Project Zero Knowledge Proofs
Exercises 1

November 27, 2014

1 Designing a Turing Machine

1. Design a TM that adds two natural numbers, so it takes as input two natural numbers and it outputs their sum. Clearly indicate (and explain):

   (a) The type of TM you use (how many tapes, how many heads),

   (b) The alphabet your TM reads,

   (c) The different states of your TM,

   (d) The transition function. You can give it as a diagram or a table.

   Hint: think of a clever way to represent the numbers you want to add

2. Demonstrate how your TM works by showing each step of the computation progress on the tape(s) when adding 2 and 3.

2 Equivalence of different Turing Machine models

Consider a TM M, consisting of 3 tapes with 3 heads, recognising the alphabet Γ, and runs in time $T(n)$ on input of length n. In this exercise we will convert this to a TM M' that has only 1 tape with 1 head.

First we merge the 3 tapes into 1. We do this by reserving the locations 1 mod 3 (so 1,4,7, etc) for tape 1, the locations 2 mod 3 (so 2,5,8, etc) for tape 2 and the locations 3 mod 3 (so 3,6,9, etc) for tape 3.

1. Recover the original 3 tapes from the following tape, assuming that the first square shown is location number 0:

	n	l	b	e	o	a	v	o	c	e	k	k	r		

Next, we simulate the 3 heads by adding, for each symbol $x \in \Gamma$, a symbol $\hat{x}$ to Γ. Putting $\hat{x}$ instead of x on the tape simulates a head of M reading that cell. By scanning the entire tape and keeping track of the symbols with hats, the head of M' can read what the 3 heads of M read together.

2. Indicate in your solution of the previous part of this exercise, where the heads of M are when the tape of M' looks like this:

	$\hat{n}$	l	b	e	o	$\hat{a}$	v	o	c	e	$\hat{k}$	k	r		

The full simulation of M on M' now works as follows:

- Input: The input is given on the first n locations of M'. M' simulates this as input for M by copying the input to locations $n+3, n+6, n+9, etc$
- For each step M would make, M' sweeps the entire used tape: one sweep from beginning to end to record the symbols that are currently read by the simulated heads of M. Then, using Ms transition function, M' makes the appropriate changes while sweeping back.

3. M can reach at most $T(n)$ locations on each of its tapes, why?
4. How long, compared to $T(n)$, does M' take to halt on input of length n?

3 Subset Sum

Consider the following problem, called subset sum:
Given a set S of n numbers: $S = \{x_1, \dots, x_n\}$ and a number N, decide if there is a subset $X \subseteq S$ such that $\sum_X x_i = N$.

This is an NP problem.

1. Formulate the problem as "$x \in$ L" (What is x? What is L?)
2. What would be a witness for $x \in$ L?
3. Prove that L $\in$ NP, that is:
   (a) Come up with an algorithm that, given x and the witness, decides whether $x \in$ L (outputs 1 iff it does, 0 iff it does not)
   (b) Show that executing the algorithm takes polynomial time.

4 The classes P and NP

1. Suppose L_1 and L_2 are in P, are the following then also in P?
   (a) $L_1 \cup L_2$?
   (b) $L_1 \cap L_2$?
   (c) The complement of L_1?[1]
2. Answer the same question with P replaced by NP.

[1]the complement L_1 contains all relevant strings that are not in L_1. For instance, if L_1 consists of a subset of $\{0,1\}*$, then the complement of L_1 consists of all finite strings of zero's and ones that are not in L_1.