Problem Set 6

Due: October 26

Reading: Notes 7 on State Machines & Notes 8 on Series and Asymptotics.

Problem 1. You've seen how the RSA encryption scheme works, but why is it hard to break? In this problem, you will see that finding secret keys is as hard as finding the prime factorizations of integers. Since there is a general consensus in the crypto community (enough to persuade many large financial institutions, for example) that factoring numbers with a few hundred digits requires astronomical computing resources, we can therefore be sure it will take the same kind of overwhelming effort to find RSA secret keys of a few hundred digits. This means we can be confident the private RSA keys are not somehow revealed by the public keys [1]

For this problem, assume that $n = p \cdot q$ where p, q are both *odd* primes and that e is the public key and d the secret key of the RSA protocol as described in Week 6 Notes. Let $x ::= e \cdot d - 1$.

(a) Show that $\phi(n)$ divides x.

(b) Conclude that 4 divides x.

(c) Show that if $\gcd(r, n) = 1$, then $r^x \equiv 1 \pmod{n}$.

A *square root* of m modulo n is a nonnegative integer $s < n$ such that $s^2 \equiv m \pmod{n}$. Here is a nice fact to know: when n is a product of two odd primes, then every number m such that $\gcd(m, n) = 1$ has 4 square roots modulo n.

In particular, the number 1 has four square roots modulo n. The two trivial ones are 1 and $n - 1$ (which is $\equiv -1 \pmod{n}$). The other two are called the *nontrivial* square roots of 1.

(d) Since you know x, then for any integer, r, you can also compute the remainder, y, of $r^{x/2}$ divided by n. So $y^2 \equiv r^x \pmod{n}$. Now if r is relatively prime to n, then y will be a square root of 1 modulo n by part (c).

[1] This is a very weak kind of "security" property, because it doesn't even rule out the possibility of deciphering RSA encoded messages by some method that did not require knowing the secret key. Nevertheless, oveer twenty years experience supports the security of RSA in practice.

Show that if y turns out to be a *nontrivial* root of 1 modulo n, then you can factor n. *Hint:* From the fact that $y^2 - 1 = (y+1)(y-1)$, show that $y+1$ must be divisible by exactly one of q and p.

(e) It turns out that at least half the positive integers $r < n$ that are relatively prime to n will yield y's in part (d) that are nontrivial roots of 1. Conclude that if, in addition to n and the public key, e, you also knew the secret key d, then you can be sure of being able to factor n.

Problem 2. The Massachusetts Turnpike Authority is concerned about the integrity of the new Zakim bridge. Their consulting architect has warned that the bridge may collapse if more than 1000 cars are on it at the same time. The Authority has also been warned by their traffic consultants that the rate of accidents from cars speeding across bridges has been increasing.

Both to lighten traffic and to discourage speeding, the Authority has decided to make the bridge *one-way* and to put tolls at *both* ends of the bridge (don't laugh, this is Massachusetts). So cars will pay tolls both on entering and exiting the bridge, but the tolls will be different. In particular, a car will pay \$3 to enter onto the bridge and will pay \$2 to exit. To be sure that there are never too many cars on the bridge, the Authority will let a car onto the bridge only if the difference between the amount of money currently at the entry toll booth minus the amount at the exit toll booth is strictly less than a certain threshold amount of $\$T_0$.

The consultants have decided to model this scenario with a state machine whose states are triples of natural numbers, (A, B, C), where

- A is an amount of money at the entry booth,
- B is an amount of money at the exit booth, and
- C is a number of cars on the bridge.

Any state with $C > 1000$ is called a *collapsed* state, which the Authority dearly hopes to avoid. There will be no transition out of a collapsed state.

Since the toll booth collectors may need to start off with some amount of money in order to make change, and there may also be some number of "official" cars already on the bridge when it is opened to the public, the consultants must be ready to analyze the system started at *any* state. So let A_0 be the initial number of dollars at the entrance toll booth, B_0 the initial number of dollars at the exit toll booth, and C_0 the number of official cars on the bridge when it is opened. The Authority will be careful to ensure that C_0 is not large enough to cause a collapse. You should assume that even official cars pay tolls on exiting or entering the bridge after the bridge is opened.

(a) Give a mathematical model of the Authority's system for letting cars on and off the bridge by specifying a transition relation between states of the form (A, B, C) above.

(b) Characterize each of the following derived variables

$$A, B, A + B, A - B, 3C - A, 2A - 3B, B + 3C, 2A - 3B - 6C, 2A - 2B - 3C$$

as one of the following

constant	C
strictly increasing	SI
strictly decreasing	SD
weakly increasing but not constant	WI
weakly decreasing but not constant	WD
none of the above	N

and briefly explain your reasoning.

The Authority has asked their engineering consultants to determine T and to verify that this policy will keep the number of cars from exceeding 1000.

The consultants reason that if A_0 is the initial number of dollars at the entrance toll booth, B_0 is the initial number of dollars at the exit toll booth, and C_0 is the number of official cars on the bridge when it is opened, then an additional $1000 - C_0$ cars can be allowed on the bridge, so as long as $A - B$ has not increased by $3(1000 - C_0)$ there shouldn't more than 1000 cars on the bridge. So they recommend defining

$$T_0 ::= 3(1000 - C_0) + (A_0 - B_0).$$

(c) Use the results of part (b) to define a simple predicate, P, on states of the transition system which is satisfied by the start state, that is $P(A_0, B_0, C_0)$ holds, is not satisfied by any collapsed state, and is an *invariant* of the system. Verify that the P you define has these properties.

(d) A clever MIT intern working for the Turnpike Authority agrees that the Turnpike's bridge management policy will be *safe*: the bridge will not collapse. But she warns her boss that the policy will lead to *deadlock*— a situation where traffic can't move on the bridge even though the bridge has not collapsed.

Explain more precisely in terms of system transitions what the intern means, and briefly, but clearly, justify her claim.

Problem 3. Vertices u, v in a digraph are said to be *unconnected* when there is no path either from u to v or from v to u. The following procedure can be applied to any digraph, G:

Pick two vertices u, v such that either

1. there is an edge (u, v) of G and there is also a path from u to v which does *not* include this edge; in this case, delete the edge (u, v), or
2. u and v are unconnected; in this case, add the edge (u, v).

Repeat these operations until it is no longer possible to find vertices u, v to which an operation applies.

This procedure can be modelled as a state machine. The start state is G, and the states are all possible digraphs with the same vertices as G. The final states are the digraphs on which no operation is possible.

(a) For any state, G, let e be its number of edges, and p its number of pairs of unconnected vertices. Define a decreasing natural number valued derived variable that is a function of e and p. Conclude that the procedure terminates started on any finite digraph, G.

(b) Prove that the set of final states reachable from DAG start states are the *line graphs*.

(c) Prove that the property of being a DAG is an invariant of this procedure.

(d) Prove that if G is a DAG, the procedure terminates with a line graph whose path relation is a topological sort of the partial order defined by G. *Hint:* Strengthen the DAG invariant in the previous part.

Problem 4. **(a)** Give an example of a stable match between 3 boys and 3 girls where no person gets their first choice.

(b) Describe a simple procedure to determine whether or not a stable marriage problem has a unique solution, that is, only one possible stable marriage assignment.

Problem 5. A Harvard BS graduates and starts with an annual salary of \$140,000, with a \$25,000 raise guaranteed every year. An MIT SB graduate starts with \$100,000, with a guaranteed 15% raise every year. Assume the bankrate is a fixed 3% per year. That is, the bank will pay \$1.03 a year from now if you deposit \$1.00 today.

(a) Suppose both graduates retire after the same number of years. Use the fact that $x = o((1+\epsilon)^x)$ to explain why the MIT SB must come out ahead if they work for enough years. (You should *not* make use of closed forms for various sums in your explanation.)

(b) Suppose both graduates retire after n years. For which values of n is the MIT graduate's salary package better that the Harvard grad's?

Problem 6. Books Books and more Books! If the 6.042 staff is to stand a chance at the Book Extension Stacking Challenge, we have to consider all the angles!

Recall the basic book stacking challenge from the course notes where you have an unlimited supply of books to stack that are all the same weight.

(a) What if instead of all books weighing the same, you have a book that weighs 1 pound, a book that weighs $\frac{1}{2}$ pounds, a book that weighs $\frac{1}{4}$ pounds, where each successive book weighs half as much as the previous book. Say you had n such books, and also that the you have a duplicate of the lightest book. How far out can you stack the books? Note that all books are still the same size, just different weights. *Hint:* Where should the heaviest books be?

(b) What if you had to stack such that the lightest books were on the bottom of the stack and the heaviest books were on top of the stack. How far out can you stack an infinite number of books where each book is twice as heavy as the book below it (we're looking for either infinitely far or finitely far)? Justify your answer.

(c) What if the books were Harmonically weighted: 1, $\frac{1}{2}$, $\frac{1}{3}$, *etc*., *etc*., and the heaviest book had to be on top. Would it be possible for the top of the stack to be arbitrarily far past the edge of the table?

Problem 7. Use the integral method to find upper and lower bounds for the following summation that differ by at most 0.05.

$$\sum_{i=1}^{\infty} \frac{1}{i^3}$$

Hint: Try adding the first few terms explicitly and then use integrals to bound the sum of the remaining terms.

Problem 8. **(a)** Given that $f(x) = O(g(x))$, prove that $f(x)^2 = O(g(x)^2)$

(b) Let $f(x) ::= 2x$ and $g(x) ::= x$, so $f(x) = O(g(x))$. Prove that $2^{g(x)} = o(2^{f(x)})$, so $2^{f(x)} \neq O(2^{g(x)})$.

Student's Solutions to Problem Set 6

Your name:

Due date: October 26

Submission date:

Circle your TA: David Jelani Sayan Hanson

Collaboration statement: Circle one of the two choices and provide all pertinent info.

1. I worked alone and only with course materials.
2. I collaborated on this assignment with:

   got help from:[1]

   and referred to:[2]

DO NOT WRITE BELOW THIS LINE

Problem	Score
1	
2	
3	
4	
5	
6	
7	
8	
Total	

[1] People other than course staff.

[2] Give citations to texts and material other than the Fall '02 course materials.