1 Undecidable Problems

As we have seen throughout this book, many problems and are **NP**-hard, or **PSPACE**-hard, **EXPTIME**-hard or **EXPSPACE**-hard. (Many of them are also complete in those classes.)

1. Are there any problems that are undecidable? Yes. The Halting problem (defined below) is undecidable. Rice [23] showed that any non trivial problem about Turing machines is undecidable. For example

$$\{M : \text{Turing Machine } M \text{ halts on all the primes}\}.$$

2. Are there any problems that do not refer to Turing machines that are undecidable? In this section we will give some examples of such.

1.1 Basic Undecidable Problems

To show that a set A is undecidable we need to already have some basic undecidable problem X and then show $A \le X$ (the reduction need not be polynomial time, just computable). We present some of these basic undecidable problems.

Problem 1.1. HALT
INSTANCE: A Turing Machine M.
QUESTION: Does M halt on 0?
NOTE: There are many equivalent formulations of HALT *that are all efficiently reducible to each other.*
NOTE: This is the problem that one first proves is undecidable from first principles. Almost all proves that a problem is undecidable use either HALT *or some other problem known to be undecidable. This is similar to how we view* ***SAT*** *except that we actually* know *that* HALT *is undecidable, whereas we need to assume* ***SAT*** *is not in* **P**.

Problem 1.2. POST CORRESPONDENCE PROBLEM *(*POSTCORRPROB*)*
INSTANCE: An finite alphabet Σ and two vectors of words over Σ, $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n)$.
QUESTION: Does there exists $1 \le i_1, \ldots, i_k \le N$ such that $\alpha_{i_1} \cdots \alpha_{i_k} = \beta_{i_1} \cdots \beta_P i_k$?
NOTE: k might be much larger than n so the naive algorithm of trying all possibilities to see if one works will go on forever if the answer is no.

A *counter machine* is another model of computation. We will not define if formally.

Problem 1.3. COUNTER MACHINES *(*COUNTERMACH*)*
INSTANCE: A Counter Machine M.
QUESTION: Does M halt on 0?

Theorem 1.

1. *(Post [22])* HALT $\le$ POSTCORRPROB *with an efficient reduction.*
2. *If* POSTCORRPROB $\le A$ *with an efficient reduction then* HALT $\le A$ *with an efficient reduction. This will be important when we claim that a reduction of* POSTCORRPROB *to a game problem will produce reasonably small, playable, initial settings for the game.*

3. *(Minsky [20], but probably also folklore))* HALT $\leq$ COUNTERMACH*; however the reduction takes a Turing machine of length n and returns a Counter machine of length* $2^{O(n)}$*. This will be important when we claim that a reduction of* COUNTERMACH *to a game problem do not produce reasonably small, playable, initial settings for the game.*

1.2 Conway's Game of Life

1.3 The Video Game Recurse

Recurse is a 2D puzzle platform game involving chests, pink flames, green glows, crystals, ledges, jars, rings, and other objects. You start in a room. If you open a chest in that room you do not get an any object or treasure. Instead you are *in another room!* Jars also lead to rooms, but in a different way. Suffice to say, the game is complicated. We hasten to point out that *this is a fun game that people actually play.*

Recurse is a 1-player game where the goal is for the player to get the crystal. RECURSE is the decision problem where you are given an initial set up for the game Recurse and need to determine if the player can win.

Demaine et al. [10] showed the following.

Theorem 2. RECURSE *is undecidable.*

Some notes about the result and the proof:

1. Theorem 2 was proven by showing POSTCORRPROB $\leq$ RECURSE and using Theorem 1. Since the basic problem used is POSTCORRPROB, and the reduction is efficient, the instances of RECURSE that are produced are fairly small.

2. Most complexity-of-games results such as those about CHESS and GO rely on (1) the *board* getting bigger and bigger, and (2) such large constants that, even for short inputs, the resulting games are not playable. The result for recurse is novel in that (1) the board stays the same size at 15×20, and (2) the games for short inputs are playable. A caveat: the number of recursions from the chests gets bigger and bigger.

1.4 Other Undecidable Games

1. The video game Braid is playable and fun. We refer the reader to Wikipedia entry on the game, for details of the rules. We denote the problem of determining if the player can win Braid by BRAID. Hamilton [14] showed that BRAID is undecidable. Hamilton's proof uses COUNTERMACH. As a result, the instance of Braid that are produced are rather large. BRAID and RECURSE are the only two video game problems that we know of that are undecidable.

2. The game Magic is well known. We refer the reader to Wikipedia entry on the game, for details of the rules (or ask someone at random since many people play it). Note that Magic is 2-player, as opposed to Recurse of Braid which are 1-player. We denote the problem of determining if the player can win Magic by MAGIC. Churchill et al. [6] showed that MAGIC is undecidable by using counter-machines. As a result, the instance of MAGIC that are produced are rather large. Later Churchill et al. [7] presented a reduction using Turing machines that was efficient; however, the instances of Magic had every players moves forced, so it was not a

natural instance of the game. Biderman [3] showed that the problem of mate-in-n for Magic is not arithmetic, which means its beyond the arithmetic hierarchy. The reduction produces natural game positions. MAGIC is the only 2-player game that we know of that is undecidable.

1.5 Diophantine Equations

In 1900 David Hilbert proposed 23 problems for mathematicians to work on. We state Hilbert's tenth problem in todays terminology.

Is the following problem decidable?

Problem 1.4. HTEN

INSTANCE: A polynomial $p \in \mathsf{Z}[x_1, \ldots, x_n]$.

QUESTION: Does there exist $a_1, \ldots, a_n \in \mathsf{Z}$ *such that* $p(a_1, \ldots, a_n) = 0$*?*

NOTE: We denote the problem where the degree $\le d$ *and the number of variables is* $\le n$ *by* HILBERT10(d, n).

NOTE: The question of decidability is equivalent to the case where $a_1, \ldots, a_n \in \mathsf{N}$*. If you compare the results we state to those in the literature they might not be the same since the literature often states results for the* N *version.*

Hilbert had hoped this problem would lead to number theory of interest. It did lead to some, but the combined efforts of Davis-Putnam-Robinson [9] and Matijasevic [17] (see also a survey article by Davis [8] and a book by Matijasevic[18]) showed that the problem was undecidable.

Gasarch [11] has a survey about what happens for particular degrees d and number of variables n. Chow (as quoted in [11] speculates that looking at degree and number of variables may be the wrong question:

> One reason there isn't already a website of the type you envision [one that has a grid of what happens for degree d, number-of-vars n] is that from a number-theoretic (or decidability) point of view, parameterization by degree and number of variables is not as natural as it might seem at first glance. The most fruitful lines of research have been geometric, and so geometric concepts such as smoothness, dimension, and genus are more natural than, say, degree. A nice survey by a number theorist is the book *Rational Points on Varieties* by Bjorn Poonen [21]. Much of it is highly technical; however, reading the preface is very enlightening. Roughly speaking, the current state of the art is that there is really only one known way to prove that a system of Diophantine equations has no rational solution.

In the list below, d is the degree and n is the number of variables.

1. Grechuk [12] stratifies diophantine equations and looks at for which levels we know they are solvable.
2. The status of the following problem with regard to decidability is not known: Given a polynomial $p \in \mathsf{Q}[x_1, \ldots, x_n]$ does there exist $a_1, \ldots, a_n \in \mathsf{Q}$ such that $p(a_1, \ldots, a_n) = 0$ Matijasevic [16] gives reasons why this may be the question Hilbert meant to ask.
3. Here are the current undecidability results with the smallest d and the smallest n. (a) (Jones [15]) HILBERT10(8,174) is undecidable, (b) (Sun [25]) There is a d such that HILBERT10$(d, 11)$ is undecidable.

4. Here are the current decidability results with the largest d and n. (Siegel [24], see also Grunewald & Segal [13]) For any n, HILBERT10$(2, n)$ is decidable.

5. The case of HILBERT10(3,2) is open; however, there are reasons to think it is decidable. See Section 4.3 of Gasarch [11].

6. Matijasevic & Robinson [19] conjecture that there is a d such that HILBERT10$(d, 3)$ is undecidable. Baker [1] stated that the number theoretic tools available at the time could not do much with degree 3. Since his paper was in 1968, the undecidability result was not yet known; however, had it been known, he might have conjectured that there is an n such that HILBERT10$(3, n)$ is undecidable.

7. The status of the following problem with regard to decidability is not known: Given k, does $x^3 + y^3 + z^3 = k$ have a solution in Z?

1.6 Mortal Matrices

We present another undecidable problem that does not refer to Turing machines.

Problem 1.5. MORTALMATRICES

INSTANCE: A set of m $n \times n$ matrices $M_1, \ldots, M_m$ over Z,

QUESTION: Does there exists $i_1, \ldots, i_N$ such that $M_{i_1} \times \cdots \times M_{i_N}$ is the all zero matrix. Note that we are allowed to use M_i many times.

Theorem 3.

(Cassaigne et al. [5]) MORTALMATRICES *is undecidable for: (1) 6* 3×3 *matrices, (2) 4* 5×5 *matrices, (3) 3* 9×9 *matrices, (4) 2* 15×15 *matrices.*

(Bournez & Branicky [4]) MORTALMATRICES *is decidable for 2* 2×2 *matrices.*

(Bell et al. [2]) MORTALMATRICES *for* 2×2 *matrics is* **NP***-hard.*

Note that the question of decidability for 2 3×3 matrices is open.

References

[1] A. Baker. On the representation of integers by binary forms. *Philosophical Transactions of the Royal Society of London*, 263:173–191, 1968.

[2] P. C. Bell, M. Hirvensalo, and I. Potapov. Mortality for 2 × 2 matrices is NP-hard. In B. Rovan, V. Sassone, and P. Widmayer, editors, *Mathematical Foundations of Computer Science 2012 - 37th International Symposium, MFCS 2012, Bratislava, Slovakia, August 27-31, 2012. Proceedings*, volume 7464 of *Lecture Notes in Computer Science*, pages 148–159. Springer, 2012.

[3] S. Biderman. Magic: the gathering is as hard as arithmetic, 2020. `https://arxiv.org/abs/2003.05119`.

[4] O. Bournez and M. S. Branicky. The mortality problem for matrices of low dimensions. *Theory Comput. Syst.*, 35(4):433–448, 2002. `https://doi.org/10.1007/s00224-002-1010-5`.

[5] J. Cassaigne, V. Halava, T. Harju, and F. Nicolas. Tighter undecidability bounds for matrix mortality, zero-in-the-corner problems, and more, 2014.
`http://arxiv.org/abs/1404.0644`.

[6] A. Churchill. Magic: The gathering is turing complete, 2012.
`http://www.toothycat.net/~hologram/Turing/`.

[7] A. Churchill, S. Biderman, and A. Herrick. Magic: The gathering is turing complete. In M. Farach-Colton, G. Prencipe, and R. Uehara, editors, *10th International Conference on Fun with Algorithms, FUN 2021, May 30 to June 1, 2021, Favignana Island, Sicily, Italy*, volume 157 of *LIPIcs*, pages 9:1–9:19. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021.
`https://doi.org/10.4230/LIPIcs.FUN.2021.9`.

[8] M. Davis. Hilbert's tenth problem is unsolvable. *American Mathematical Monthly*, pages 233–2695, 1973.
`https://www.math.umd.edu/~laskow/Pubs/713/Diophantine.pdf`.

[9] M. Davis, H. Putnam, and J. Robinson. The decision problem for exponential diophantine equations. *Annal of Mathematics*, 74:425–436, 1961.

[10] E. D. Demaine, J. Kopinsky, and J. Lynch. Recursed is not recursive: A jarring result. In Y. Cao, S. Cheng, and M. Li, editors, *31st International Symposium on Algorithms and Computation, ISAAC 2020, December 14-18, 2020, Hong Kong, China (Virtual Conference)*, volume 181 of *LIPIcs*, pages 50:1–50:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020.
`https://doi.org/10.4230/LIPIcs.ISAAC.2020.50`.

[11] W. Gasarch. Why is there no (d, n) grid for Hilbert's 10th problem?, 2020. May 5, 2020 Blog Entry on Complexity Blog.

[12] B. Grechuk. Diophantine equations: a systematic approach, 2021.
`https://arxiv.org/abs/2108.08705`.

[13] F. J. Grunewald and D. Segal. How to solve a quadratic equations in integers. *Mathematical Proceedings of the Cambridge Philosophical Society*, 89:1–5, 1981.

[14] L. Hamilton. Braid is undecidable, 2014.
`https://arxiv.org/pdf/1412.0784.pdf`.

[15] J. Jones. Universal diophantine equations. *Journal of Symbolic Logic*, 47(3):549–571, 1982.
`http://www.jstor.org/stable/2273588?seq=1#metadata_info_tab_contents`.

[16] Y. Matijasevic. Hilbert's tenth problem: What can we do with diophantine equations?
`https://logic.pdmi.ras.ru/~yumat/personaljournal/H10history/H10histe.pdf`.

[17] Y. Matijasevič. Enumerable sets are diophantine (Russian). *Doklady Academy Nauk, SSSR*, 191:279–282, 1970. Translation in Soviet Math Doklady, Vol 11, 1970.

[18] Y. Matijasevič. *Hilbert's Tenth Problem*. MIT Press, Cambridge, 1993.

[19] Y. Matijasevič and J. Robinson. Reduction of an arbitrary diophantine equation to one in 13 unknowns. *Acta Arithmetica*, pages 521–553, 1975.

[20] M. Minsky. *Computation: Finite and Infinite Machines*, pages 255–258. Prentice-Hall, Inc., Englewood Cliffs, NJ, 1st edition, 1967.

[21] B. Poonen. *Rational points on varieties*, volume 186 of *Graduate studies in mathematics*. American Mathematical Society, 2017.

[22] E. Post. A variant of a recursively unsolvable problem. *Bulletin of the American Mathematical Society*, 52(4):264–268, 1946.

[23] H. G. Rice. Classes of recursively enumerable sets and their decision problems. *Transactions of the the American Mathematics Society*, 74:358–366, 1953.

[24] C. L. Siegel. Zur theorie der quadratischen formen. *Nachrichten der Akademie der Wissenschaften in Göttingen, Mathematisch-Physikalische Klasse*, 3:21–46, 1972.

[25] Z.-W. Sun. Further results on Hilbert's tenth problem. *Science China Mathematics*, This Journal Does not have Volumes:1–26, 2020.