Undecidability everywhere

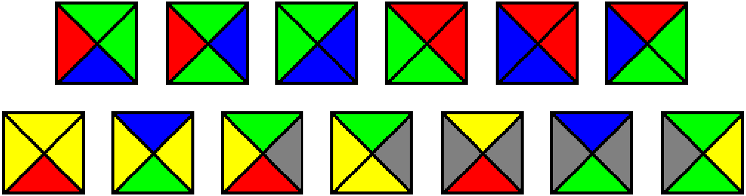
Bjorn Poonen

University of California at Berkeley

Cantrell Lecture 3
University of Georgia
March 28, 2008

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, 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, 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.*

Group theory

Question

Can a computer decide whether an element of a group equals the identity?

To make sense of this question, we must specify

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

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

Finitely presented groups (examples)

Example (Pairs of integers)

$$\mathbb{Z}^2 = \langle a, b \mid ab = ba \rangle$$

Think of a as $(1, 0)$ and b as $(0, 1)$.

Example (The symmetric group on 3 letters)

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

Think of r as (123) and t as (12).

Example (The free group on 2 generators)

$$F_2 = \langle g_1, g_2 \mid \rangle.$$

An f.p. group can be described using finitely many characters, and hence is suitable input for a Turing machine.

Finitely presented groups (definition)

Definition

A group G is finitely presented (f.p.) if there exist $n \in N$ and finitely many elements $r_1, \ldots, r_m \in F_n$ such that $G \simeq F_n/R$ where R is the smallest normal subgroup of F_n containing $r_1, \ldots, r_m$.

Think of $r_1, \ldots, r_n$ as relations imposed on the generators of G, and think of R as the set of relations *implied* by $r_1, \ldots, r_n$. We write

$$G = \langle g_1, \ldots, g_n \mid r_1, \ldots, r_m \rangle.$$

Words

How are elements of f.p. groups represented?

Definition

A word in the elements of a set S is a finite sequence in which each term is an element $s \in S$ or a symbol s^{-1} for some $s \in S$.

Example

$aba^{-1}a^{-1}bb^{-1}b$ is a word in a and b.

If G is an f.p. group with generators $g_1, \ldots, g_n$, then each word in $g_1, \ldots, g_n$ represents an element of G.

Example

In $S_3 = \langle r, t \mid r^3 = 1, t^2 = 1, trt^{-1} = r^{-1} \rangle$ with $r = (123)$ and $t = (12)$, the words tr and $r^{-1}t$ both represent (23). And $trt^{-1}r$ represents the identity.

The word problem

Given a 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 represents the identity in G.*

Harder problem:

Uniform word problem

Find an algorithm with

input: *a f.p. group G, and a word w in the generators of G*

output: *YES or NO, according to whether w represents the identity in G.*

Word problem for F_n

The word problem for the free group F_n is decidable: given a word in the generators, it represents the identity if and only if the reduced word obtained by iteratively cancelling adjacent inverses is the empty word.

Example

In the free group $F_2 = \langle a, b \rangle$, the reduced word associated to

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

is

$$abbb.$$

Undecidability of the word problem

- For any f.p. group G, the set W of words w representing the identity in G is listable: a computer can generate all possible consequences of the given relations.
- But the word problem for G is asking whether W is computable, whether an algorithm can test whether a particular word belongs to W.

In fact:

Theorem (P. S. Novikov 1955)

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

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:

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

Other Markov properties: trivial, abelian, nilpotent, solvable, free, torsion-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.

Given an f.p. group G and a word w in its generators, one can build another f.p. group K such that K has $\mathcal{P}$ if and only if w represents the identity of G. If $\mathcal{P}$ were a decidable property, then one could solve the uniform word problem. □

Corollary

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

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

Simplicial complexes

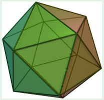
From now on, manifold means "compact manifold represented by a particular finite simplicial complex", so that it can be the input to a Turing machine.

Definition

Roughly speaking, a finite simplicial complex is a finite union of simplices 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.



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 represents the identity, $\Sigma_{G,w} \approx S^n$.
2. If not, 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. □

In fact, the homeomorphism problem is known to be

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

Theorem (S. P. Novikov 1974)

Fix an n-manifold M with $n \geq 5$. Then M is unrecognizable; i.e., the problem of deciding whether a given n-manifold is homeomorphic to M is undecidable.

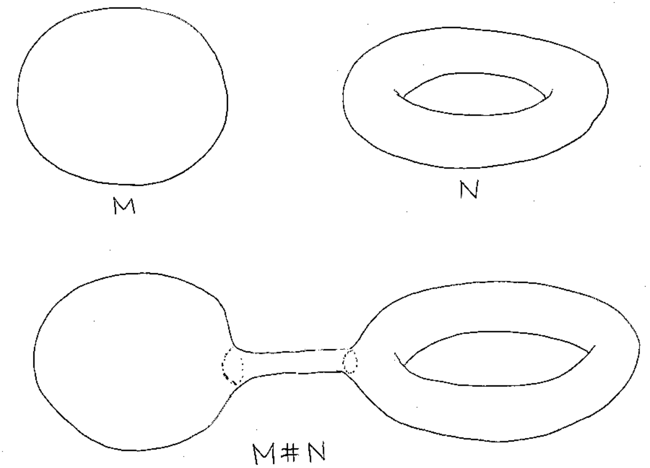
Question

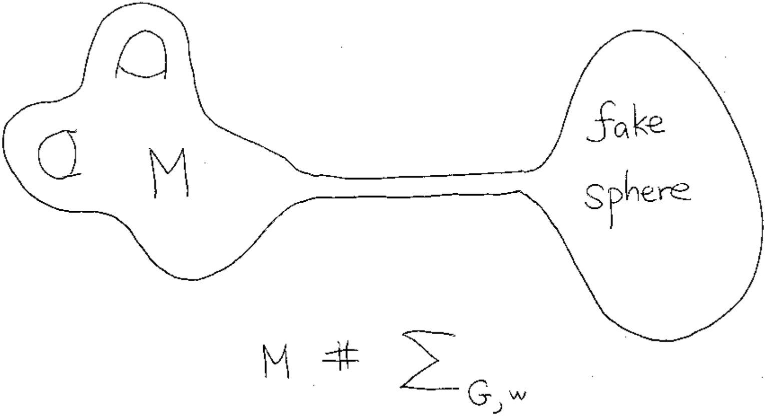
Is S^4 recognizable?

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.

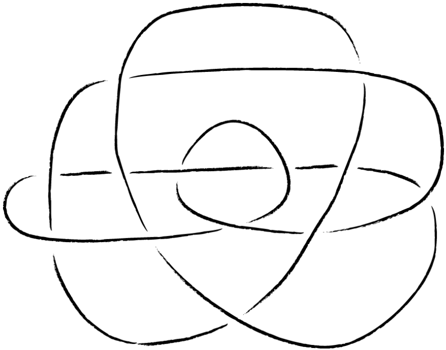



M
fake
sphere
M # ΣG,w

Knot theory

Definition

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



Definition

Two knots are equivalent if there is an ambient isotopy (i.e., deformation of $\mathbb{R}^3$) that transforms one into the other.

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.

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

Theorem

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.

Varieties

Let $\overline{\mathbb{Q}} \subset \mathbb{C}$ be the field of algebraic numbers.

- The set of $(x, y, z) \in \overline{\mathbb{Q}}^3$ satisfying the system

$$x^2 + 3y + 5yz = 0$$
$$x^3 + y^4 z - 7 = 0$$

  is an example of an affine variety over $\overline{\mathbb{Q}}$.
- Arbitrary varieties are obtained by gluing finitely many affine varieties, with transition maps given by ratios of polynomials (just as differentiable manifolds are obtained by gluing charts, with differentiable transition maps).
- A morphism of varieties is an everywhere-defined map that is locally given by ratios of polynomials.

Varieties form a category. One goal of algebraic geometry is to classify varieties up to isomorphism.

Isomorphism problem for varieties

Question

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

Burt Totaro suggested to me that maybe the problem could be proved undecidable. But no one has succeeded in doing this yet.

Question

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

Finitely generated algebras

Definition

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

The isomorphism problem for affine varieties is equivalent to

Question

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

Question

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

The same questions for $\overline{\mathbb{Q}}$ can be restated in geometric terms:

Question

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

All of these questions are unanswered.

A few references

1. Charles F. Miller III, *On group-theoretic decision problems and their classification*, Annals of Mathematics Studies **68**, Princeton Univ. Press, Princeton, NJ; Univ. of Tokyo Press, Tokyo, 1971.
2. —, *Decision problems for groups—survey and reflections*, Algorithms and classification in combinatorial group theory (Berkeley, CA, 1989), 1–59, Math. Sci. Res. Inst. Publ., **23**, Springer, New York, 1992.
3. Bjorn Poonen, Undecidability in number theory, *Notices Amer. Math. Soc.* **55** (2008), no. 3, 344–350.
4. Shmuel Weinberger, *Computers, rigidity, and moduli. The large-scale fractal geometry of Riemannian moduli space*, M. B. Porter Lectures, Princeton Univ. Press, Princeton, NJ, 2005.
5. Wikipedia!