

MATH 145, EXAM 2 SOLUTIONS, 07 MARCH, 2008

(Each of the following four problems is worth 15 points.)

- (1) In designing a toy RSA encryption system, the public data is $N = 39$, with public key $e = 5$. Answer the following:

- (a) What is the encryption $f(15)$ of 15?

This is simply $15^5 \bmod 39$, which everyone in the class calculated correctly to be 6.

- (b) What are all the possible other public keys you could use in this system?

When $N = pq$, where p and q are distinct primes, the messages are members of \mathbb{Z}_N , but the keys are from $\mathbb{Z}_{(p-1)(q-1)}$. In this case $p = 3$, $q = 13$; so keys are units in \mathbb{Z}_{24} . Of course some units are better than others—imagine encrypting with 1—but the entire collection of possible keys is $\{1, 5, 7, 11, 13, 17, 19, 23\}$.

- (c) Why—in principle—is it “hard” to find the decryption key d , given N and the encryption key e ?

The big obstacle to finding d is that you need to factor N into the primes p and q . When N has 200 digits, this can be a huge computation overhead. Once you find these primes, though, the inversion of the public key is not excessively time consuming.

- (2) Use truth table semantics to establish the following:

- (a) $\neg(p \wedge q)$ and $(\neg p) \vee (\neg q)$ are logically equivalent.

The truth table involving both propositions is:

p	q	$\neg(p \wedge q)$	$(\neg p) \vee (\neg q)$
0	0	1	1
0	1	1	1
1	0	1	1
1	1	0	0

Since the relevant columns are identical, we conclude the propositions to be logically equivalent.

- (b) If $p * q$ is a binary connective whose truth value semantics is defined by the function $f(m, n) = mn + n + 1$ over \mathbb{Z}_2 , then $p * q$ is logically equivalent to $p \vee (\neg q)$.

We're taking $T(p * q) = f(T(p), T(q))$, so the relevant truth table is:

p	q	$p * q$	$p \vee (\neg q)$
0	0	1	1
0	1	0	0
1	0	1	1
1	1	1	1

Again, the two rightmost columns are identical, so we conclude that $p * q$ is an abbreviation for $p \vee (\neg q)$.

(c) $p \wedge (q \vee r)$ is *not* logically equivalent to $(p \wedge q) \vee r$.

Any truth assignment T with $T(p) = 0$ and $T(r) = 1$ will give truth value 0 to $p \wedge (q \vee r)$ and value 1 to $(p \wedge q) \vee r$. This shows the two expressions to be logically inequivalent.

(3) Using only the predicates: $P(x, y, z)$ for “ x is the product of y and z ”; $S(x, y, z)$ for “ x is the sum of y and z ”; $L(x, y)$ for “ x is strictly less than y ”; $E(x, y)$ for “ x equals y ”; and 0, 1 for the constants zero and one, write down a first order formula which says of an integer $n \in \mathbb{Z}$ that:

(a) n is nonnegative.

To express “ n is negative” is to write $L(n, 0)$. So to express “ n is nonnegative,” we write $\neg L(n, 0)$. (Equivalently, one could also write $L(n, 0) \vee E(n, 0)$.)

(b) n is odd.

n is odd just in case n is not even. This becomes $\neg \exists x S(n, x, x)$. There are lots of other reformulations one could concoct; for example, you could write $\forall x [S(x, 1, 1) \Rightarrow \neg \exists y P(n, x, y)]$. This simply says that n is not the product of anything and 2.

(c) n is prime.

This says that n cannot be written as a product without one or the other of the factors being 1. To wit: $\forall x \forall y [P(n, x, y) \Rightarrow (E(x, 1) \vee E(y, 1))]$.

(4) (a) Show that $S(n) = 3^n(1 + n)$ is a solution to the recurrence, $T(n) = 3T(n - 1) + 3^n$, with $T(0) = 1$.

First, to establish the base case, we have $S(0) = 3^0(1+0) = 1 = T(0)$. Now assume $n \geq 1$ is fixed and that $S(n - 1) = T(n - 1)$. Then

$$T(n) = 3T(n-1) + 3^n = 3S(n-1) + 3^n = 3[3^{n-1}(1 + (n-1))] + 3^n = 3^n(1 + (n-1) + 1) = S(n).$$

- (b) Show that $S(n) = 3^n(1 + n)$ is *not* a solution to the recurrence, $T(n) = 2T(n-1) + 3^n$, with $T(0) = 1$.

The two start to disagree fairly early. Although $T(0) = S(0)$, it turns out that $T(1) = 2 \cdot 1 + 3^1 = 5 \neq 6 = 3^1(1 + 1) = S(1)$. This is enough to show that the functions given by the formula for $S(n)$ and the recurrence for $T(n)$ are not the same.

- (c) Give a concrete example of a recurrence that is not first order.

Any recurrence that depends on two or more previous values will do. For example, you could use the Fibonacci sequence $F(0) = F(1) = 1$; $F(n) = F(n-1) + F(n-2)$ for $n \geq 2$.