CS 125 Algorithms & Complexity — Fall 2016

Problem Set 8

Due: 11:59pm, Friday, November 4th

See homework submission instructions at `http://seas.harvard.edu/~cs125/fall16/schedule.htm`

Problem 1

Determine whether the following languages are decidable, and justify your answers. Throughout, M is a 1-tape Turing Machine.

(a) (5 points) $\{\langle M, \sigma\rangle : M$ eventually writes symbol σ to tape when run on the empty string$\}$.

(b) (5 points) $\{\langle M\rangle : M$ eventually writes a nonblank symbol to tape when run on the empty string$\}$.

(c) (5 points) $\{\langle M, m\rangle : M$ accepts only strings whose length is a multiple of $m\}$.
Hint: use Rice's theorem, which we will cover on Tuesday, Nov. 1.

(d) (5 points) $\{\langle M\rangle : L(M)$ is countable$\}$.

(e) (extra credit) $\{\langle M, k\rangle : M$ never moves left more than k times when run on the empty string$\}$

Problem 2

It is 2016 and you and your classmates have dropped out of college in order to launch the CS 125 App Store, where developers can sell *Word-RAM* programs to smartphone users. You have also managed to convince many smartphone manufacturers to develop hardware that is optimized for running Word-RAM programs. However, you now realize that you did not provide a complete spec for the semantics of the Word-RAM, and did not specify what should happen when a Word-RAM program tries to read or write to a memory location that has not yet been MALLOC'ed. On some phones, the implementation of such operations can lead to serious security vulnerabilities, e.g. allowing a malicious app to steal private data from other apps and send it out over the network. Call a Word-RAM program *safe* iff it never writes outside allocated memory (on any input).

(a) (5 points) Your CEO from HBS demands that you write software that will check programs as they are uploaded to the CS 125 App Store and reject all unsafe ones (and only the unsafe ones). Prove that your CEO's request is impossible.

(b) (5 points) Show that nevertheless, you can still accomplish something nearly as good. Describe a compiler that converts any word-RAM program P into a word-RAM program P' such that (a) P' is safe, (b) if P is safe, then P' has exactly the same functionality as P, and (c) P' is at most a constant-factor slower than P.

Problem 3

Prove that the following Bounded Halting language is decidable but not in P:

$$\text{BH} = \{\langle M, w, k\rangle : M \text{ is a TM that halts on } w \text{ within } k \text{ steps}\},$$

where k is represented in binary.
Hint: Start by showing that $L \leq_p \text{BH}$, for $L = \{\langle M\rangle \# a^t : M \text{ rejects } \langle M\rangle \# a^t \text{ within } 2^t \text{ steps}\}$. Then do a proof by contradiction, being careful about the fact that "polynomial time" is an asymptotic notion.