UNDECIDABLE PROBLEMS: A SAMPLER

BJORN POONEN

ABSTRACT. After discussing two senses in which the notion of undecidability is used, we present a survey of undecidable decision problems arising in various branches of mathematics.

1. INTRODUCTION

The goal of this survey article is to demonstrate that undecidable decision problems arise naturally in many branches of mathematics. The criterion for selection of a problem in this survey is simply that the author finds it entertaining! We do not pretend that our list of undecidable problems is complete in any sense. And some of the problems we consider turn out to be decidable or to have unknown decidability status. For another survey of undecidable problems, see [Dav77].

2. TWO NOTIONS OF UNDECIDABILITY

There are two common settings in which one speaks of undecidability:

1. **Independence from axioms:** A single statement is called undecidable if neither it nor its negation can be deduced using the rules of logic from the set of axioms being used. (Example: The continuum hypothesis, that there is no cardinal number strictly between $\aleph_0$ and $2^{\aleph_0}$, is undecidable in the ZFC axiom system, assuming that ZFC itself is consistent [Göd40, Coh63, Coh64].) The first examples of statements independent of a "natural" axiom system were constructed by K. Gödel [Göd31].

2. **Decision problem:** A family of problems with YES/NO answers is called undecidable if there is no algorithm that terminates with the correct answer for every problem in the family. (Example: Hilbert's tenth problem, to decide whether a multivariable polynomial equation with integer coefficients has a solution in integers, is undecidable [Mat70].)

Remark 2.1. In modern literature, the word "undecidability" is used more commonly in sense 2, given that "independence" adequately describes sense 1.

To make 2 precise, one needs a formal notion of algorithm. Such notions were introduced by A. Church [Chu36a] and A. Turing [Tur36] independently in the 1930s. From now on, we interpret algorithm to mean Turing machine, which, loosely speaking, means that it is a computer program that takes as input a finite string of 0s and 1s. The role of the finite string is to specify which problem in the family is to be solved.

Remark 2.2. Often in describing a family of problems, it is more convenient to use higher-level mathematical objects such as polynomials or finite simplicial complexes as input. This is acceptable if these objects can be encoded as finite binary strings. It is not necessary to specify the encoding as long as it is clear that a Turing machine could convert between reasonable encodings imagined by two different readers.

Remark 2.3. One cannot speak of a *single* YES/NO question being undecidable in sense 2, because there exists an algorithm that outputs the correct answer for it, even if one might not know *which* algorithm it is!

There is a connection between the two notions of undecidability. Fix a decision problem and an axiom system $\mathcal{A}$ such that

(a) there is a computer program that generates exactly the axioms of $\mathcal{A}$; and
(b) there is a computer program that, when fed an instance i of the decision problem, outputs a statement Y_i in the language of $\mathcal{A}$ such that
- if Y_i is provable in $\mathcal{A}$, then the answer to i is YES, and
- if $\neg Y_i$ is provable in $\mathcal{A}$, then the answer to i is NO.

Under these assumptions, if the decision problem is undecidable in sense 2, then at least one of its instance statements Y_i is undecidable in sense 1, i.e., independent of $\mathcal{A}$. The proof of this is easy: if every Y_i could be proved or disproved in $\mathcal{A}$, then the decision problem could be solved by a computer program that generates all theorems deducible from $\mathcal{A}$ until it finds either Y_i or $\neg Y_i$. In fact, under the same assumptions, there must be *infinitely many* Y_i that are independent of $\mathcal{A}$, since if there were only finitely many, there would exist a decision algorithm that handled them as special cases.

Remark 2.4. In all the undecidable decision problems we present, the source of the undecidability can be traced back to a single undecidable decision problem, namely the halting problem, or equivalently the membership problem for listable sets (see Sections 3.1 and 3.2). For any of these problems, in principle we can compute a *specific i* for which Y_i is independent of $\mathcal{A}$ (cf. the last paragraph of page 294 of [Pos44]). The value of i depends on $\mathcal{A}$; more precisely, i can be computed in terms of the programs in (a) and (b).

Example 2.5. Assume that ZFC is consistent, and, moreover, that theorems in ZFC about integers are true. Then, because the undecidability of Hilbert's tenth problem in sense 2 is proved via the halting problem (see Section 8.1), there is a specific polynomial $f \in \mathbb{Z}[x_1, \ldots, x_n]$ one could write down in principle such that neither

$$(1) \qquad\qquad (\exists x_1, \ldots, x_n \in \mathbb{Z})\ f(x_1, \ldots, x_n) = 0$$

nor its negation can be proved in ZFC. Moreover, (1) must be false, because if it were true, it could be proved in ZFC by exhibiting a single $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ satisfying $f(x_1, \ldots, x_n) = 0$. (It might seem as if this is a ZFC proof of the negation of (1), but in fact it is only a ZFC proof of the *implication*

> "If ZFC is consistent and proves only true theorems about integers, then the negation of (1) holds."

This observation is related to Gödel's second incompleteness theorem, which implies that ZFC cannot prove the hypothesis of the implication unless ZFC is inconsistent!)

3. Logic

Gödel's incompleteness theorems [Göd31] provided undecidable statements in sense 1 for a wide variety of axiom systems. Inspired by this, Church and Turing began to prove that certain decision problems were undecidable in sense 2, as soon as they developed their notions of algorithm.

3.1. **The halting problem.** The halting problem asks whether it is possible write a debugger that takes as input a computer program and decides whether it eventually halts instead of entering an infinite loop. For convenience, let us assume that each program accepts a natural number as input:

Halting problem.

> **input:** a program p and a natural number x
> **question:** Does p eventually halt when run on input x?

Theorem 3.1 (Turing [Tur36])**.** *The halting problem is undecidable.*

Sketch of proof. We will use an encoding of programs as natural numbers, and identify programs with numbers. Suppose that there were an algorithm for deciding when program p halts on input x. Using this, we could write a new program H such that

$$H \text{ halts on input } x \quad \Longleftrightarrow \quad \text{program } x \text{ does not halt on input } x.$$

Taking $x = H$, we find a contradiction: H halts on input H if and only if H does not halt on input H. □

To turn the sketch above into a complete proof would require some programming, to show that there is a "universal" computer program that can simulate any other program given its number; this could then be used to construct H.

3.2. **Listable sets.** Let $\mathbb{N}$ be the set of natural numbers. Let A be a subset of $\mathbb{N}$. Call A computable[1] if there is an algorithm that takes an input an element $n \in \mathbb{N}$ and decides whether or not $n \in A$. On the other hand, call A listable or computably enumerable (c.e.) if there is a computer program that when left running forever eventually prints out exactly the elements of A. Computable sets are listable.

For each listable set A, we then have the following decision problem:

Membership in a listable set A.

> **input:** $n \in \mathbb{N}$
> **question:** Is $n \in A$?

Theorem 3.2 ([Chu36a, Ros36, Kle36])**.** *There exists a listable set A for which the membership problem is undecidable.*

Proof. Let A be the set of numbers of programs that halt. Then A is listable (write a program that during iteration N runs each of the first N programs for N steps, and prints the numbers of those that have already halted). But the undecidability of the halting problem implies that A is not computable; in other words, the membership problem for A is undecidable. □

---

[1] In most twentieth century literature in the subject one finds the terms recursive and recursively enumerable (r.e.). But R. Soare [Soa96] has argued in favor of the use of the terms "computable" and "c.e." instead, and many researchers in the field have followed his recommendation.

It would be just as easy to argue in reverse, to use the existence of a non-computable listable set to prove the undecidability of the halting problem.

3.3. **The Entscheidungsproblem.** Fix a finite set of axioms. Then there are some (first-order) statements that are universally valid, meaning that they are true for every mathematical structure satisfying the axioms. By the completeness theorem of first-order logic [Göd30], the universally valid statements are exactly the ones that are provable in the sense that they can be deduced from the axioms using the rules of logic.

Can one decide in a finite amount of time whether or not any given statement is universally valid? This is the Entscheidungsproblem, proposed by D. Hilbert [HA28, Chapter 3, §11]. (Entscheidung is the German word for "decision".) One could try searching for a proof by day and searching for a proof of the negation by night, but such an algorithm might fail to terminate for some input statements since it could be that neither proof exists.

More formally, but still without providing full definitions, given a first-order logic $\mathcal{F}$, possibly including a finite number of special axioms beyond the basic axioms of first-order logic, one has the following decision problem:

Entscheidungsproblem for $\mathcal{F}$.

>   **input:** a first-order sentence s in the language of $\mathcal{F}$
>   **question:** Is s true in every model of the axioms of $\mathcal{F}$?

It was known to Hilbert that there is a single first-order logic $\mathcal{F}_0$ without special axioms such that if the Entscheidungsproblem for $\mathcal{F}_0$ is decidable, so is the Entscheidungsproblem for any other first-order logic. But Church [Chu36a, Chu36b] and Turing [Tur36, §11] independently proved that the Entscheidungsproblem for $\mathcal{F}_0$ was undecidable. For more information, see [Dav58, Chapter 8, §4].

4. COMBINATORICS

4.1. **The Post correspondence problem.** Imagine a rectangular block with a finite string of a's and b's written along the top and another such string written along the bottom, both upright. When finitely many such blocks are laid side to side, the strings along the top may be concatenated, and the strings along the bottom may be concatenated. E. Post [Pos46] proved that the following simple-sounding problem is undecidable.

Post correspondence problem.

>   **input:** a finite collection of blocks, labelled as above
>   **question:** Given an unlimited supply of copies of these particular blocks, can one form a nonempty finite sequence of them for which the concatenation of the top strings equals the concatenation of the bottom strings?

The reason that it is undecidable is that one can embed the halting problem in it. Namely, with some work it is possible, given a computer program p, to construct an instance of Post correspondence problem that has a positive answer if and only if p halts.

Because of its simplicity, the Post correspondence problem is often used to prove the undecidability of other problems, for instance, in the formal theory of languages: see [Dav77].
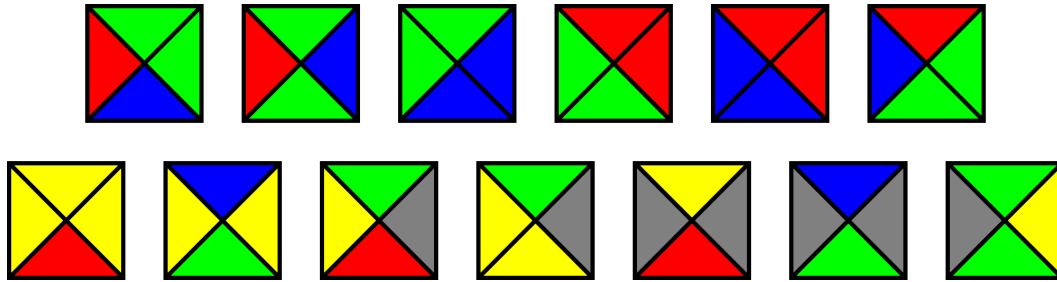
FIGURE 1. A collection of 13 Wang tiles that can tile the plane, but only aperiodically. (Source: `http://commons.wikimedia.org/wiki/File:Wang_tiles.svg` ,based on [Cul96].)

4.2. **Tiling the plane.** Wang tiles, introduced by H. Wang [Wan61, §4.1], are unit squares in the plane, with sides parallel to the axes, such that each side of each square has been assigned a color. Figure 1 shows a collection of 13 such tiles. They may be translated, but not rotated or reflected. A tiling of the plane into such squares is valid if whenever two squares share an edge, the colors match, as in the game of dominoes. Wang proposed the following problem:

Tiling problem.

> **input:** a finite collection of Wang tiles
> **question:** Is there a valid tiling of the entire plane using only translated copies of the given tiles?

Wang also conjectured [Wan61, 4.1.2] that if a tiling exists for a given finite collection, then there exists a *periodic* tiling, i.e., one that is invariant under translations by the vectors in a finite-index subgroup of $\mathbb{Z}^2$, or equivalently by the vectors in $(n\mathbb{Z})^2$ for some fixed $n \geq 1$. He observed that this conjecture would imply that the tiling problem was decidable: on the nth day one could search for tilings that are invariant under translations in $(n\mathbb{Z})^2$, and on the nth night one could search for an $n \times n$ square that cannot be tiled (a compactness argument shows that if the entire plane cannot be tiled, then there exists n such that the $n \times n$ square cannot be tiled).

But R. Berger [Ber66] then proved that the tiling problem was undecidable, by embedding the halting problem as a subproblem of the tiling problem. Combining this with Wang's observation shows that there exist finite collections that can tile the plane, but only *aperiodically*. Simplifications by R. Robinson [Rob71], J. Kari [Kar96], and K. Culik II [Cul96] led to the example in Figure 1, with only 13 tiles.

Remark 4.1. R. Robinson [Rob78] and M. Margenstern [Mar08] proved similar undecidability results for tilings of the *hyperbolic* plane.

Other tiling problems involve polyominoes. A polyomino is a connected planar region obtained by connecting finitely many unit squares along shared edges. It is unknown whether the following is undecidable (see [Rho05, p. 330], for instance):

Polyomino tiling.

> **input:** a polyomino P
> **question:** Can one tile the entire plane using translated and rotated copies of P?

5

4.3. Graph theory. Fix finite graphs G and H. Let $V(G)$ be the vertex set of G; define $V(H)$ similarly. A homomorphism from H to G is a (not necessarily injective) map $V(H) \to V(G)$ such that every edge of H maps to an edge of G. The homomorphism density $t(H,G)$ is the probability that a uniformly chosen random map $V(H) \to V(G)$ is a homomorphism. If $H_1 \dot{\cup} H_2$ denotes the disjoint union of graphs H_1 and H_2, then $t(H_1 \dot{\cup} H_2, G) = t(H_1, G)t(H_2, G)$ for any G.

There are certain known inequalities relating these densities. For instance, for the complete graph K_n on n vertices, elementary counting arguments similar to those in [Goo59] show that
$$t(K_3, G) \geq 2t(K_2, G)^2 - t(K_2, G),$$
or equivalently
$$t(K_3, G) - 2t(K_2 \dot{\cup} K_2, G) + t(K_2, G) \geq 0,$$
for every finite graph G. This suggests the following problem:

Linear inequalities between graph homomorphism densities.

    input: $k \in \mathbb{Z}_{\geq 0}$, finite graphs $H_1, \ldots, H_k$, and integers $a_1, \ldots, a_k$
    question: Does $a_1 t(H_1, G) + \cdots + a_k t(H_k, G) \geq 0$ hold for all finite graphs G?

H. Hatami and S. Norine proved this problem undecidable by relating it to Hilbert's tenth problem [HN11, Theorem 2.12].

5. Matrix semigroups

5.1. Matrix mortality. Given a finite list of square integer matrices, there are many ways to form products, especially if the factors may be repeated. Can one decide whether some product yields the zero matrix $\mathbf{0}$? More formally, we have the following:

Matrix mortality problem.

    input: $n \in \mathbb{Z}_{\geq 0}$ and a finite set S of $n \times n$ integer matrices
    question: Does the multiplicative semigroup generated by S contain $\mathbf{0}$?

M. Paterson proved that this problem is undecidable, even for sets of 3×3 matrices, via reduction to the Post correspondence problem [Pat70]. Subsequent work showed that it is undecidable also for sets consisting of seven 3×3 matrices [HHH07, Corollary 1] and for sets consisting of two 21×21 matrices [HHH07, Theorem 11]. Whether there exists an algorithm for sets of 2×2 matrices remains an open problem. For a more detailed introduction to the matrix mortality problem, see [HH01].

5.2. Freeness. One can ask, given n and S, whether distinct finite sequences of matrices in S yield distinct products, i.e., whether the semigroup generated by S is free. This turns out to be undecidable too, and already for sets of 3×3 matrices [KBS91]. In fact, sets of fourteen 3×3 matrices suffice for undecidability [HHH07, Theorem 13].

5.3. Finiteness. Can one decide whether the semigroup generated by S is finite? This time the answer turns out to be yes, as was proved independently by G. Jacob [Jac78, Jac77] and by A. Mandel and I. Simon [MS77].

Let us outline a proof. The main step consists of showing that there is a computable bound $f(n, s)$ for the size of any finite semigroup of $M_n(\mathbb{Z})$ generated by s matrices. Now for any $r \geq 1$, let P_r be the set of products of length at most r of matrices in S. Start computing

P_1, P_2, and so on. If $\#P_1 < \cdots < \#P_N$ for $N = f(n, s) + 1$, then $\#P_N > f(n, s)$, so the semigroup is infinite. Otherwise $P_r = P_{r+1}$ for some $r < N$, in which case the semigroup equals P_r and hence is finite.

The algorithm can be extended to decide finiteness of a finitely generated semigroup of $M_n(k)$ for any finitely generated field k presented as an explicit finite extension of $\mathbb{F}_p(t_1, \ldots, t_d)$ or $\mathbb{Q}(t_1, \ldots, t_d)$.

5.4. **Powers of a single matrix.** There are even some nontrivial questions about semigroups generated by one matrix! Given $A \in M_k(\mathbb{Z})$, can one decide whether there exists $n \in \mathbb{Z}_{>0}$ such that the upper right corner of A^n is 0? This problem, whose undecidability status is unknown, is equivalent to the following:

Zero in a linear recursive sequence.

> **input:** a linear recursive sequence of integers $(x_n)_{n \geq 0}$, specified by giving $x_0, \ldots, x_{k-1} \in \mathbb{Z}$ and $a_0, \ldots, a_{k-1} \in \mathbb{Z}$ such that $x_{n+k} = a_{k-1}x_{n+k-1} + \cdots + a_0 x_n$ for all $n \geq 0$
> **question:** Does there exist n such that $x_n = 0$?

This is known also as Skolem's problem, since Skolem proved that $\{n : x_n = 0\}$ is a union of a finite set and finitely many arithmetic progressions [Sko34]. See [HHHK05].

6. Group theory

Motivated by topology, M. Dehn [Deh11] asked three questions about groups:

1. Is there an algorithm to recognize the identity of a group?
2. Is there an algorithm to decide whether two given elements of a group are conjugate?
3. Is there an algorithm to decide whether two given groups are isomorphic?

Dehn formulated the questions precisely, except for the precise notion of algorithm.

6.1. **Finitely presented groups.** To make sense of such questions, one must specify how a group is presented and how an element is presented. A natural choice is to describe a group by means of a finite presentation such as

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

This example describes the group of symmetries of an equilateral triangle as being generated by a $120°$ rotation r and a reflection t, and lists relations satisfied by r and t such that all other relations are consequences of these. More formally, if $n \in \mathbb{Z}_{\geq 0}$, and F_n is the free group on n generators, and R is a finite subset of F_n, and H is the smallest normal subgroup of F_n containing R, then we may form the quotient group F_n/H. Any group arising in this way is called a finitely presented (f.p.) group. An element of an f.p. group can be specified by giving a word in the generators, i.e., a finite sequence of the generators and their inverses, such as $rtr^{-1}r^{-1}ttt^{-1}$.

6.2. **The word problem.** For each fixed f.p. group G (or more precisely, for each such group equipped with a particular presentation), we have the following:

Word problem for an f.p. group G.

> **input:** word w in the generators of G
> **question:** Does w represent 1 in G?

The decidability of the word problem depends only on the isomorphism type of the group, and not on the presentation. There are many classes of groups for the word problem is decidable: finite groups, f.p. abelian groups, and free groups on finitely many generators, for instance. (For free groups, one algorithm is to cancel pairs of adjacent inverse symbols repeatedly for as long as possible; the resulting reduced word represents 1 if and only if it is empty.)

But in the 1950s, P.S. Novikov [Nov55] and W. Boone [Boo59] independently proved that there is an f.p. group for which the word problem is undecidable. The analogue for f.p. semigroups had been proved earlier, by Post [Pos47] and A. Markov [Mar47, Mar51]; one proof of this goes through the undecidability of another word problem, namely that for semi-Thue systems, which can also be used to prove undecidability of the Post correspondence problem. Ultimately, the proofs of all these results are via reduction to the halting problem: Novikov and Boone essentially showed, that for a certain f.p. group G, one could associate to any computer program p a word w in the generators of G such that w represents $1 \in G$ if and only if p halts.

The undecidability of the word problem admits another proof, using the Higman embedding theorem, which we state below after introducing a definition. A finitely generated group is called recursively presented if it has the form F_n/H, where H is the smallest normal subgroup of F_n containing a given subset R, which is no longer required to be finite, but is instead required to be listable. Amazingly, it is possible to characterize such groups without mentioning computability:

Higman embedding theorem ([Hig61]). *A finitely generated group is recursively presented if and only if it can be embedded in a finitely presented group.*

The Higman embedding theorem implies the existence of an f.p. group P with undecidable word problem, as we now explain. First, it is rather easy to construct a recursively presented group for which the word problem is undecidable: for instance, if S is any non-computable listable set of positive integers, then one can show that in the recursively presented group

$$G_S := \langle a, b, c, d \mid a^n b a^{-n} = c^n d c^{-n} \text{ for all } n \in S \rangle,$$

$a^n b a^{-n} c^n d^{-1} c^{-n}$ represents 1 if and only if $n \in S$, so G_S has an undecidable word problem. By the Higman embedding theorem, G_S embeds in some finitely presented group P, which therefore has an undecidable word problem too.

6.3. **The conjugacy problem.** For each fixed f.p. group G, we have another problem:

Conjugacy problem for an f.p. group G.

    input: words w_1, w_2 in the generators of G
    question: Do w_1 and w_2 represent conjugate elements of G?

The word problem can be viewed as the subproblem of the conjugacy problem consisting of the instances for which w_2 is the empty word, which represents 1. Thus the conjugacy problem for G is at least as hard as the word problem for G, which means that it is easier (or at least no harder) to find a G for which the conjugacy problem is undecidable. In fact, P.S. Novikov published a proof of the existence of an f.p. group for which the conjugacy problem is undecidable before publishing the result on the word problem, and this earlier proof is much simpler [Nov54].

The inequality above between the difficulties of the two problems is the only one, in a sense that can be made precise using basic notions of computability theory, namely the notions of c.e. degrees of unsolvability and Turing reducibility $\leq_T$:

Theorem 6.1 ([Col72]). *Given c.e. degrees W and C such that $W \leq_T C$, there exists an f.p. group G for which the word problem has degree W and the conjugacy problem has degree C.*

This means that given c.e. subsets W and C of $\mathbb{N}$ such that the membership problem for W is decidable given an oracle for the membership problem for C, there exists an f.p. group G such that the word problem for G can be solved using an oracle for membership in W and vice versa, and the conjugacy problem for G can be solved using an oracle for membership in C and vice versa.

6.4. **Properties of groups.** Instead of fixing an f.p. group G, one can ask about algorithms that accept a finite presentation as input and try to decide whether the group it defines has a given property. For a wide variety of natural properties, the decision problem turns out to be undecidable. To make this precise, define a Markov property to be a property P of f.p. groups, depending only on the isomorphism type of the group, not on the presentation, such that

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

Examples are the properties of being trivial, finite, abelian, nilpotent, solvable, free, or torsion-free, because all these properties are inherited by subgroups. The property of having a decidable word problem is yet another Markov property, for the same reason!

Using the undecidability of the word problem, S.I. Adian [Ady57a, Ady57b] and M. Rabin [Rab58] proved the following:

Theorem 6.2. *For any Markov property P, it is impossible to decide whether an f.p. group G has P.*

Corollary 6.3. *It is impossible to decide whether a finite presentation describes the trivial group.*

Deciding triviality is a subproblem of the general problem of deciding whether two finite presentations define isomorphic groups, so the isomorphism problem is undecidable too.

For a more extended survey of undecidability in group theory, see [Mil92].

7. TOPOLOGY

7.1. **The homeomorphism problem.** Given two manifolds, can one decide whether they are homeomorphic? As usual, to make sense of such a question, we need to specify how a manifold is described. Since every compact smooth manifold can be triangulated, a natural choice is to use finite simplicial complexes to represent manifolds.

Homeomorphism problem.

> **input:** finite simplicial complexes M and N representing smooth manifolds
> **question:** Are M and N homeomorphic?

(One could alternatively replace homeomorphic by PL-homeomorphic, where PL stands for piecewise-linear.)

Given a finite simplicial complex M representing a compact manifold, one obtains a sub-problem of the homeomorphism problem by fixing the first input to be M:

Recognizing M.

> **input:** a finite simplicial complex N representing a smooth manifold
> **question:** Is N homeomorphic to M?

One can also restrict these problems according to dimension. For $d \leq 3$, the homeomorphism problem for d-folds turns out to be decidable, because of classification theorems; for $d = 3$, this uses the work of G. Perelman on W. Thurston's geometrization conjecture. But for each $d \geq 4$, the homeomorphism problem for d-folds is undecidable, as was proved by Markov [Mar58]. Moreover, S.P. Novikov (the son of P.S. Novikov!) proved that recognizing whether a finite simplicial complex is homeomorphic to the d-sphere S^d is an undecidable problem for each $d \geq 5$ (a proof appears in the appendix to [VKF74]). From this, one can prove that for any fixed compact d-fold M with $d \geq 5$, recognizing whether a finite simplicial complex is homeomorphic to M is undecidable.

All these results are proved by reduction to the undecidability results for f.p. groups. We now sketch the proofs of the unrecognizability results. (For a survey with more details, see [Wei05, Chapter 2].) Fix $d \geq 5$. Choose an f.p. group G with undecidable word problem. From G and a word w in the generators of G, one can build an f.p. group G_w such that G_w is trivial if and only if w represents 1, and such that the first and second homology groups $H^1(G_w)$ and $H^2(G_w)$ are trivial. These conditions on H^1 and H^2 of an f.p. group are necessary and sufficient for there to exist a homology sphere (a compact d-manifold with the same homology as S^d) with that fundamental group. In fact, one can effectively construct a finite simplicial complex X_w representing such a homology sphere with fundamental group G_w. Now:

- If w represents 1, then G_w is trivial, and X_w is a simply connected homology sphere, but in dimensions $d \geq 5$ a theorem of S. Smale [Sma61] implies that any such space is homeomorphic to S^d.
- If w does not represent 1, then X_w has nontrivial fundamental group, so X_w is not homeomorphic to S^d.

Hence, if we had an algorithm to recognize whether a finite simplicial complex is homeomorphic to S^d, it could be used to solve the word problem for G, a contradiction. Thus recognizing S^d is an undecidable problem.

Next suppose that M is *any* compact d-fold for $d \geq 5$. The connected sum $M \# X_w$ is obtained by punching a small hole in each of M and X_w and connecting them with a thin cylinder. This construction can be done effectively on finite simplicial complexes. The fundamental group $\pi_1(M \# X_w)$ is the free product of the groups $\pi_1(M)$ and $\pi_1(X_w)$. A group-theoretic theorem states that a free product $G * H$ of finitely generated groups can be isomorphic to G only if H is trivial. Now:

- If w represents 1, then X_w is homeomorphic to S^d, and $M \# X_w$ is homeomorphic to M.
- If w does not represent 1, then $M \# X_w$ does not even have the same fundamental group as M.

Hence, if we had an algorithm to recognize M, it could be used to solve the word problem for G, a contradiction.

Question 7.1. Is S^4 recognizable?

Remark 7.2. P. Seidel used similar ideas to find undecidable problems in *symplectic* geometry [Sei08, Corollary 6.8].

7.2. **Am I a manifold?** We have seen that it is impossible to recognize whether two manifolds represented by given finite simplicial complexes are homeomorphic. Even worse, one cannot even decide whether a finite simplicial complex represents a manifold! In other words, the following problem is undecidable:

Manifold detection.

  input: finite simplicial complex M
  question: Is M homeomorphic to a manifold?

Let us prove the undecidability by embedding the word problem in this problem. Recall that in Section 7.1, we constructed a finite simplicial complex X_w, in terms of a word w in the generators of an f.p. group G with unsolvable word problem, such that

- if w represents 1, then X_w is homeomorphic to a sphere S^d, and
- if w does not represent 1, then X_w is a manifold with nontrivial fundamental group.

The suspension SX_w of X_w is the simplicial complex whose vertices are those of X_w together with two new points a and b, and set of faces is $\bigcup_{\Delta \in X_w} \{\Delta, \Delta \cup \{a\}, \Delta \cup \{b\}\}$. Geometrically, one may realize X_w in a hyperplane in $\mathbb{R}^n$, and a and b as points on either side of the hyperplane; then SX_w is the union of the line segments connecting a point of $\{a, b\}$ to a point of the realization of X_w. Now:

- If w represents 1, then X_w is homeomorphic to a sphere S^d, and SX_w is homeomorphic to a sphere S^{d+1}.
- If w does not represent 1, then X_w has nontrivial fundamental group, so SX_w contains loops arbitrarily close to a with nontrivial class in the fundamental group of $SX_w - \{a, b\}$, so SX_w is not locally euclidean at a.

Thus SX_w is homeomorphic to a manifold if and only if w represents 1. Therefore no algorithm can decide whether a given finite simplicial complex represents a manifold.

7.3. **Knot theory.** A knot is a smooth embedding of the circle S^1 in $\mathbb{R}^3$. Two knots are equivalent if there is an ambient isotopy that transforms one into other; loosely speaking, this means that there is a smoothly varying family of diffeomorphisms of $\mathbb{R}^3$, parametrized by an interval, starting with the identity and ending with a diffeomorphism that maps one knot onto the other.

How do we describe a knot in a way suitable for input into a computer? A knot may be represented by a finite sequence of distinct points in $\mathbb{Q}^3$: the knot is obtained by connecting the points in order by line segments, the last of which connects the last point back to the first point (we assume that each segment intersects its neighbors only at its endpoints and intersects other segments not at all, and the piecewise-linear curve should then be rounded at the vertices so as to obtain a smooth curve).

Knot equivalence problem.

> **input:** knots K_1 and K_2, each represented by a finite sequence in $\mathbb{Q}^3$
> **question:** Are K_1 and K_2 equivalent?

W. Haken constructed an algorithm to decide whether a knot was unknotted [Hak61], and for the general problem he outlined an approach, the last step of which was completed by G. Hemion [Hem79]. Thus the knot equivalence problem is decidable!

One can also consider knots in higher dimension. An n-dimensional knot is a smooth embedding of S^n in $\mathbb{R}^{n+2}$ (or S^{n+2}), and one can define equivalence as before. Any embedding equivalent to the standard embedding of S^n as the unit sphere in a hyperplane in $\mathbb{R}^{n+2}$ is called unknotted. A. Nabutovsky and S. Weinberger prove that the problem of deciding whether an n-dimensional knot is unknotted is undecidable for $n \geq 3$ [NW96]. Since this is a subproblem of the equivalence problem for n-dimensional knots, the latter is undecidable too.

Nabutovsky and Weinberger leave open the following question:

Question 7.3. Is the equivalence problem for 2-dimensional knots decidable?

See [Soa04] for an exposition of some other undecidable problems in topology and differential geometry.

8. NUMBER THEORY

8.1. **Hilbert's tenth problem.** One of the 23 problems in a list that Hilbert published after a famous lecture in 1900 asked for an algorithm to decide the solvability of diophantine equations:

Hilbert's tenth problem.

> **input:** a multivariable polynomial $f \in \mathbb{Z}[x_1, \ldots, x_n]$
> **question:** Does there exist $\vec{a} \in \mathbb{Z}^n$ with $f(\vec{a}) = 0$?

This was eventually proved undecidable by Yu. Matiyasevich [Mat70]. To explain more, we need a definition. Call a subset A of $\mathbb{Z}$ diophantine if there exists a polynomial $p(t, \vec{x}) \in \mathbb{Z}[t, x_1, \ldots, x_n]$ such that

$$A = \{a \in \mathbb{Z} : (\exists \vec{x} \in \mathbb{Z}^n) \, p(a, \vec{x}) = 0\}.$$

In other words, if one views $p(t, \vec{x}) = 0$ as a family of diophantine equations in the variables $x_1, \ldots, x_n$ depending on a parameter t, then A is the set of parameter values that yield a solvable diophantine equation.

It is easy to see that diophantine sets are listable. What is remarkable is that the converse holds:

Theorem 8.1 (conjectured in [Dav53, p. 35], proved in [Mat70]). *A subset of $\mathbb{Z}$ is diophantine if and only if it is listable.*

Work of M. Davis, H. Putnam, and J. Robinson culminating in [DPR61] proved the analogue for exponential diophantine equations, in which polynomials are replaced by expressions built up from integers using not only addition and multiplication, but also exponentiation. Matiyasevich then showed how to express exponentiation in diophantine terms, to complete the proof of Theorem 8.1.

Theorem 8.1 immediately yields a negative answer to Hilbert's tenth problem, because there are listable subsets A of $\mathbb{Z}$ for which there is no algorithm to decide whether a given integer belongs to A (see Section 3.2). The role played by Theorem 8.1 for Hilbert's tenth problem is similar to the role played by the Higman embedding theorem (Section 6.2) for the word problem.

8.2. **Hilbert's tenth problem for other rings.** After the negative answer to Hilbert's tenth problem, researchers turned to variants in which the ring $\mathbb{Z}$ is replaced by some other commutative ring, such as $\mathbb{Q}$, or the ring of integers $\mathcal{O}_k$ of a fixed number field.

8.2.1. *The field of rational numbers.* The problem for $\mathbb{Q}$ is equivalent to the problem of deciding whether an algebraic variety over $\mathbb{Q}$ has a rational point, because any variety is a finite union of affine varieties, and any system of equations $f_1(\vec{x}) = \cdots = f_m(\vec{x}) = 0$ is solvable over $\mathbb{Q}$ if and only if the single equation $f_1(\vec{x})^2 + \cdots + f_n(\vec{x})^2 = 0$ is. It is still not known whether an algorithm exists for this problem. The notion of a subset of $\mathbb{Q}$ being diophantine over $\mathbb{Q}$ can be defined as in the previous section, except with all variables running over $\mathbb{Q}$ instead of $\mathbb{Z}$. If the subset $\mathbb{Z}$ were diophantine over $\mathbb{Q}$, then an easy reduction to Matiyasevich's theorem would prove the undecidability of Hilbert's tenth problem for $\mathbb{Q}$. J. Koenigsmann [Koe10, Corollary 2], building on [Poo09], proved that the *complement* $\mathbb{Q} - \mathbb{Z}$ is diophantine over $\mathbb{Q}$; a generalization to number fields was recently proved by J. Park [Par12].

In hopes of finding an undecidable problem, one can make the problem harder, by asking for an algorithm to decide the truth of first-order sentences, such as

$$(\exists x)(\forall y)(\exists z)(\exists w) \quad (x \cdot z + 3 = y^2) \ \vee \ \neg(z = x + w).$$

Using the theory of quadratic forms over $\mathbb{Q}$, J. Robinson [Rob49] proved that the following decision problem is undecidable:

Decision problem for the first-order theory of $\mathbb{Q}$.

    input: a first-order sentence ϕ in the language of fields
    question: Is ϕ true when the variables run over elements of $\mathbb{Q}$?

8.2.2. *Rings of integers.* Recall that a number field is a finite extension k of $\mathbb{Q}$, and that the ring of integers $\mathcal{O}_k$ of k is the set of $\alpha \in k$ satisfying $f(\alpha) = 0$ for some monic $f(x) \in \mathbb{Z}[x]$. The problem for $\mathcal{O}_k$ is conjectured to have a negative answer for each k [DL78]. This has been proved for some k, namely when k is totally real [Den80], k is a quadratic extension of a totally real number field [DL78], or k has exactly one conjugate pair of nonreal embeddings [Phe88, Shl89]. Through arguments of the author and A. Shlapentokh [Poo02, Theorem 1; Shl08, Theorem 1.9(3)], certain statements about ranks of elliptic curves over number fields would imply a negative answer for every k, and such statements have been proved by B. Mazur and K. Rubin [MR10, §8] assuming a conjecture of I. Shafarevich and J. Tate.

For more about Hilbert's tenth problem and its variants, see the survey articles [DMR76, Maz94, Poo08], the books [Mat93, DLPVG00, Shl07], the website [Vse], and the movie [Csi08].

9. ANALYSIS

9.1. **Inequalities.** Given a real-valued function on $\mathbb{R}$ or on $\mathbb{R}^n$, can one decide whether it is nonnegative everywhere? The answer depends on the kind of functions allowed as input.

9.1.1. *Real polynomials.* For polynomials in any number of variables, A. Tarski showed that the answer is yes (to make sense of this, one should restrict the input to have coefficients in $\mathbb{Q}$ or in the field $\mathbb{R} \cap \overline{\mathbb{Q}}$ of real algebraic numbers, so that the polynomial admits a finite encoding suitable for a Turing machine). In fact, Tarski [Tar51] gave a decision procedure, based on elimination of quantifiers for $\mathbb{R}$ in the language of ordered fields, for the following more general problem:

Decision problem for the first-order theory of the ordered field $\mathbb{R}$.

    input: a first-order sentence ϕ in the language of ordered fields
    question: Is ϕ true when the variables run over elements of $\mathbb{R}$?

9.1.2. *Adjoining the exponential function.* If one tries to extend this by allowing expressions involving also the real exponential function, then one runs into questions of transcendental number theory whose answer is still unknown. For example, can one decide for which rational numbers r, s, t the equation

$$e^{e^r} + e^s + t = 0$$

holds? But assuming Schanuel's conjecture [Lan66, pp. 30–31], which rules out such "accidental identities", A. Macintyre and A. Wilkie [MW96] gave a decision algorithm for all first-order sentences for $\mathbb{R}$ with exponentiation in addition to the usual operations and $\leq$.

Remark 9.1. In contrast, for the set $\mathscr{E}$ of *complex* functions built up from integers and z using addition, multiplication, and composing with e^z, A. Adler proved that it is impossible to decide whether a finite list of functions in $\mathscr{E}$ has a common zero in $\mathbb{C}$ [Adl69, Theorem 1]. This can be proved by reduction to Hilbert's tenth problem, using two observations:

1. One can characterize $\mathbb{Q}$ in $\mathbb{C}$ as the set of ratios of zeros of $e^z - 1$.
2. One can characterize $\mathbb{Z}$ as the set of $x \in \mathbb{Q}$ such that there exists $z \in \mathbb{C}$ with $e^z = 2$ and $e^{zx} \in \mathbb{Q}$.

9.1.3. *Adjoining the sine function.* Adjoining most other transcendental functions leads quickly to undecidable problems. For example, consider the following, a variant of a theorem of D. Richardson:

Theorem 9.2 (cf. [Ric68, §1, Corollary to Theorem One]). *There is a polynomial $P \in \mathbb{Z}[t, x_1, \ldots, x_n, y_1, \ldots, y_n]$ such that for each $a \in \mathbb{Z}$, the real analytic function*

$$P(a, x_1, \ldots, x_n, \sin \pi x_1, \ldots, \sin \pi x_n)$$

on $\mathbb{R}^n$ is either everywhere greater than 1, or else assumes values less than -1 and values greater than 1, but it is impossible to decide which, given a.

Sketch of proof. By Theorem 8.1, we can find a polynomial $p(t, \vec{x}) \in \mathbb{Z}[t, x_1, \ldots, x_n]$ defining a diophantine subset A of $\mathbb{Z}$ that is not computable. A little analysis shows that there is another polynomial $G \in \mathbb{Z}[t, x_1, \ldots, x_n]$ whose values are positive and growing so quickly that if we define

$$L_a(\vec{x}) := -2 + 4p(a, \vec{x})^2 + G(a, \vec{x}) \sum_{i=1}^{n} \sin^2 \pi x_i,$$

then $L_a(\vec{x}) \leq 1$ holds only in tiny neighborhoods of the integer solutions to $p(a, \vec{x}) = 0$. If $a \in A$, then such integer solutions exist and L_a takes the value -2 at those integer solutions and large positive values at some points with half-integer coordinates; otherwise, $L_a(\vec{x}) > 1$ on $\mathbb{R}^n$. $\qquad\square$

Remark 9.3. Richardson's original statement and proof of Theorem 9.2 were slightly more involved because they came before Hilbert's tenth problem had been proved undecidable. Richardson instead had to use the undecidability result for exponential diophantine equations mentioned in Section 8.1.

M. Laczkovich [Lac03] found a variant of Theorem 9.2 letting one use $\sin x_i$ in place of $\sin \pi x_i$ for all i. Also, there exist functions $h \colon \mathbb{R} \to \mathbb{R}^n$ with dense image, such as

$$h(x) := (x \sin x, x \sin x^3, \ldots, x \sin x^{2n-1}),$$

(this function, used by J. Denef and L. Lipshitz in [DL89, Lemma 3.2], is a simpler version of one used in [Ric68, §1, Theorem Two]). By composing a multivariable function with h, one obtains analogues of Theorem 9.2 for functions of *one* variable:

Theorem 9.4 (cf. [Lac03, Theorem 1], which improves upon [Ric68, Corollary to Theorem Two]). *Let $\mathscr{S}$ be the set of functions $\mathbb{R} \to \mathbb{R}$ built up from integers and x using addition, multiplication, and composing with* $\sin$*. Then it is impossible to decide, given $f \in \mathscr{S}$, whether f is everywhere nonnegative. Deciding whether f is everywhere positive or whether f has a zero are impossible too.*

For later use, we record the fact that there exist functions $F_a \in \mathscr{S}$, depending in a computable way on an integer parameter a, such that either $F_a(x) > 1$ on $\mathbb{R}$, or else $F_a(x)$ assumes values less than -1 and values greater than 1, but it is impossible to decide which.

9.2. **Equality of functions.** Automatic homework graders sometimes need to decide whether two expressions define the same function. But deciding whether $|f(\vec{x})|$ is the same function as $f(\vec{x})$ amounts to deciding whether $f(\vec{x})$ is everywhere nonnegative, which, by Section 9.1.3, is impossible for $f \in \mathbb{Z}[x_1, \ldots, x_n, \sin x_1, \ldots, \sin x_n]$ or for $f \in \mathscr{S}$ (cf. [Ric68, §2, Theorem Two]).

For further undecidability results in analysis deduced from the negative answer to Hilbert's tenth problem, see [Adl69, DL89, SR97].

9.3. **Integration.** There exists an entire function on $\mathbb{C}$ whose derivative is e^{z^2}. But work of J. Liouville shows that no such function is expressible by an elementary formula, in the following sense.

For a connected open subset U of $\mathbb{C}$, let $\mathcal{M}(U)$ be the field of meromorphic functions on U. Say that a function $g \in \mathcal{M}(U)$ is elementary if it belongs to the last field K_n in a tower $\mathbb{C}(z) = K_0 \subset K_1 \subset \cdots \subset K_n$ of subfields of $\mathcal{M}(U)$ such that each extension K_{i+1} over K_i is either algebraic or obtained by adjoining to K_i either e^f or a branch of $\log f$ defined on U for some $f \in K_i$. For instance, the trigonometric functions and their inverses on a suitable U are elementary functions.

Liouville proved a general theorem [Lio35, §VII] that implies that there is no elementary antiderivative of e^{z^2} on any U. (Earlier, Liouville proved that certain algebraic functions, such as $(1 + x^4)^{-1/2}$, have no elementary antiderivative [Lio33].) See [Ros72] for an account of Liouville's methods.

Can one decide whether a given elementary function has an elementary antiderivative? Building on the work of Liouville, R. Risch sketched a positive answer to a precise version of this question [Ris70]. To obtain a positive answer, the question must be formulated carefully to avoid having to answer questions about whether a constant or function is identically 0.

For example, it is not clear whether we can decide, given rational numbers r, s, t, whether $\int (e^{e^r} + e^s + t)e^{x^2}\, dx$ is an elementary function.

Risch avoids this difficulty by restricting attention to functions in a tower of fields in which the constant field is an algebraically closed field of characteristic 0 with a specified finite transcendence basis, and in which each successive extension in the tower is either an explicit algebraic extension or an extension adjoining $\exp f$ or a branch of $\log f$ that does not change the field of constants.

Remark 9.5. If we try to generalize by allowing expressions involving the absolute value function $|\,|$, we encounter undecidability, as we now explain (cf. [Ric68, §2, Theorem Three]). Define

$$(2) \qquad \sigma(x) := \frac{1}{2}\left(|x| - |x-1| + 1\right) = \begin{cases} 0, & \text{if } x \leq 0 \\ x, & \text{if } 0 < x < 1 \\ 1, & \text{if } x \geq 1. \end{cases}$$

Recall the functions F_a at the end of Section 9.1.3. Then $\sigma(-F_a(x))$ is either 0 on all of $\mathbb{R}$, or it agrees with 1 on some open interval, but we cannot decide which. Thus we cannot decide whether $\int \sigma(-F_a(x))e^{x^2}\, dx$ is an elementary function on all of $\mathbb{R}$.

Remark 9.6. Deciding whether an improper integral converges is undecidable too, as was observed by P. Wang [Wan74]. Specifically, we cannot decide whether

$$\int_{-\infty}^{\infty} \frac{1}{(x^2+1)F_a(x)^2}\, dx$$

converges.

9.4. Differential equations.
Consider algebraic differential equations (ADEs)

$$P(x, y, y', y'', \ldots, y^{(n)}) = 0$$

to be solved by a function y of x, where P is a polynomial with integer coefficients. Denef and Lipshitz [DL89, Theorem 4.1] proved that the following problem is undecidable:

Existence of solutions to algebraic differential equations.
  input: $P \in \mathbb{Z}[x, y_1, y_2, \ldots, y_n]$
  question: Does $P(x, y', y'', \ldots, y^{(n)})$ admit a real analytic solution on $[0, \infty)$?

It remains undecidable even if one restricts the input so as to allow only ADEs that have a unique analytic solution in a neighborhood of 0. The idea of the proof is to consider a function built up using sin as in Section 9.1.3 for which one cannot decide whether it is either everywhere positive, and then to show that its reciprocal satisfies an ADE.

Remark 9.7. To avoiding having to use π in the coefficients of P, Denef and Lipschitz observed that $\tan^{-1} x$ is a function satisfying an ADE such that $\lim_{x \to +\infty} \tan^{-1} x = \pi/2$. An alternative would be to use the approach of [Lac03] for eliminating π.

Remark 9.8. ADEs can behave strangely in other ways too. L. Rubel [Rub81] constructed a single explicit ADE whose solutions approximate any continuous function: more precisely, for any continuous functions $f\colon \mathbb{R} \to \mathbb{R}$ and $\epsilon\colon \mathbb{R} \to \mathbb{R}_{>0}$, there exists a C^∞ solution $g\colon \mathbb{R} \to \mathbb{R}$ to the ADE satisfying $|g(x) - f(x)| < \epsilon(x)$ for all $x \in \mathbb{R}$.

For other results and questions concerning existence and computability of solutions to differential equations, see [Jaś54, Adl69, Abe71, PER79, PER83, Rub83, DL84, Rub92].

10. Dynamical systems

Many nonlinear dynamical systems are capable of simulating universal Turing machines, and hence they provide undecidable problems.

10.1. **Dynamical systems on $\mathbb{R}^n$.** Call a map $\mathbb{R}^n \to \mathbb{R}^m$ affine linear if it is a linear map plus a constant vector. Call a map $f \colon \mathbb{R}^n \to \mathbb{R}^m$ piecewise affine linear if $\mathbb{R}^n$ can be partitioned into finitely many subsets U_i each defined by a finite number of affine linear inequalities such that $f|_{U_i}$ agrees with an affine linear map depending on i. Call such a map rational if all the coefficients of the affine linear polynomials involved are rational. Given such map f, let f^k be its kth iterate. C. Moore [Moo90] proved that the following problem is undecidable:

Point goes to origin in finite time.

> **input:** a rational piecewise affine linear map $f \colon \mathbb{R}^2 \to \mathbb{R}^2$ and a point $\vec{a} \in \mathbb{Q}^2$
> **question:** Does there exist k such that $f^k(\vec{a}) = \vec{0}$?

Similarly, H. Siegelmann and E. Sontag proved that neural nets can simulate a universal Turing machine: in particular, if $\sigma \colon \mathbb{R}^n \to \mathbb{R}^n$ is the map obtained by applying the function (2) coordinatewise, then there exists n and a specific matrix $A \in M_n(\mathbb{Z})$, for which it is impossible to decide, given a starting point $\vec{a} \in \mathbb{Q}^n$, whether some iterate of $\sigma(A\vec{x})$ maps $\vec{a}$ to $\vec{0}$ [SS95].

Instead of asking about the trajectory of one point, one can ask global questions about the dynamical system, such as whether every trajectory converges. V. Blondel, O. Bournez, P. Koiran, and J. Tsitsiklis prove that many such questions are undecidable for piecewise affine linear maps [BBKT01].

For further results relating dynamical systems and computability, see the survey article [BT00].

10.2. **Dynamical systems on the set of positive integers.** There are also undecidable problems concerning dynamics of maps $f \colon \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ such as

$$f(x) := \begin{cases} 3x + 1, & \text{if } x \text{ is odd} \\ x/2, & \text{if } x \text{ is even.} \end{cases}$$

The Collatz $3x + 1$ problem, which asks whether for every $n \in \mathbb{Z}_{>0}$, there exists k such that $f^k(n) = 1$, has been open since the 1930s [Lag85]; see [Lag10] for a recent compilation of articles on this subject. The following generalization has been proved undecidable:

Generalized Collatz problem.

> **input:** $m \in \mathbb{Z}_{>0}$, $a_0, \ldots, a_{m-1}, b_0, \ldots, b_{m-1} \in \mathbb{Q}$ such that the function f given by $f(x) = a_i x + b_i$ for $x \bmod m = i$ maps $\mathbb{Z}_{>0}$ to itself
> **question:** Is it true that for every $n \in \mathbb{Z}_{>0}$ there exists k such that $f^k(n) = 1$?

For this and related results, see the papers by J. Conway [Con72], by S. Kurtz and J. Simon [KS07], and by J. Endrullis, C. Grabmayer, and D. Hendriks [EGH09].

11. Probability

Consider a random walk on the set $(\mathbb{Z}_{\geq 0})^n$ of lattice points in the nonnegative orthant. At each time, the walker takes a step by adding a vector in $\{-1, 0, 1\}^n$. If $\vec{x} = (x_1, \ldots, x_n)$ is the current position, the vector to add is chosen with respect to a probability distribution Λ_S depending only on the set $S = \{i : x_i \neq 0\}$, and Λ_S is such that the walker never leaves the orthant. Suppose also that every probability in the description of each Λ_S is in $\mathbb{Q}$. Say that the random walk starting at $\vec{a}$ is stable if there exists $C > 0$ such that with probability 1 the walker returns to $\{\vec{x} : |\vec{x}| < C\}$ infinitely often.

Stability of random walks.

> **input:** $n \in \mathbb{Z}_{\geq 0}$, probability distributions Λ_S as above for $S \subseteq \{1, \ldots, n\}$, and $\vec{a} \in (\mathbb{Z}_{\geq 0})^n$
>
> **question:** Is the random walk starting at $\vec{a}$ stable?

D. Gamarnik [Gam02] proved that this problem is undecidable even if all the probabilities are 0 or 1! To do this, he showed that any Turing machine could be simulated by such a deterministic walk.

Moreover, many basic questions about the stationary distribution of a random walk as above turn out to be undecidable, even if one assumes that the stationary distribution exists [Gam07].

12. Algebraic geometry

12.1. **Rational sections.** K.H. Kim and F.W. Roush proved the undecidability of Hilbert's tenth problem for the field $\mathbb{C}(t_1, t_2)$ of rational functions in two variables [KR92]. (Strictly speaking, one should assume that the input has coefficients in $\overline{\mathbb{Q}}(t_1, t_2)$ instead of $\mathbb{C}(t_1, t_2)$, for the sake of encoding it for input into a Turing machine, but we will ignore this subtlety from now on.) By the same argument as in Section 8.2.1, Hilbert's tenth problem for $\mathbb{C}(t_1, t_2)$ is equivalent to the problem of deciding whether a $\mathbb{C}(t_1, t_2)$-variety over has a $\mathbb{C}(t_1, t_2)$-point (any pair of equations $f = g = 0$ can be converted to $f^2 + t_1 g^2 = 0$). K. Eisenträger [Eis04], using work of L. Moret-Bailly [MB05], generalized the Kim–Roush result to the function field of any fixed irreducible $\mathbb{C}$-variety S of dimension at least 2. Whether Hilbert's tenth problem for $\mathbb{C}(t)$ is undecidable is an open question, studied in J. Kollár's article [Kol08]. It is also open for the function field of each other curve over $\mathbb{C}$.

Let us return to the Kim–Roush result. By interpreting the "constants" t_1 and t_2 as variables, one can associate to each $\mathbb{C}(t_1, t_2)$-variety X a $\mathbb{C}$-variety Y equipped with a rational map $\pi \colon Y \dashrightarrow \mathbb{A}^2$. The $\mathbb{C}(t_1, t_2)$-points of X correspond to rational sections of π, i.e., rational maps $s \colon \mathbb{A}^2 \dashrightarrow Y$ such that $\pi \circ s$ is the identity. This dictionary translates the Kim–Roush result into the undecidability of the following problem:

Existence of rational sections.

> **input:** a $\mathbb{C}$-variety Y and a rational map $\pi \colon Y \dashrightarrow \mathbb{A}^2$
>
> **question:** Does π admit a rational section?

12.2. **Automorphisms.** Using the undecidability of Hilbert's tenth problem, one can show that it is impossible to decide, given a variety X, a point $x \in X$, and a subvariety $Z \subset X$, whether there exists an automorphism of X mapping x into Z [Poo11]. In fact, there are fixed X and x for which the problem for a variable input Z is undecidable. More precisely,

18

there is a smooth projective geometrically irreducible $\mathbb{Q}$-variety X and a point $x \in X(\mathbb{Q})$ such that the following problem is undecidable:

Automorphisms mapping a point into a subvariety.

> **input:** a smooth projective geometrically irreducible subvariety $Z \subset X$
> **question:** Does there exist an automorphism of X mapping x into Z?

Moreover, X can be chosen so that all its automorphisms over any field extension are already defined over $\mathbb{Q}$, so it does not matter whether we require the automorphisms to be defined over the base field.

On the other hand, the following question has remained open:

Question 12.1. Is there an algorithm to decide whether a given variety has a nontrivial automorphism?

Possibly related to this is the following:

Question 12.2. Given an f.p. group G, can one effectively construct a variety X_G whose automorphism group is G?

A positive answer to Question 12.2 would yield a negative answer to Question 12.1, since it is impossible to decide whether an f.p. group is trivial (Corollary 6.3).

12.3. **Isomorphism.** Given the undecidability of the homeomorphism problem for manifolds, it is natural to ask for the algebraic geometry analogue:

Variety isomorphism problem.

> **input:** two varieties X and Y over $\overline{\mathbb{Q}}$
> **question:** Is $X \simeq Y$?

The question of whether this problem might be undecidable was asked to the author by B. Totaro in 2007.

We stated the problem over $\overline{\mathbb{Q}}$, because most algebraic geometry is done over an algebraically closed field and we wanted the input to admit a finite description. Alternatively, we could work over an algebraically closed field $\overline{\mathbb{Q}(t_1, t_2, \ldots)}$ of countable transcendence degree over $\mathbb{Q}$; this would capture the essence of the problem over $\mathbb{C}$, since any pair of varieties over $\mathbb{C}$ may be simultaneously defined over a finitely generated subfield of $\mathbb{C}$ and the existence of an isomorphism is unaffected by enlarging the ground field from one algebraically closed field to another. One could also consider other fields, such as $\mathbb{Q}$, $\overline{\mathbb{F}}_p$, $\mathbb{F}_p$, or $\overline{\mathbb{F}_p(t_1, t_2, \ldots)}$. There is no field over which it is known whether one can solve the variety isomorphism problem.

12.4. **Birational equivalence.** It is also unknown whether there is an algorithm to decide whether two given varieties are birationally equivalent. On the other hand, given an explicit rational map, one can decide whether it is a birational map, and whether it is an isomorphism.

Remark 12.3. For algebraic geometers: if at least one of the varieties X and Y over $\overline{\mathbb{Q}}$ is of general type, then the set of birational maps $X \dashrightarrow Y$ is finite and computable (see below), and we can decide which of these birational maps are isomorphisms, and hence solve the variety isomorphism problem in this restricted setting. H. Matsumura proved that the birational automorphism group of a variety of general type is finite [Mat63]. The set

of birational maps $X \dashrightarrow Y$ is either empty or a principal homogeneous space under this group, so it is finite too. Let us sketch an algorithm for computing this set. For $n = 1, 2, \ldots$, compute the maps determined by the pluricanonical linear system $|nK|$ for X and Y until an n is found for which at least one of the two maps is birational onto its image. Then the other must be too and the linear systems must have the same dimension, say n, since otherwise we know already that $X \not\simeq Y$. The birational maps are then in bijection with the linear automorphisms of $\mathbb{P}^n$ mapping one canonical image to the other, and we can find equations for the locus of these automorphisms as a (finite) subscheme of PGL_{n+1}.

13. Algebra

13.1. Commutative algebra.
If we restrict the variety isomorphism problem to the category of *affine* varieties, we obtain, equivalently, the isomorphism problem for finitely generated $\overline{\mathbb{Q}}$-algebras. Here each algebra can be presented as $\overline{\mathbb{Q}}[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$ by specifying n and explicit polynomials $f_1, \ldots, f_m$.

One can replace $\overline{\mathbb{Q}}$ by other rings of constants (whose elements can be encoded for computer input). For example, taking $\mathbb{Z}$ yields the following problem:

Commutative ring isomorphism problem.

> **input:** two finitely generated commutative rings A and B
> **question:** Is $A \simeq B$?

The undecidability status of this problem is unknown. In fact, the status is unknown also for the isomorphism problem for finitely generated commutative algebras over any fixed nonzero commutative ring (with elements encoded such that addition and multiplication are computable).

13.2. Noncommutative algebra.
The noncommutative analogue of the previous problem is undecidable, as we now explain. Let $\mathbb{Z}\langle x_1, \ldots, x_n \rangle$ be the noncommutative polynomial ring (free associative algebra with 1) in n variables over $\mathbb{Z}$. A (possibly noncommutative) f.p. $\mathbb{Z}$-algebra is the quotient of $\mathbb{Z}\langle x_1, \ldots, x_n \rangle$ by the 2-sided ideal generated by a finite list of elements $f_1, \ldots, f_m$. 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 $G \simeq \{1\}$. So if there were an algorithm to decide whether two f.p. $\mathbb{Z}$-algebras were isomorphic, we could use it to decide whether an f.p. group is trivial, contradicting Corollary 6.3.

For other undecidable problems concerning noncommutative f.p. algebras, see [Ani85].

14. Games

14.1. Abstract games.
Given $m \geq 1$ and a computable function $W \colon \mathbb{N}^m \to \{A, B\}$, consider the two-player game of no chance in which

- the players (A and B) alternately choose natural numbers, starting with A, and ending after m numbers $x_1, \ldots, x_m$ have been chosen;
- there is perfect information (both players know the rules and can see all previously made choices); and
- the winner is $W(x_1, x_2, \ldots, x_m)$.

Many games can be fit into this framework.

A result of L. Kalmár [Kal28], building on work of E. Zermelo [Zer13] and D. König [Kön27], states that exactly one of the two players has a winning strategy. But:

Theorem 14.1. *It is impossible to decide, given m and 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. □

More surprising is the following result of Rabin [Rab57]:

Theorem 14.2. *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).*

Proof. Post [Pos44, §5] proved that there exists a simple set, i.e., a c.e. set $S \subset \mathbb{N}$ whose complement $\overline{S}$ is infinite but contains no infinite c.e. set. Fix such an S. Let $g \colon \mathbb{N} \to \mathbb{N}$ be a computable function with $g(\mathbb{N}) = S$. Consider the three-move game in which A wins if and only if $x_1 + x_2 = g(x_3)$.

Player B's winning strategy is to find $t \in \overline{S}$ with $t > x_1$, and to choose $x_2 = t - x_1$. A computable winning strategy $x_2 = w(x_1)$, however, would yield an infinite c.e. subset $\{x_1 + w(x_1) : x_1 \in \mathbb{N}\}$ of $\overline{S}$. □

Remark 14.3. Using the undecidability of Hilbert's tenth problem, J.P. Jones gave new proofs of these theorems using games in which W simply evaluates a given polynomial at the m-tuple of choices to decide who wins [Jon82].

R. Hearn [Hea06] proved that team games with imperfect information can be undecidable even if they have only *finitely* many positions! For an account of this work and a complexity analysis of many finite games, see [HD09].

14.2. **Chess.** R. Stanley [Sta10] asked whether the following problem is decidable:

Infinite chess.

> **input:** A finite list of chess pieces and their starting positions on a $\mathbb{Z} \times \mathbb{Z}$ chessboard
> **question:** Can White force mate?

(For a precise specification of the rules, and for related problems, see [BHS12].)

It is unknown whether this problem is decidable. On the other hand, D. Brumleve, J. Hamkins, and P. Schlicht [BHS12] showed that one *can* decide whether White can mate in n moves, if a starting configuration and n are given. This statement can be proved quickly by encoding each instance of the problem as a first-order sentence in Presburger arithmetic, which is the theory of $(\mathbb{N}; 0, 1, +)$. (Presburger arithmetic, unlike the theory of $(\mathbb{N}; 0, 1, +, \cdot)$, is decidable [Pre29].)

15. Final remarks

Each undecidable problem P we presented is at least as hard as the halting problem H, because the undecidability proof ultimately depended on encoding an arbitrary instance of

H as an instance of P. In the other direction, many of these problems could be solved if one could decide whether a certain search terminates; for these P, an arbitrary instance of P can be encoded as an instance of H. The problems for which both reductions are possible are called c.e. complete, and they are all of exactly the same difficulty with respect to Turing reducibility. For example, an algorithm for deciding whether a finitely presented group is trivial could be used to decide whether multivariable polynomial equations have integer solutions, and vice versa!

On the other hand, certain other natural problems are strictly harder than the halting problem. One such problem is the generalized Collatz problem of Section 10.2: see [KS07, EGH09].

References

[Abe71] Oliver Aberth, *The failure in computable analysis of a classical existence theorem for differential equations*, Proc. Amer. Math. Soc. **30** (1971), 151–156. MR0302982 (46 #2124) ↑9.4

[Adl69] Andrew Adler, *Some recursively unsolvable problems in analysis*, Proc. Amer. Math. Soc. **22** (1969), 523–526. MR0248020 (40 #1277) ↑9.1, 9.2, 9.4

[Ady57a] S. I. Adyan, *Unsolvability of some algorithmic problems in the theory of groups.*, Trudy Moskov. Mat. Obšč. **6** (1957), 231–298 (Russian). MR0095872 (20 #2370) ↑6.4

[Ady57b] _____, *Finitely presented groups and algorithms*, Dokl. Akad. Nauk SSSR (N.S.) **117** (1957), 9–12 (Russian). MR0095873 (20 #2371) ↑6.4

[Ber66] Robert Berger, *The undecidability of the domino problem*, Mem. Amer. Math. Soc. No. **66** (1966), 72. MR0216954 (36 #49) ↑4.2

[Ani85] David J. Anick, *Diophantine equations, Hilbert series, and undecidable spaces*, Ann. of Math. (2) **122** (1985), no. 1, 87–112, DOI 10.2307/1971370. MR799253 (87b:55008) ↑13.2

[BT00] Vincent D. Blondel and John N. Tsitsiklis, *A survey of computational complexity results in systems and control*, Automatica J. IFAC **36** (2000), no. 9, 1249–1274, DOI 10.1016/S0005-1098(00)00050-9. MR1834719 (2002c:93001) ↑10.1

[BBKT01] Vincent D. Blondel, Olivier Bournez, Pascal Koiran, and John N. Tsitsiklis, *The stability of saturated linear dynamical systems is undecidable*, J. Comput. System Sci. **62** (2001), no. 3, 442–462, DOI 10.1006/jcss.2000.1737. MR1824455 (2002d:03077) ↑10.1

[Boo59] William W. Boone, *The word problem*, Ann. of Math. (2) **70** (1959), 207–265. MR0179237 (31 #3485) ↑6.2

[BHS12] Dan Brumleve, Joel David Hamkins, and Philipp Schlicht, *The mate-in-n problem of infinite chess is decidable* (January 31, 2012). Preprint, `arXiv:1201.5597v2`. ↑14.2

[Chu36a] Alonzo Church, *An unsolvable problem of elementary number theory*, Amer. J. Math. **58** (1936), 345–363. ↑2, 3.2, 3.3

[Chu36b] _____, *A note on the Entscheidungsproblem*, J. Symbolic Logic **1** (1936), 40–41. ↑3.3

[Coh63] Paul Cohen, *The independence of the continuum hypothesis*, Proc. Nat. Acad. Sci. U.S.A. **50** (1963), 1143–1148. MR0157890 (28 #1118) ↑2

[Coh64] Paul J. Cohen, *The independence of the continuum hypothesis. II*, Proc. Nat. Acad. Sci. U.S.A. **51** (1964), 105–110. MR0159745 (28 #2962) ↑2

[Col72] Donald J. Collins, *Representation of Turing reducibility by word and conjugacy problems in finitely presented groups*, Acta Math. **128** (1972), no. 1-2, 73–90. MR0392539 (52 #13356) ↑6.1

[Con72] J. H. Conway, *Unpredictable iterations*, Proceedings of the 1972 Number Theory Conference, University of Colorado, Boulder, Colo., 1972. Held at the University of Colorado, Boulder, Colo., August 14–18, 1972; reprinted in Jeffrey C. Lagarias (ed.), *The ultimate challenge: the $3x + 1$ problem*, American Mathematical Society, Providence, RI, 2010. ↑10.2

[Csi08] George Csicsery, *Julia Robinson and Hilbert's tenth problem*, 2008. Documentary, Zala Films, `http://zalafilms.com/films/juliarobinson.html` . ↑8.2.2

[Cul96] Karel Culik II, *An aperiodic set of* 13 *Wang tiles*, Discrete Math. **160** (1996), no. 1-3, 245–251, DOI 10.1016/S0012-365X(96)00118-5. MR1417576 (97f:05045) ↑1, 4.2

[Dav53] Martin Davis, *Arithmetical problems and recursively enumerable predicates*, J. Symbolic Logic **18** (1953), 33–41. MR0055281 (14,1052c) ↑8.1

[Dav58] ———, *Computability and unsolvability*, McGraw-Hill Series in Information Processing and Computers, McGraw-Hill Book Co., Inc., New York, 1958. MR0124208 (23 #A1525) ↑3.3

[Dav77] ———, *Unsolvable problems*, Handbook of mathematical logic, North-Holland Publishing Co., Amsterdam. Edited by Jon Barwise; With the cooperation of H. J. Keisler, K. Kunen, Y. N. Moschovakis and A. S. Troelstra; Studies in Logic and the Foundations of Mathematics, Vol. 90, 1977, pp. 567–594. ↑1, 4.1

[DMR76] Martin Davis, Yuri Matiyasevich, and Julia Robinson, *Hilbert's tenth problem: Diophantine equations: positive aspects of a negative solution*, Mathematical developments arising from Hilbert problems (Proc. Sympos. Pure Math., Vol. XXVIII, Northern Illinois Univ., De Kalb, Ill., 1974), Amer. Math. Soc., Providence, R. I., 1976, pp. 323–378. (loose erratum). MR0432534 (55 #5522) ↑8.2.2

[DPR61] Martin Davis, Hilary Putnam, and Julia Robinson, *The decision problem for exponential diophantine equations*, Ann. of Math. (2) **74** (1961), 425–436. MR0133227 (24 #A3061) ↑8.1

[Deh11] M. Dehn, *Über unendliche diskontinuierliche Gruppen*, Math. Ann. **71** (1911), no. 1, 116–144 (German). ↑6

[Den80] J. Denef, *Diophantine sets over algebraic integer rings. II*, Trans. Amer. Math. Soc. **257** (1980), no. 1, 227–236, DOI 10.2307/1998133. MR549163 (81b:12031) ↑8.2.2

[DL78] J. Denef and L. Lipshitz, *Diophantine sets over some rings of algebraic integers*, J. London Math. Soc. (2) **18** (1978), no. 3, 385–391. MR518221 (80a:12030) ↑8.2.2

[DL84] ———, *Power series solutions of algebraic differential equations*, Math. Ann. **267** (1984), no. 2, 213–238, DOI 10.1007/BF01579200. MR738249 (85j:12010) ↑9.4

[DL89] ———, *Decision problems for differential equations*, J. Symbolic Logic **54** (1989), no. 3, 941–950, DOI 10.2307/2274755. MR1011182 (91b:03074) ↑9.1.3, 9.2, 9.4

[DLPVG00] Jan Denef, Leonard Lipshitz, Thanases Pheidas, and Jan Van Geel (eds.), *Hilbert's tenth problem: relations with arithmetic and algebraic geometry*, Contemporary Mathematics, vol. 270, American Mathematical Society, Providence, RI, 2000. Papers from the workshop held at Ghent University, Ghent, November 2–5, 1999. MR1802007 (2001g:00018) ↑8.2.2

[Eis04] Kirsten Eisenträger, *Hilbert's tenth problem for function fields of varieties over* ℂ, Int. Math. Res. Not. **59** (2004), 3191–3205. MR2097039 (2005h:11273) ↑12.1

[EGH09] Jörg Endrullis, Clemens Grabmayer, and Dimitri Hendriks, *Complexity of fractran and productivity*, Automated deduction—CADE-22, Lecture Notes in Comput. Sci., vol. 5663, Springer, Berlin, 2009, pp. 371–387. MR2550348 ↑10.2, 15

[Gam02] David Gamarnik, *On deciding stability of constrained homogeneous random walks and queueing systems*, Math. Oper. Res. **27** (2002), no. 2, 272–293, DOI 10.1287/moor.27.2.272.321. MR1908527 (2003c:90022) ↑11

[Gam07] ———, *On the undecidability of computing stationary distributions and large deviation rates for constrained random walks*, Math. Oper. Res. **32** (2007), no. 2, 257–265, DOI 10.1287/moor.1060.0247. MR2324425 (2008g:60131) ↑11

[Göd30] Kurt Gödel, *Die Vollständigkeit der Axiome des logischen Funktionenkalküls*, Monatsh. Math. Phys. **37** (1930), no. 1, 349–360, DOI 10.1007/BF01696781 (German); English transl., Kurt Gödel, *Collected works. Vol. I* (1986), 103–123. Publications 1929–1936; Edited and with a preface by Solomon Feferman. MR831941 (87h:01096). MR1549799 ↑3.3

[Göd31] K. Gödel, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter System I*, Monatshefte für Math. und Physik **38** (1931), 173–198; English transl., ———, *On formally undecidable propositions of Principia mathematica and related systems* (1992), viii+72. Translated from the German and with a preface by B. Meltzer; With an introduction by R. B. Braithwaite; Reprint of the 1963 translation. MR1160352 (93d:01094); reprinted in ———,

Collected works. Vol. I, The Clarendon Press, Oxford University Press, New York, 1986. Publications 1929–1936; Edited and with a preface by Solomon Feferman. MR831941 (87h:01096). ↑2, 3

[Göd40] Kurt Gödel, *The Consistency of the Continuum Hypothesis*, Annals of Mathematics Studies, no. 3, Princeton University Press, Princeton, N. J., 1940. MR0002514 (2,66c) ↑2

[Goo59] A. W. Goodman, *On sets of acquaintances and strangers at any party*, Amer. Math. Monthly **66** (1959), 778–783. MR0107610 (21 #6335) ↑4.3

[Hak61] Wolfgang Haken, *Theorie der Normalflächen*, Acta Math. **105** (1961), 245–375 (German). MR0141106 (25 #4519a) ↑7.3

[HH01] Vesa Halava and Tero Harju, *Mortality in matrix semigroups*, Amer. Math. Monthly **108** (2001), no. 7, 649–653, DOI 10.2307/2695274. MR1862104 ↑5.1

[HHH07] Vesa Halava, Tero Harju, and Mika Hirvensalo, *Undecidability bounds for integer matrices using Claus instances*, Internat. J. Found. Comput. Sci. **18** (2007), no. 5, 931–948, DOI 10.1142/S0129054107005066. MR2363737 (2008m:03091) ↑5.1, 5.2

[HHHK05] Vesa Halava, Tero Harju, Mika Hirvensalo, and Juhani Karhumäki, *Skolem's problem—on the border between decidability and undecidability*, TUCS Technical Reports, no. 683, Turku Centre for Computer Science, April 2005. Available at `http://tucs.fi/publications/view/?pub_id=tHaHaHiKa05a`. ↑5.4

[HN11] Hamed Hatami and Serguei Norine, *Undecidability of linear inequalities in graph homomorphism densities*, J. Amer. Math. Soc. **24** (2011), no. 2, 547–565, DOI 10.1090/S0894-0347-2010-00687-X. MR2748400 ↑4.3

[Hea06] Robert Aubrey Hearn, *Games, puzzles, and computation*, 2006. Ph.D. thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology. Available at `http://www.swiss.ai.mit.edu/~bob/hearn-thesis-final.pdf` . ↑14.1

[HD09] Robert A. Hearn and Erik D. Demaine, *Games, puzzles, and computation*, A K Peters Ltd., Wellesley, MA, 2009. MR2537584 ↑14.1

[Hem79] Geoffrey Hemion, *On the classification of homeomorphisms of 2-manifolds and the classification of 3-manifolds*, Acta Math. **142** (1979), no. 1-2, 123–155, DOI 10.1007/BF02395059. MR512214 (80f:57003) ↑7.3

[Hig61] G. Higman, *Subgroups of finitely presented groups*, Proc. Roy. Soc. Ser. A **262** (1961), 455–475. MR0130286 (24 #A152) ↑6.2

[HA28] D. Hilbert and W. Ackermann, *Grundzüge der theoretischen Logik*, Springer-Verlag, Berlin, 1928 (German); English transl. in *Principles of mathematical logic* (Robert E. Luce, ed.), translated by George G. Leckie Lewis M. Hammond F. Steinhardt, Chelsea, New York, 1950. Based on second German edition of 1938. ↑3.3

[Jac77] Gérard Jacob, *Un algorithme calculant le cardinal, fini ou infini, des demi-groupes de matrices*, Theoret. Comput. Sci. **5** (1977/78), no. 2, 183–204 (French, with English summary). MR0473075 (57 #12754) ↑5.3

[Jac78] ———, *La finitude des représentations linéaires des semi-groupes est décidable*, J. Algebra **52** (1978), no. 2, 437–459 (French, with English summary). MR0473071 (57 #12750) ↑5.3

[Jaś54] S. Jaśkowski, *Example of a class of systems of ordinary differential equations having no decision method for existence problems*, Bull. Acad. Polon. Sci. Cl. III. **2** (1954), 155–157. MR0063327 (16,103g) ↑9.4

[Jon82] J. P. Jones, *Some undecidable determined games*, Internat. J. Game Theory **11** (1982), no. 2, 63–70, DOI 10.1007/BF01769063. MR686391 (84b:90107) ↑14.3

[Kal28] Lázló Kalmár, *Zur Theorie der abstrakten Spiele*, Acta Sci. Math. Szeged **4** (1928/29), 65–85 (German); English transl., *The foundations of game theory, volume I* (1997), 247–262. ↑14.1

[Kar96] Jarkko Kari, *A small aperiodic set of Wang tiles*, Discrete Math. **160** (1996), no. 1-3, 259–264, DOI 10.1016/0012-365X(95)00120-L. MR1417578 (97f:05046) ↑4.2

[KR92] K. H. Kim and F. W. Roush, *Diophantine undecidability of* $\mathbb{C}(t_1, t_2)$, J. Algebra **150** (1992), no. 1, 35–44. MR1174886 (93h:03062) ↑12.1

[KBS91] David A. Klarner, Jean-Camille Birget, and Wade Satterfield, *On the undecidability of the freeness of integer matrix semigroups*, Internat. J. Algebra Comput. **1** (1991), no. 2, 223–226, DOI 10.1142/S0218196791000146. MR1128014 (92g:20093) ↑5.2

[Kle36] S. C. Kleene, *General recursive functions of natural numbers*, Math. Ann. **112** (1936), no. 1, 727–742, DOI 10.1007/BF01565439. MR1513071 ↑3.2

[Koe10] Jochen Koenigsmann, *Defining $\mathbb{Z}$ in $\mathbb{Q}$*, November 15, 2010. Preprint, `arXiv:1011.3424` . ↑8.2.1

[Kol08] János Kollár, *Diophantine subsets of function fields of curves*, Algebra Number Theory **2** (2008), no. 3, 299–311. MR2407117 ↑12.1

[Kön27] Dénes König, *Über eine Schlussweise aus dem Endlichen ins Unendliche*, Acta Sci. Math. Szeged **3** (1927), 121–130 (German). ↑14.1

[KS07] Stuart A. Kurtz and Janos Simon, *The undecidability of the generalized Collatz problem*, Theory and applications of models of computation, Lecture Notes in Comput. Sci., vol. 4484, Springer, Berlin, 2007, pp. 542–553. MR2374341 (2008m:03092) ↑10.2, 15

[Lac03] M. Laczkovich, *The removal of π from some undecidable problems involving elementary functions*, Proc. Amer. Math. Soc. **131** (2003), no. 7, 2235–2240 (electronic), DOI 10.1090/S0002-9939-02-06753-9. MR1963772 (2004d:03020) ↑9.1.3, 9.4, 9.7

[Lag85] Jeffrey C. Lagarias, *The $3x+1$ problem and its generalizations*, Amer. Math. Monthly **92** (1985), no. 1, 3–23, DOI 10.2307/2322189. MR777565 (86i:11043) ↑10.2

[Lag10] ———— (ed.), *The ultimate challenge: the $3x+1$ problem*, American Mathematical Society, Providence, RI, 2010. MR2663745 (2012a:11001) ↑10.2

[Lan66] Serge Lang, *Introduction to transcendental numbers*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1966. MR0214547 (35 #5397) ↑9.1.2

[Lio33] Joseph Liouville, *Premier et second memoire sur la détermination des intégrales dont la valeur est algébrique*, J. de l'École Polytech. **14** (1833), 124–148 and 149–193. ↑9.3

[Lio35] ————, *Mémoire sur l'intégration d'une classe de fonctions transcendentes*, J. reine angew. Math. **13** (1835), no. 2, 93–118. ↑9.3

[MW96] Angus Macintyre and A. J. Wilkie, *On the decidability of the real exponential field*, Kreiseliana, A K Peters, Wellesley, MA, 1996, pp. 441–467. MR1435773 ↑9.1.2

[MS77] Arnaldo Mandel and Imre Simon, *On finite semigroups of matrices*, Theoret. Comput. Sci. **5** (1977/78), no. 2, 101–111. MR0473070 (57 #12749) ↑5.3

[Mar08] Maurice Margenstern, *The domino problem of the hyperbolic plane is undecidable*, Theoret. Comput. Sci. **407** (2008), no. 1-3, 29–84, DOI 10.1016/j.tcs.2008.04.038. MR2462998 (2009m:52040) ↑4.1

[Mar47] A. Markov, *The impossibility of certain algorithms in the theory of associative systems. II*, Doklady Akad. Nauk SSSR (N.S.) **58** (1947), 353–356 (Russian). MR0023208 (9,321b) ↑6.2

[Mar51] ————, *The impossibility of certain algorithms in the theory of associative systems*, Doklady Akad. Nauk SSSR (N.S.) **77** (1951), 19–20 (Russian). MR0040231 (12,661e) ↑6.2

[Mar58] ————, *The insolubility of the problem of homeomorphy*, Dokl. Akad. Nauk SSSR **121** (1958), 218–220 (Russian). MR0097793 (20 #4260) ↑7.1

[Mat70] Yu. Matiyasevich, *The Diophantineness of enumerable sets*, Dokl. Akad. Nauk SSSR **191** (1970), 279–282 (Russian). MR0258744 (41 #3390) ↑2, 8.1, 8.1

[Mat93] Yuri V. Matiyasevich, *Hilbert's tenth problem*, Foundations of Computing Series, MIT Press, Cambridge, MA, 1993. Translated from the 1993 Russian original by the author; With a foreword by Martin Davis. MR1244324 (94m:03002b) ↑8.2.2

[Mat63] Hideyuki Matsumura, *On algebraic groups of birational transformations*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **34** (1963), 151–155. MR0159825 (28 #3041) ↑12.3

[Maz94] B. Mazur, *Questions of decidability and undecidability in number theory*, J. Symbolic Logic **59** (1994), no. 2, 353–371. MR1276620 (96c:03091) ↑8.2.2

[MR10] Barry Mazur and Karl Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181** (2010), 541–575. ↑8.2.2

[Mil92] Charles F. Miller III, *Decision problems for groups—survey and reflections*, Algorithms and classification in combinatorial group theory (Berkeley, CA, 1989), Math. Sci. Res. Inst. Publ., vol. 23, Springer, New York, 1992, pp. 1–59. MR1230627 (94i:20057) ↑6.4

[Moo90]   Cristopher Moore, *Unpredictability and undecidability in dynamical systems*, Phys. Rev. Lett. **64** (1990), no. 20, 2354–2357, DOI 10.1103/PhysRevLett.64.2354. MR1050259 (91b:58158) ↑10.1

[MB05]   Laurent Moret-Bailly, *Elliptic curves and Hilbert's tenth problem for algebraic function fields over real and p-adic fields*, J. reine angew. Math. **587** (2005), 77–143. MR2186976 ↑12.1

[NW96]   Alexander Nabutovsky and Shmuel Weinberger, *Algorithmic unsolvability of the triviality problem for multidimensional knots*, Comment. Math. Helv. **71** (1996), no. 3, 426–434, DOI 10.1007/BF02566428. MR1418946 (98i:57045) ↑7.3

[Nov54]   P. S. Novikov, *Unsolvability of the conjugacy problem in the theory of groups*, Izv. Akad. Nauk SSSR. Ser. Mat. **18** (1954), 485–524 (Russian). MR0075196 (17,706a) ↑6.3

[Nov55]   _____, *Ob algoritmičeskoĭ nerazrešimosti problemy toždestva slov v teorii grupp*, Trudy Mat. Inst. im. Steklov. no. 44, Izdat. Akad. Nauk SSSR, Moscow, 1955 (Russian); English transl., *On the algorithmic insolvability of the word problem in group theory*, 1958. MR0092784 (19,1158b). MR0075197 (17,706b) ↑6.2

[Par12]   Jennifer Park, *A universal first order formula defining the ring of integers in a number field*, February 28, 2012. Preprint, `arXiv:1202.6371v1`. ↑8.2.1

[Pat70]   Michael S. Paterson, *Unsolvability in 3×3 matrices*, Studies in Appl. Math. **49** (1970), 105–107. MR0255400 (41 #62) ↑5.1

[Phe88]   Thanases Pheidas, *Hilbert's tenth problem for a class of rings of algebraic integers*, Proc. Amer. Math. Soc. **104** (1988), no. 2, 611–620, DOI 10.2307/2047021. MR962837 (90b:12002) ↑8.2.2

[Poo02]   Bjorn Poonen, *Using elliptic curves of rank one towards the undecidability of Hilbert's tenth problem over rings of algebraic integers*, Algorithmic number theory (Sydney, 2002), 2002, pp. 33–42. MR2041072 (2004m:11206) ↑8.2.2

[Poo08]   _____, *Undecidability in number theory*, Notices Amer. Math. Soc. **55** (2008), no. 3, 344–350. MR2382821 ↑8.2.2

[Poo09]   _____, *Characterizing integers among rational numbers with a universal-existential formula*, Amer. J. Math. **131** (2009), no. 3, 675–682, DOI 10.1353/ajm.0.0057. MR2530851 (2010h:11203) ↑8.2.1

[Poo11]   _____, *Automorphisms mapping a point into a subvariety*, J. Algebraic Geom. **20** (2011), no. 4, 785–794, DOI 10.1090/S1056-3911-2011-00543-2. With an appendix by Matthias Aschenbrenner. MR2819676 ↑12.2

[Pos44]   Emil L. Post, *Recursively enumerable sets of positive integers and their decision problems*, Bull. Amer. Math. Soc. **50** (1944), 284–316. MR0010514 (6,29f) ↑2.4, 14.1

[Pos46]   _____, *A variant of a recursively unsolvable problem*, Bull. Amer. Math. Soc. **52** (1946), 264–268. MR0015343 (7,405b) ↑4.1

[Pos47]   _____, *Recursive unsolvability of a problem of Thue*, J. Symbolic Logic **12** (1947), 1–11. MR0020527 (8,558b) ↑6.2

[PER79]   Marian Boykan Pour-El and Ian Richards, *A computable ordinary differential equation which possesses no computable solution*, Ann. Math. Logic **17** (1979), no. 1-2, 61–90, DOI 10.1016/0003-4843(79)90021-4. MR552416 (81k:03064) ↑9.4

[PER83]   _____, *Noncomputability in analysis and physics: a complete determination of the class of noncomputable linear operators*, Adv. in Math. **48** (1983), no. 1, 44–74, DOI 10.1016/0001-8708(83)90004-X. MR697614 (84j:03114) ↑9.4

[Pre29]   Mojżesz Presburger, *Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt*, Comptes Rendus du I congrès de Mathématiciens des Pays Slaves, Warsaw, 1929 (German); English transl., *On the completeness of a certain system of arithmetic of whole numbers in which addition occurs as the only operation*, 1991, pp. 225–233, DOI 10.1080/014453409108837187. Translated from the German and with commentaries by Dale Jacquette. MR1111343 (92i:03003). ↑14.2

[Rab57]   Michael O. Rabin, *Effective computability of winning strategies*, Contributions to the theory of games, vol. 3, Annals of Mathematics Studies, no. 39, Princeton University Press, Princeton, N. J., 1957, pp. 147–157. MR0093740 (20 #263) ↑14.1

[Rab58]   _____, *Recursive unsolvability of group theoretic problems*, Ann. of Math. (2) **67** (1958), 172–194. MR0110743 (22 #1611) ↑6.4

[Rho05] Glenn C. Rhoads, *Planar tilings by polyominoes, polyhexes, and polyiamonds*, J. Comput. Appl. Math. **174** (2005), no. 2, 329–353, DOI 10.1016/j.cam.2004.05.002. MR2106443 (2005h:05042) ↑4.2

[Ric68] Daniel Richardson, *Some undecidable problems involving elementary functions of a real variable*, J. Symbolic Logic **33** (1968), 514–520. MR0239976 (39 #1330) ↑9.2, 9.1.3, 9.4, 9.2, 9.5

[Ris70] Robert H. Risch, *The solution of the problem of integration in finite terms*, Bull. Amer. Math. Soc. **76** (1970), 605–608. MR0269635 (42 #4530) ↑9.3

[Rob49] Julia Robinson, *Definability and decision problems in arithmetic*, J. Symbolic Logic **14** (1949), 98–114. MR0031446 (11,151f) ↑8.2.1

[Rob71] Raphael M. Robinson, *Undecidability and nonperiodicity for tilings of the plane*, Invent. Math. **12** (1971), 177–209. MR0297572 (45 #6626) ↑4.2

[Rob78] _____, *Undecidable tiling problems in the hyperbolic plane*, Invent. Math. **44** (1978), no. 3, 259–264, DOI 10.1007/BF01403163. MR484409 (81h:03091) ↑4.1

[Ros72] Maxwell Rosenlicht, *Integration in finite terms*, Amer. Math. Monthly **79** (1972), 963–972. MR0321914 (48 #279) ↑9.3

[Ros36] Barkley Rosser, *Extensions of some theorems of Gödel and Church*, J. Symbolic Logic **1** (1936), 87–91, DOI 10.2307/2269028. ↑3.2

[Rub81] Lee A. Rubel, *A universal differential equation*, Bull. Amer. Math. Soc. (N.S.) **4** (1981), no. 3, 345–349, DOI 10.1090/S0273-0979-1981-14910-7. MR609048 (82e:34015) ↑9.8

[Rub83] _____, *Some research problems about algebraic differential equations*, Trans. Amer. Math. Soc. **280** (1983), no. 1, 43–52, DOI 10.2307/1999601. MR712248 (84j:34005) ↑9.4

[Rub92] _____, *Some research problems about algebraic differential equations. II*, Illinois J. Math. **36** (1992), no. 4, 659–680. MR1215800 (94c:34003) ↑9.4

[Sei08] Paul Seidel, *A biased view of symplectic cohomology*, Current developments in mathematics, 2006, Int. Press, Somerville, MA, 2008, pp. 211–253. MR2459307 (2010k:53153) ↑7.2

[Shl89] Alexandra Shlapentokh, *Extension of Hilbert's tenth problem to some algebraic number fields*, Comm. Pure Appl. Math. **42** (1989), no. 7, 939–962, DOI 10.1002/cpa.3160420703. MR1008797 (91g:11155) ↑8.2.2

[Shl07] _____, *Hilbert's tenth problem. Diophantine classes and extensions to global fields*, New Mathematical Monographs, vol. 7, Cambridge University Press, Cambridge, 2007. MR2297245 ↑8.2.2

[Shl08] _____, *Elliptic curves retaining their rank in finite extensions and Hilbert's tenth problem for rings of algebraic numbers*, Trans. Amer. Math. Soc. **360** (2008), no. 7, 3541–3555, DOI 10.1090/S0002-9947-08-04302-X. MR2386235 (2010e:11116) ↑8.2.2

[SS95] Hava T. Siegelmann and Eduardo D. Sontag, *On the computational power of neural nets*, J. Comput. System Sci. **50** (1995), no. 1, 132–150, DOI 10.1006/jcss.1995.1013. MR1322637 (97b:68054) ↑10.1

[Sko34] Th. Skolem, *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen*, 8. Skand. Mat.-Kongr., Stockholm, 1934, pp. 163–188 (German). ↑5.4

[Sma61] Stephen Smale, *Generalized Poincaré's conjecture in dimensions greater than four*, Ann. of Math. (2) **74** (1961), 391–406. MR0137124 (25 #580) ↑7.1

[Soa96] Robert I. Soare, *Computability and recursion*, Bull. Symbolic Logic **2** (1996), no. 3, 284–321, DOI 10.2307/420992. MR1416870 (97j:03077) ↑1

[Soa04] _____, *Computability theory and differential geometry*, Bull. Symbolic Logic **10** (2004), no. 4, 457–486, DOI 10.2178/bsl/1102083758. MR2136634 (2005m:03084) ↑7.3

[SR97] Daniel T. Stallworth and Fred W. Roush, *An undecidable property of definite integrals*, Proc. Amer. Math. Soc. **125** (1997), no. 7, 2147–2148, DOI 10.1090/S0002-9939-97-03822-7. MR1377008 (97i:03006) ↑9.2

[Sta10] Richard Stanley, *Decidability of chess on an infinite board*, MathOverflow, July 20, 2010. `http://mathoverflow.net/questions/27967`. ↑14.2

[Tar51] Alfred Tarski, *A decision method for elementary algebra and geometry*, University of California Press, Berkeley and Los Angeles, Calif., 1951. 2nd ed. MR0044472 (13,423a) ↑9.1.1

[Tur36] A. M. Turing, *On computable numbers, with an application to the Entscheidungsproblem*, Proc. London Math. Soc. (2) **42** (1936), 230–265. Erratum in: *Proc. London Math. Soc. (2)*, **43** (1937), 544–546. ↑2, 3.1, 3.3

[VKF74] I. A. Volodin, V. E. Kuznecov, and A. T. Fomenko, *The problem of the algorithmic discrimination of the standard three-dimensional sphere*, Uspehi Mat. Nauk **29** (1974), no. 5(179), 71–168 (Russian). Appendix by S. P. Novikov. MR0405426 (53 #9219) ↑7.1

[Vse] Maxim Vserminov (ed.), *Hilbert's tenth problem page*. Website created under the supervision of Yuri Matiyasevich, `http://logic.pdmi.ras.ru/Hilbert10` . ↑8.2.2

[Wan61] Hao Wang, *Proving theorems by pattern recognition—II*, Bell System Tech. J. **40** (January 1961), no. 1, 1–41. ↑4.2

[Wan74] Paul S. Wang, *The undecidability of the existence of zeros of real elementary functions*, J. Assoc. Comput. Mach. **21** (1974), 586–589. MR0363862 (51 #117) ↑9.6

[Wei05] Shmuel Weinberger, *Computers, rigidity, and moduli*, M. B. Porter Lectures, Princeton University Press, Princeton, NJ, 2005. The large-scale fractal geometry of Riemannian moduli space. MR2109177 (2006f:53059) ↑7.1

[Zer13] Ernst Zermelo, *Über eine Anwendung der Mengenlehre auf die Theorie des Schachspiels*, Proc. Fifth Congress Mathematicians (Cambridge 1912), 1913, pp. 501–504 (German); English transl., Ulrich Schwalbe and Paul Walker, *Zermelo and the early history of game theory*, 2001, pp. 123–137, DOI 10.1006/game.2000.0794. MR1895174 (2003a:01019). ↑14.1

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA

E-mail address: `poonen@math.mit.edu`

URL: `http://math.mit.edu/~poonen/`