Math 17
Winter 2015
Written Exercises due Friday, February 20

(1.) Describe a Turing machine that does the following:

With input coding $(a, N, b_1, c_1, b_2, c_2)$, where (N, b_1, c_1) is a code for a Diophantine set $X_1 \subseteq \mathbb{N}$ and (N, b_2, c_2) is a code for another Diophantine set $X_2 \subseteq \mathbb{N}$:

If $a \in X_1$ but $a \notin X_2$, the machine will halt in state q_2.

If $a \in X_2$ but $a \notin X_1$, the machine will halt in state q_3.

If $a \in X_1$ and $a \in X_2$, the machine will halt, possibly in state q_2 and possibly in state q_3.

If $a \notin X_1$ and $a \notin X_2$, the machine will never halt.

You may make use of the machines that we described in class, in particular:

DECODEX$^{(2)}$, when the beginning of the tape codes a sequence of at least two numbers $(a, N, \dots)$ and the end of the tape codes another number x that is the Cantor code for a sequence $(x_1, x_2, \dots, x_N)$, replaces the code for x with

$$\alpha_1\beta_1\alpha_2\beta_2 \cdots \alpha_{N-1}\beta_{N-1}\beta_N$$

where α_i is a block X's and β_i consists of a 0 followed by x_i-many 1's.

That is, DECODEX$^{(2)}$ replaces the code for x with the codes for x_1, x_2, …, x_N, interspersed with some X's.

EVAL does the following. Suppose the tape ends with the sequence $7\alpha7\beta\gamma$, where γ is any sequence not containing any 7's, α codes the sequence coding a polynomial P, interspersed with some X's, and β codes the sequence coding inputs $a, x_1, x_2, \dots, x_N$ to P, also interspersed with some X's. Then EVAL adds to the end of the tape a sequence of 0's and 1's containing $P(a, x_1, \dots, x_N)$-many 1's. It leaves most of the original sequence α replaced by a block of X's.

You may also use simple submachines like "go left to the third 7" (where "7" means the symbol 7, not the sequence 01111111).

Finally, you may describe your Turing machine using a sequence of steps, as in the class handout from today.

(2.) Show that if $X \subseteq \mathbb{N}$, and both X and its complement $Y = \{a \in \mathbb{N} \mid a \notin X\}$ are Diophantine, then X is Turing decidable.

Note that you can use the preceding problem to produce a decision machine, but the input to that machine must be just one number, a.

(3.) Show the converse, that if $X \subseteq \mathbb{N}$ is Turing decidable, then both X and its complement are Diophantine.

You may want to use the fact that all Turing semidecidable sets are Diophantine.

(4.) We designed a Turing machine UD with the following property.

Every Diophantine set $X \subseteq \mathbb{N}$ has a code (N, b, c) such that

$$(\forall a)\,[a \in X \iff \text{UD with input } (a, N, b, c) \text{ halts}].$$

If we set

$$U = \{(a, N, b, c) \mid M \text{ with input } (a, N, b, c) \text{ halts},$$

then U is a *universal* Diophantine set. This means

Every Diophantine set $X \subseteq \mathbb{N}$ has a code (N, b, c) such that

$$(\forall a)\,[a \in X \iff (a, N, b, c) \in U].$$

Recall, if $a = \mathrm{Cantor}_3(x, y, z)$, then $\mathrm{Elem}_{3,1}(a) = x$, $\mathrm{Elem}_{3,2}(a) = y$, and $\mathrm{Elem}_{3,1}(a) = z$. The functions Cantor_3, $\mathrm{Elem}_{3,1}$, $\mathrm{Elem}_{3,2}$, and $\mathrm{Elem}_{3,3}$ are Diophantine.

Define a Diophantine set by

$$S = \{a \mid (a, \mathrm{Elem}_{3,1}(a), \mathrm{Elem}_{3,2}(a), \mathrm{Elem}_{3,3}(a)) \in U\},$$

and let

$$\overline{S} = \{a \mid a \notin S\}.$$

Show that $\overline{S}$ is not Diophantine.

Suggestion: Suppose, toward a contradiction, that $\overline{S}$ is Diophantine. Then it has a code (M, d, e). Let $\overline{a} = Cantor_3(M, d, e)$. Show that both the assumption $\overline{a} \in \overline{S}$ and the assumption $\overline{a} \notin \overline{S}$ lead to contradictions.

(5.) Conclude, from (3) and (4), that Hilbert's tenth problem is unsolvable. (That is, assuming that we interpret Hilbert's "process according to which it can be determined in a finite number of operations. . . " as something that could be carried out by a Turing machine.)