Math 29: Noncomputable Problems from Mathematics

May 2nd, 2022

1 Diophantine Equations

Recall that a **Diophantine equation** is obtained by setting a polynomial with finitely many variables and integer coefficients equal to 0. Given a polynomial in variables $x_0, \ldots, x_k$ defined using unknowns $y_0, \ldots, y_n$ (variables to which we assign a value), let $P(x_0, \ldots, x_k, y_0, \ldots, y_n) = 0$ denote the corresponding Diophantine equation. For example, $x^2 + 2x + 1 = 0$ can be written as $Q(x, 1, 2, 1) = 0$, where $Q(a, b, c, d) = ba^2 + ca + d$.

A set X is **Diophantine** if it is of the form

$$\{\langle x_0, \ldots, x_k\rangle : \exists \langle y_0, \ldots, y_n\rangle \; P(x_0, \ldots, x_k, y_0, \ldots, y_n) = 0\}$$

for some Diophantine equation $P(x_0, \ldots, x_k, y_0, \ldots, y_n) = 0$. In other words, a set is Diophantine if it can be represented as the set of all tuples $\langle x_0, \ldots, x_k\rangle$ for which there is some collection of coefficients such that $\langle x_0, \ldots, x_k\rangle$ is a solution to the corresponding equation.

For example, the set of all natural numbers is Diophantine:

$$\omega = \{x : \exists \langle a, b, c\rangle \; ax^2 - bx + c = 0\}$$

For any natural number n, we can choose natural a, b, and c such that n is a root of the resulting polynomial: namely, $x^2 - nx = 0$. In general, of course, there could be infinitely many ways to give a Diophantine description of a set. Below is an amazing fact.

Theorem 1. *(Jones, Sato, Wada, Wiens) The set of prime numbers is Diophantine.*

Proof. Polynomial and Proof □

This polynomial is neither elegant nor "nice," but it seems on the surface to even be surprising that it exists. However, the authors knew that such a polynomial existed, and simply had to find it. (No small feat, of course!)

The following theorem guaranteed that it existed, which is somehow even more surprising.

Theorem 2. *(Matiyasevich, Robinson, Davis, Putnam) A set is Diophantine if and only if it is c.e.*

This is not only incredibly surprising, since functions like the Ackermann function grow at an astounding rate and are yet computable, but it answers Hilbert's Tenth Problem: Hilbert asked for an algorithm or process by which we could determine whether or not a given Diophantine equation had (integer) solutions. But as we will see, determining if a given c.e. set is nonempty cannot be done computably. (In fact, being able to do so would allow us to compute K.) Therefore, we cannot have such an algorithm. (Or if there is one, it is not Turing computable.)

2 Word Problem for Groups

Lemma 3. *Let A be c.e. but not computable. Then*

$$\{\langle a, b, c, d\rangle : a^n b a^n = c^n d c^n \text{ for } n \in A\}$$

is a finitely generated group with c.e. presentation whose word problem isn't computable.

Proof: It is finitely generated by definition, and its presentation is c.e. because A is.

Suppose there is a total computable function $f(\sigma, \tau)$ which decided the word problem, i.e. $f(\sigma, \tau) = 1$ if σ and τ are group words with $\sigma = \tau$, and $f(\sigma, \tau) = 0$ otherwise. (Suppressed here is some discussion on coding, which is in-line with the coding methods we use elsewhere.) Then to determine membership of $n \in A$, calculate $f(a^n b a^n, c^n d c^n)$. Clearly if $n \in A$, then these words will be equal.

Now suppose that $a^n b a^n = c^n d c^n$. We just need to prove that it is not the case that $n \notin A$, that is there is no combination of other rules which can give us the n-rule for free. But notice that nothing we can multiply by simplifies an equality of this form: if we multiply by the same thing on both sides, then at least one of them will add with the outer term, not cancel it. If we multiply by something for which there is a rule, it will cancel things out if and only if the power is the same.

A group is **finitely presented** if it has finitely many generators and finitely many reducibility rules. Even this is not solvable in general: Collins gave an example using 10 generators and 27 relationships, viewable here. Even if we restrict ourselves to those finitely presented groups which do have a solvable word problem, they are still not uniformly computable, as proven by Boone and Rogers.

3 Weak König's Lemma

Lemma 4. *Given any two disjoint c.e. sets A and B, the sets which separate A and B form a computable tree.*

Proof: Let $W_e = A$ and $W_k = B$. Define the tree T as follows: given σ, let $\sigma \in T$ if and only if, for all $n < |\sigma|$, $\varphi_{e,|s|}(n) \downarrow$ implies that $\sigma(n) = 1$, and $\varphi_{k,|s|}(n) \downarrow$ implies $\sigma(n) = 0$. Clearly this is computable because all of our computations are time-bounded.

Now suppose $X \in [T]$. Then for all $n \in W_e$, there is some s where $\varphi_{e,s}(n)$. Then by the definition of a path, the first s bits of X form a finite binary string τ, and it must be in T. Then it must be the case that $\tau(n) = X(n) = 1$. Similarly, if $n \in W_k$, $X(n) = 0$. Therefore, X separates A and B.

Conversely, if X separates A and B, then it is clearly a path through T by the definition of separation.

We know (or will know) from the Take-Home Midterm that there are disjoint c.e. sets A and B which cannot be computably separated. Therefore, the tree constructed above for A and B is an infinite computable tree with no computable paths.

3.1 Gödel's Incompleteness Theorems

A consequence of Gödel's Incompleteness Theorems is that, informally, there is no logical system which can describe basic arithmetic (**Peano Arithmetic** is often stated here, but it is still true for weaker fragments), be **complete** in that it assigns true or false to every sentence, be **consistent** in that it does not prove a contradiction, and have axioms which are computably enumerable under some effective coding of formulas.

This in fact gives an alternate proof that Weak König's Lemma is not computably true: one can construct a computable tree T whose included binary

strings σ code the information for finitely many statements in the formal language of arithmetic for which there is no proof of a contradiction coded by a natural number less than the length of σ. (Again, under some suitable coding of valid proofs.) Then, assuming Peano Arithmetic is consistent, this will be an infinite binary tree, and thus have a path by Weak König's Lemma. However, there will be no computable path by the above.