.

$$\text{Fundamental group } \pi_1(M) := \{\text{paths}\}/\text{homotopy}.$$

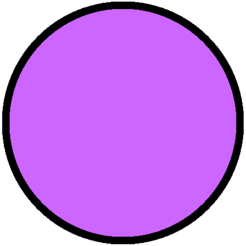
Group law: concatenation of paths.



Examples of fundamental groups



$\pi_1(\text{torus}) = \mathbb{Z} \times \mathbb{Z}$



$\pi_1(\text{sphere}) = \{1\}$

This gives one way to prove that the torus and the sphere are not homeomorphic, i.e., that they do not have the same shape even after stretching.

The homeomorphism problem

Question

Given two manifolds, can one decide whether they are homeomorphic?

To make sense of this question, we must specify how a manifold is described.

This will be done using the notion of simplicial complex.

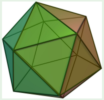
Simplicial complexes

Definition

Roughly speaking, a finite simplicial complex is a finite union of simplices (points, segments, triangles, tetrahedra, ...) together with data on how they are glued. The description is purely combinatorial.

Example

The icosahedron is a finite simplicial complex homeomorphic to the 2-sphere S^2.



From now on, manifold means "compact manifold represented by a particular finite simplicial complex", so that it can be the input to a Turing machine.

Undecidability of the homeomorphism problem

Theorem (Markov 1958)

The problem of deciding whether two manifolds are homeomorphic is undecidable.

Sketch of proof.

Let $n \geq 5$. Given an f.p. group G and a word w in its generators, one can construct a n-manifold $\Sigma_{G,w}$ such that

1. If $w = 1$ in G, then $\Sigma_{G,w} \approx S^n$.
2. If $w \neq 1$, then $\pi_1(\Sigma_{G,w})$ is nontrivial (so $\Sigma_{G,w} \not\approx S^n$).

Thus, if the homeomorphism problem were decidable, then the uniform word problem would be too. But it isn't. $\square$

In fact, the homeomorphism problem is known to be

- decidable in dimensions ≤ 3, and
- undecidable in dimensions ≥ 4.

The previous proof showed that for $n \geq 5$, the manifold S^n is unrecognizable: the problem of deciding whether a given n-manifold is homeomorphic to S^n is undecidable.

Theorem (S. P. Novikov 1974)

Each n-manifold M with $n \geq 5$ is unrecognizable.

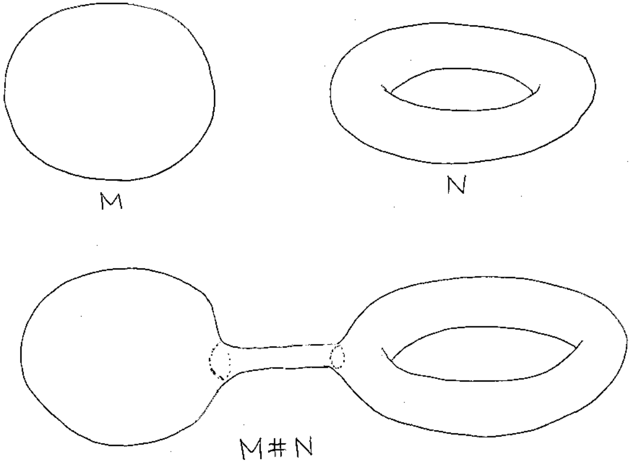
Question

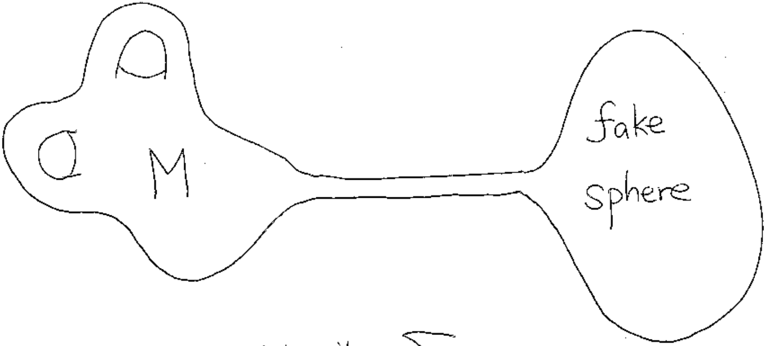
Is S^4 recognizable? (The answer is not known.)

To explain the idea of the proof of the theorem, we need the notion of connected sum.

Connected sum

The connected sum of n-manifolds M and N is the n-manifold obtained by cutting a small disk out of each and connecting them with a tube.





$$M \# \Sigma_{G,w}$$

Am I a manifold?

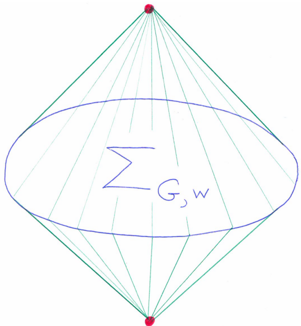
Theorem

It is impossible to decide whether a finite simplicial complex is homeomorphic to a manifold.

Proof.

$S\Sigma_{G,w}$:= suspension over our possibly fake sphere $\Sigma_{G,w}$.

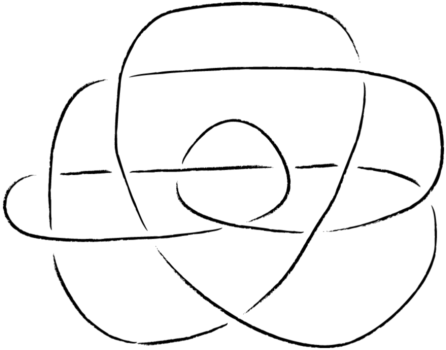
- If $w = 1$ in G, then $\Sigma_{G,w} \approx S^n$, so $S\Sigma_{G,w} \approx S^{n+1}$.
- If $w \neq 1$, then $S\Sigma_{G,w}$ is not locally Euclidean. □



Knot theory

Definition

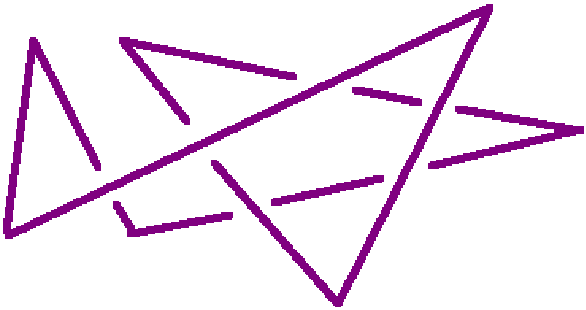
A knot is an embedding of the circle S^1 in $\mathbb{R}^3$.



Definition

Two knots are equivalent if one can be deformed into the other within $\mathbb{R}^3$, without crossing itself.

From now on, knot means "a knot obtained by connecting a finite sequence of points in $\mathbb{Q}^3$", so that it admits a finite description.



Theorem (Haken 1961 and Hemion 1979)

There is an algorithm that takes as input two knots in $\mathbb{R}^3$ *and decides whether they are equivalent.*

Higher-dimensional knots

Though the knot equivalence problem is decidable, a higher-dimensional analogue is not:

Theorem (Nabutovsky & Weinberger 1996)

If $n \geq 3$, the problem of deciding whether two embeddings of S^n in $\mathbb{R}^{n+2}$ are equivalent is undecidable.

Question

What about $n = 2$? Not known.

Polynomial inequalities

Question

Which of the following inequalities are true for all real values of the variables?

$$a^2 + b^2 \geq 2ab$$

$$x^4 - 4x + 5 \geq 0$$

Polynomial inequalities

Question

Which of the following inequalities are true for all real values of the variables?

$$a^2 + b^2 \geq 2ab \qquad \text{TRUE}$$

$$x^4 - 4x + 5 \geq 0$$

Polynomial inequalities

Question

Which of the following inequalities are true for all real values of the variables?

$$a^2 + b^2 \geq 2ab$$ TRUE

$$x^4 - 4x + 5 \geq 0$$ TRUE

Polynomial inequalities

Question

Which of the following inequalities are true for all real values of the variables?

$$a^2 + b^2 \geq 2ab \qquad \text{TRUE}$$

$$x^4 - 4x + 5 \geq 0 \qquad \text{TRUE}$$

$$\begin{gathered}
536x^{287196896} - 210y^{287196896} + 777x^3y^{16}z^{4732987} \\
-1111x^{54987896} - 2823y^{927396} + 27x^{94572}y^{9927}z^{999} \\
-936718x^{726896} + 887236y^{726896} - 9x^{24572}y^{7827}z^{13} \\
+89790876x^{26896} + 30y^{26896} + 987x^{245}y^6z^{6876} \\
+982370970979079x^{28} - 1987y^{28} + 1467890461986x^2y^6z^4 \\
+80398600x^2z^{12} - 27980186xy + 3789720156y^2 + 9328769x \\
-1956820y - 2758932498270987907686458 46898z \geq -389?
\end{gathered}$$

Polynomial inequalities

Question

Which of the following inequalities are true for all real values of the variables?

$$a^2 + b^2 \geq 2ab \qquad \text{TRUE}$$

$$x^4 - 4x + 5 \geq 0 \qquad \text{TRUE}$$

$$\begin{gathered}
536x^{287196896} - 210y^{287196896} + 777x^3y^{16}z^{4732987} \\
-1111x^{54987896} - 2823y^{927396} + 27x^{94572}y^{9927}z^{999} \\
-936718x^{726896} + 887236y^{726896} - 9x^{24572}y^{7827}z^{13} \\
+89790876x^{26896} + 30y^{26896} + 987x^{245}y^6z^{6876} \\
+98237097097907 90x^{28} - 1987y^{28} + 1467890461986x^2y^6z^4 \\
+80398600x^2z^{12} - 27980186xy + 3789720156y^2 + 9328769x \\
-1956820y - 27589324982709879076864584 6898z \geq -389?
\end{gathered}$$

FALSE

Polynomial inequalities, continued

Question

Can a computer decide, given a polynomial inequality

$$f(x_1, \ldots, x_n) \geq 0$$

with rational coefficients, whether it is true for all real numbers $x_1, \ldots, x_n$*?*

Polynomial inequalities, continued

Question

Can a computer decide, given a polynomial inequality

$$f(x_1, \ldots, x_n) \geq 0$$

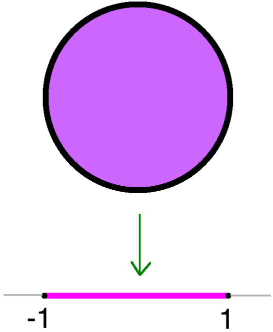
with rational coefficients, whether it is true for all real numbers $x_1, \ldots, x_n$*?*

YES! (Tarski 1951) More generally, it can decide the truth of any first-order sentence involving polynomial inequalities.

How? For example, how could it decide whether a given set defined by a Boolean combination of inequalities is empty?

Inequalities: induction on the number of variables

$$x^2 + y^2 < 1$$



$$x > -1 \quad \wedge \quad x < 1$$

- In general, the projection $(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_{n-1})$ maps a set S defined by an explicit Boolean combination of inequalities to another such set S'.
- $S \neq \emptyset$ if and only if $S' \neq \emptyset$.
- Keep projecting until only 1 variable is left; then use calculus.

Exponential inequalities

Can a computer decide the truth of inequalities like

$$e^{e^{x+y}} + 20 \geq 5x + 4y \ ?$$

Exponential inequalities

Can a computer decide the truth of inequalities like

$$e^{e^{x+y}} + 20 \geq 5x + 4y \; ?$$

Warmup: What about $e^{e^{3/2}} + e^{5/3} \geq \dfrac{13396}{143}$?

This should be easy: compute both sides to high precision, but...

Exponential inequalities

Can a computer decide the truth of inequalities like

$$e^{e^{x+y}} + 20 \geq 5x + 4y \text{ ?}$$

Warmup: What about $e^{e^{3/2}} + e^{5/3} \geq \dfrac{13396}{143}$?

This should be easy: compute both sides to high precision, but...

What if they turn out to be exactly equal?

Schanuel's conjecture in transcendental number theory predicts that "coincidences" like these never occur, but it has not been proved.

Theorem (Macintyre and Wilkie)

If Schanuel's conjecture is true, then exponential inequalities in any number of variables are decidable.

Trigonometric inequalities

Question

Can a computer decide the truth of inequalities involving expressions built up from x and $\sin x$?

Trigonometric inequalities

Question

Can a computer decide the truth of inequalities involving expressions built up from x and $\sin x$?

NO! (Richardson 1968)

Idea: Let $p, L \in \mathbb{Z}[x_1, \ldots, x_n]$ be such that $L(\vec{x}) \gg p(\vec{x})^2$.

$$f(\vec{x}) := -1 + 4p(\vec{x})^2 + L(\vec{x})(\sin^2 \pi x_1 + \cdots + \sin^2 \pi x_n).$$

If $f(\vec{x}) < 0$, then

- $\sin^2 \pi x_i \approx 0$, so x_i is very close to an integer a_i, and
- $p(\vec{x}) < 1/2$, which forces $p(a_1, \ldots, a_n) = 0$

Conclusion:

$f < 0$ somewhere $\iff$ $p(\vec{x}) = 0$ has an integer solution

(undecidable)

Inequalities in *one* variable

Question

Can a computer at least decide the truth of trigonometric inequalities in one variable?

Inequalities in *one* variable

Question

Can a computer at least decide the truth of trigonometric inequalities in one variable?

NO! In fact, the one-variable inequality problem is just as hard as the many-variable inequality problem.

The proof uses the parametrized curve

$$\vec{G}(t) := (t \sin t, t \sin t^3).$$

What does this curve in $\mathbb{R}^2$ look like?

As t ranges over real numbers,

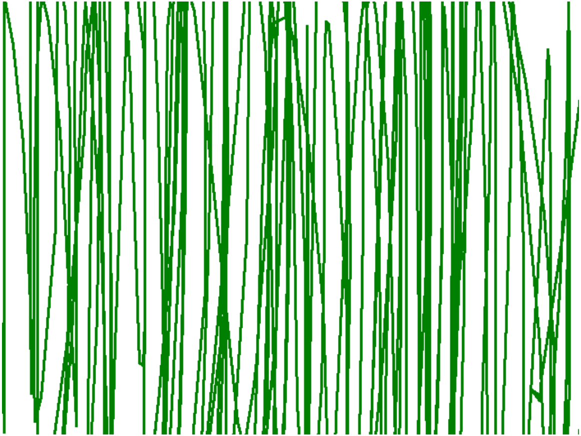
$$\vec{G}(t) := (t \sin t, t \sin t^3)$$

traces out

As t ranges over real numbers,

$$\vec{G}(t) := (t \sin t, t \sin t^3)$$

traces out



For a continuous function $f(x, y)$,

$$f(x, y) \geq 0 \text{ on } \mathbb{R}^2 \iff f(\vec{G}(t)) \geq 0 \text{ for all } t$$

Equality of functions

Bad news for automated homework checkers:

Theorem

It is impossible for a computer to decide, given two functions built out of x, $\sin x$, $|\;|$, whether they are equal.

Proof: If you can't decide whether $f(x) \geq 0$, then you can't decide whether $f(x)$ and $|f(x)|$ are the same function.

Complex analysis

Example

Does

$$e^z = w^3 + 5z + 4$$
$$e^w = w^2 + 3z^4 - 7$$
$$w^4 = z^9 + z^5 + 2.$$

have a solution in complex numbers z and w?

Question

Can a computer decide whether a system of equations involving the complex exponential function has a complex solution?

Complex analysis

Question

Can a computer decide whether a system of equations involving the complex exponential function has a complex solution?

NO! (Adler 1969)

Proof: The 3 steps below characterize $\mathbb{Z}$ in $\mathbb{C}$ by equations:

1. $2\pi i\mathbb{Z}$ is the set of solutions to $e^z = 1$
2. $\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in 2\pi i\mathbb{Z} \text{ and } b \neq 0 \right\}$
3. $\mathbb{Z}$ is the set of $q \in \mathbb{Q}$ such that $2^q \in \mathbb{Q}$; thus

$$\mathbb{Z} := \{q \in \mathbb{Q} : \ \exists z \in \mathbb{C} \text{ such that } e^z = 2 \text{ and } e^{qz} \in \mathbb{Q}\}.$$

Thus

- Hilbert's tenth problem $\subseteq$ the complex analysis problem.
- Hilbert's tenth problem is undecidable,
  so the complex analysis problem is undecidable.

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!