CSCI3390-Lecture 8: A Sampler of Undecidable Problems

September 27, 2018

1 Summary

- All of the undecidable problems we've seen up to this point are problems about the long-term behavior of Turing machines (that is, of computer programs).
- Here we give a list of computational problems from many different domains that are also undecidable. In a later lecture will focus on a couple of these and give the undecidability proof.

2 The string rewriting problem, revisited

This problem was discussed in Lecture 4.

> *Input:* A finite set $\{(u_1, v_1), \ldots, (u_r, v_r)\}$ of pairs of words over a finite alphabet Σ, and two additional words $w_1, w_2 \in \Sigma^*$
>
> *Output:* Yes if w_2 can be derived from w_1 by a sequence of applications of the substitution rules $u_i \mapsto v_i$. No otherwise.

We have already argued that the set of 'Yes' instances of this problem is Turing-recognizable, and that if the substitution rules are restricted so that we always have $|u_i| \leq |v_i|$, then the problem is decidable. We will prove in the next lecutre that in general the problem is undecidable.

Figure 1: A set of tiles.

3 Undecidable Problems about Combinatorial Designs

3.1 Tiling

You are given a finite set of square tiles, such as the ones pictured in Figure 1. Assume that you have an unlimited supply of each kind of tile. Tiles are placed on the floor in such a manner that two adjacent tiles have the same color on both sides of the shared edge. We also make a rule that the orientation of a tile is fixed—that is, the tiles cannot be turned.[1]

Figure 2 shows that the entire infinite plane can be covered using these three tile types. We ask whether there is an algorithm that will solve this problem in general.

> *Input:* A finite set T of square tiles.
>
> *Output:* Yes if the entire plane can be tiled using only tiles from this set. No otherwise.

So the set of three tiles in Figure 1 is a 'yes' instance of this problem. On the other hand, any proper subset of this set of tiles is a 'No' instance.

The tiling problem is undecidable. The proof of this is rather involved, but in the next lecture we will prove undecidability of a simpler version: Let us just consider tilings of the first quadrant of the plane—the points where both x- and y-coordinates are positive, and let us specify a 'starter' tile to tile the lower left corner. Here is the *fixed-corner tiling problem:*

[1] If you want to enforce this rule, imagine that little indentations are carved into the bottom edge of each tile, and matching teeth (*exdentations?*) in the top edge.

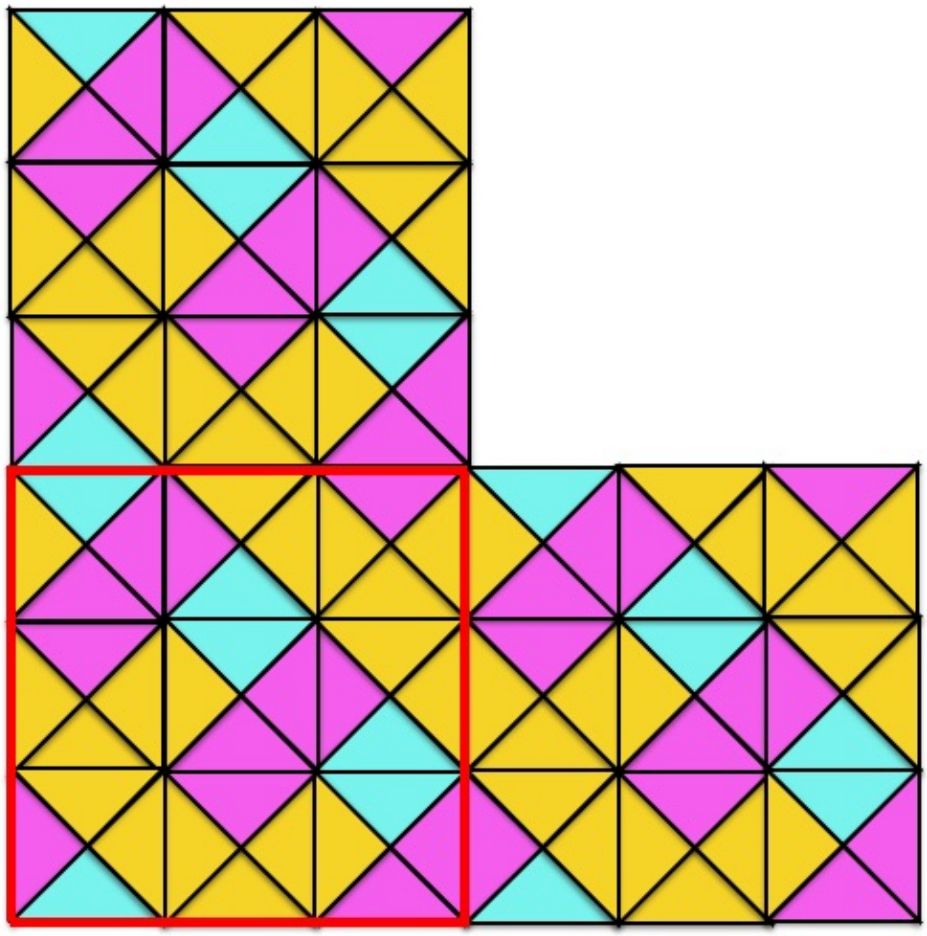

Figure 2: A tiling using the tiles from Figure 1. Observe that the 3×3 square of tiles at the lower left is reproduced exactly both directly above and directly to its right. This shows us that the tiling can be extended to cover the entire plane.

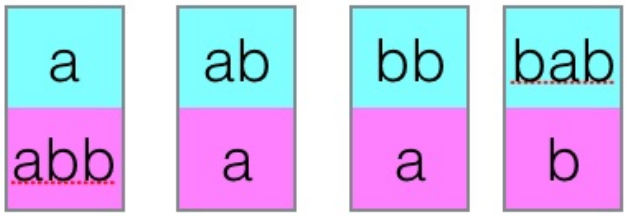

Figure 3: A set of dominos. This forms a 'Yes' instance for the Post Correspondence Problem, because of the match shown in the next figure.

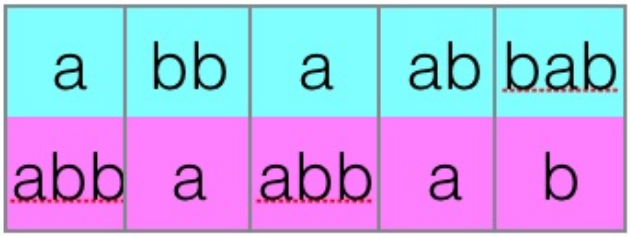

Figure 4: A match for the Post Correspondence Problem using the tiles from Figure 3. Both the top and bottom rows spell out the same word $abbaabbab$

> *Input:* A finite set T of square tiles, and a tile $t \in T$.
>
> *Output:* Yes if the entire first quadrant can be tiled using only tiles from this set with t as the tile in the lower left corner. No otherwise.

3.2 Post Correspondence Problem.

Here the input consists of a finite collection of dominos, each with a word over some finite alphabet written in each half. Once again, the orientation of the dominos cannot change, so each has a top half and a bottom half. If we line up a row of such dominos we obtain words u, v in both the top and bottom halves by concatenating the words in the individual dominos. This arrangement is called a *match* if $u = v$. Figure 4 shows a set of dominos, and Figure 5 a match.

The *Post Correspondence Problem* is:

> *Input:* A finite set of dominos.

Output: Yes if it is possible to produce a match with this set of dominos, no otherwise.

4 Undecidable Problems from Logic

Mathematical statements, for example statements about the arithmetic of the natural numbers, are formulated as sentences of *first-order predicate logic*. These are built using the operations *and, or, not,* which we abbreviate by $\wedge, \vee, \neg$, respectively, quantifiers, the constants 0 and 1, and the operations of addition and multiplication. For instance, the following sentence says that there is a largest natural number (it's false!) while the next one says that for every natural number, there is a larger one (which is true).

$$\exists x \forall y (y \leq x),$$
$$\forall y \exists x (y < x).$$

The following formula, which has a *free variable* z, says that z is prime (it is bigger than 1, and there is no factorization into factors bigger than 1).

$$(z > 1) \wedge \neg \exists x \exists y ((z = x \times y) \wedge (x > 1) \wedge (y > 1)).$$

We can abbreviate this as prime(z). We can then write the statement 'there are infinitely many primes' as

$$\forall x (\text{prime}(x) \rightarrow \exists y ((x < y) \wedge \text{prime}(y))).^2$$

The true sentences above are *theorems* of arithmetic, meaning that there are *proofs* of them. Discussing this next question in a strictly formal manner requires a precise definition of what a proof is, but the undecidability of the following problem holds as long as what constitutes a proof satisfies some general requirements that we *expect* proofs to satisfy.

Input: A sentence of predicate logic of arithmetic.

Output: Yes if the sentence is a theorem. No otherwise.

[2] If you are bothered by the appearance of additional symbols like $<$ and $\rightarrow$ (implies) in these formulas, don't worry. We can say 'oh, yeah, let's throw these in our language, too', but in fact they can be defined in terms of the other elements we are allowing in formulas.

This problem is undecidable, a fact that you can take as meaning, 'mathematics cannot be completely automated'. In a later lecture, we will prove the undecidability of theoremhood, along with a stunning corollary of this fact: There are statements of arithmetic that can neither be proved nor disproved. This is called *Gödel's Incompleteness Theorem.*

5 Undecidable Problems from Algebra and Analysis

5.1 Hilbert's Tenth Problem

We've already seen this one!

5.2 Equivalence of Elementary Functions of Analysis

Bad news for calculus graders. Consider the set of expressions that we can form starting from the rational numbers, the functions $f(x) = x, e^x, \cos x$ and $\sin x$, using addition, multiplication, subtraction and composition. Two such expressions might define the same function, for examples

$$2\cos^2 x - 1$$

and

$$\cos 2x.$$

It would be nice to have a general method for testing the identity of two such functions, but it can be proved that no such function exists. That is, the decision problem whose input is a pair of such expressions and whose output is Yes if and only if the two expressions define identical functions, is undecidable.