Math 17
Winter 2015
Monday, February 9

$X \subseteq \mathbb{N}^n$ is a Turing semidecicable set.
M is a semidecision machine for X, using symbols

$$\alpha_1 = *,\ \alpha_2 = 0,\ \alpha_3 = 1,\ \alpha_4, \dots, \alpha_w$$

and states

$$q_1 \text{ (starting state)}, q_2, \dots, q_{\overline{w}}.$$

We wish to prove that X is Diophantine by simulating the action of M.

We code a configuration of M by a pair (p,t).
The coding we use is positional coding base b, where b is prime, $b \geq w + \overline{w}$.
The number p codes a sequence that represents the head location and state of M. An i in position j means that M is in state i and the head is positioned to read cell j.
The number t codes a sequence that represents the contents of the tape. An i in position j means that symbol α_i is written in cell j. A 0 in position j can mean either that cell j contains λ or that cell j is empty.

The starting configuration for running M with input $(a_1, \dots, a_n)$ (in which the sequence $(a_1, \dots, a_n)$ is coded on the tape, the head is reading the leftmost cell, and the machine is in state q_1) is coded by the pair

$$(p,t) = (InitP(a_1, \dots, a_n),\ InitT(a_1, \dots, a_n)).$$

We showed that $InitP$ and $InitT$ are Diophantine functions.

If (p,t) codes a configuration, the configuration obtained by running M for one step is coded by the pair

$$(NextP(p,t),\ NextT(p,t))$$

(provided (p,t) does not code a configuration in a final state), and the configuration obtained by running M for k steps is coded by the pair

$$(AfterP(k,p,t),\ AfterT(k,p,t))$$

(provided a final state is not reached in fewer than k steps).
If the configuration (p,t) represents a machine in a final state, then $NextP(p,t) = 0$ and $NextT(p,t) = t$.
If, beginning with the configuration coded by (p,t), a final state is reached in fewer than k steps, then $AfterP(k,p,t) = 0$, and $AfterT(k,p,t)$ codes the contents of the tape at the time the final state is reached.

If we can show that $AfterP$ is a Diophantine function, then we will have shown that X is Diophantine. That is because we will now have $(a_1, \ldots, a_n) \in X$ iff M with input $(a_1, \ldots, a_n)$ eventually halts, and M with input $(a_1, \ldots, a_n)$ eventually halts iff

$$(\exists k)\,[AfterP(k, InitP(a_1, \ldots, a_n), InitT(a_1, \ldots, a_n)) = 0]\,.$$

We talked about showing $NextP$ and $NextT$ are Diophantine, in the following way:

Suppose M has instructions I_1, I_2, ..., I_θ.

For each instruction I, there is a Diophantine property $MoveI(p, t, p', t')$, which means that instruction I applies to the configuration coded by (p, t), and when the machine acts according to that instruction, the resulting configuration is coded by (p', t').

Now we have

$$p' = NextP(p,t) \iff (\exists t')\big[MoveI_1(p,t,p',t',) \vee MoveI_2(p,t,p',t',) \vee \cdots \vee MoveI_\theta(p,t,p',t',)\big]$$

$$t' = NextT(p,t) \iff (\exists p')\big[MoveI_1(p,t,p',t',) \vee MoveI_2(p,t,p',t',) \vee \cdots \vee MoveI_\theta(p,t,p',t',)\big]$$

Now we will show that $AfterP$ and $AfterT$ are Diophantine. We will not use the fact that $NextP$ and $NextT$ are Diophantine in this proof, so since $NextP(p,t) = AfterP(1,p,t)$ and $NextT(p,t) = AfterT(1,p,t)$, this will constitute another proof that $NextP$ and $NextT$ are Diophantine.