University of Washington
Department of Computer Science and Engineering
CSE 321, Winter 2008

February 10, 2008

Midterm Exam Answers, Friday, February 8, 2008

Problem 1 (10 points):

a) Show that the expression $(p \to q) \to (p \to r)$ is a contingency.

The expression is true if all variables are true. It is false if p and q are true, and r is false.

b) Give an expression that is logically equivalent to $(p \to q) \to (p \to r)$ using the logical operators $\neg$, $\vee$, and $\wedge$ (but not $\to$).

The simplest method is just to use the equivalence $a \to b \equiv (\neg a \vee b)$. This gives $\neg(\neg p \vee q) \vee (\neg p \vee r)$, which can be simplified by DeMorgan's law to $(p \wedge \neg q) \vee \neg p \vee r$ and can be further simplifed to $\neg p \vee \neg q \vee r$.

Problem 2 (20 points):

Using the predicates:

$Likes(p, f)$: "Person p likes to eat the food f."
$Serves(r, f)$: "Restaurant r serves the food f."

translate the following statements into logical expressions.

a) Every restaurant serves a food that no one likes.

$$\forall r \exists f \forall p(Serves(r, f) \wedge \neg Likes(p, f))$$

The most common incorrect answer had the quantifers in the wrong order: $\forall r \forall p \exists f$. This would say "At every restaurant, everyone has something that they don't like,"

b) Every restaurant that serves TOFU also serves a food which RANDY does not like.

$$\forall r \exists f(Serves(r, \text{TOFU}) \to (Serves(r, f) \wedge \neg Likes(\text{RANDY}, f)))$$

Translate the following logical expressions into English. (You may want to give a couple of sentences of explanation - the point of this question is to demonstrate that you understand the logical expression.)

c) $\exists r \forall p \exists f(Serves(r, f) \wedge Likes(p, f))$

There is a restaurant where everyone likes something it serves.

The answer "There is some restaurant that serves some food that everyone likes" is incorrect, since that says that the same food is liked by everyone.

d) $\forall r \exists p \forall f (Serves(r, f) \rightarrow Likes(p, f))$

Every restaurant has a person that likes everything it serves.

Problem 3 (10 points):

Determine the value of the following. (You will probably want to use different methods to compute the values.)

a) $3^{303} \bmod 101$

$3^{303} \bmod 101 = 27$

Fermat's little theorem says that $a^{p-1} \equiv 1 (\mathrm{mod} p)$ for p a prime number. Since 101 is prime, $3^{303} \bmod 101 = 3^{300+3} \bmod 101 = 3^3 \bmod 101 = 27 \bmod 101 = 27$.

b) $3^{64} \bmod 100$

$3^{64} \bmod 100 = 81$

To compute $3^{64} \bmod 100$ we use repeated squaring to compute $3^2, 3^4, 3^8, 3^{16}, 3^{32}, 3^{64}$. The key is to reduce modulo 100 during the computations to avoiding having to do too much arithmetic.

$$
\begin{aligned}
3^2 \bmod 100 &= 3 \times 3 \bmod 100 &&= 9 \\
3^4 \bmod 100 &= 9 \times 9 \bmod 100 &&= 81 \\
3^8 \bmod 100 &= 81 \times 81 \bmod 100 &&= 61 \\
3^{16} \bmod 100 &= 61 \times 61 \bmod 100 &&= 21 \\
3^{32} \bmod 100 &= 21 \times 21 \bmod 100 &&= 41 \\
3^{64} \bmod 100 &= 41 \times 41 \bmod 100 &&= 81
\end{aligned}
$$

Problem 4 (15 points):

a) What is public key cryptography?

A method of exchanging secret messages that does not require a prior exchange of secret data. For RSA, the receiver publicizes an encryption key e and modulus n.

b) What is the computation that "Alice" employs when she encodes a message using RSA?

$M^e \bmod n$.

c) Why is RSA considered secure?

Because very large integers are used, and there is no known method of finding the decryption key efficiently. Since the number involved have hundreds of decimal digits, brute force methods are not feasible. (The answer "because there is no efficient algorithm for factoring" is technically not correct, but received full credit. If one could factor quickly, one could break RSA, but the converse is not necessarily true. It is possible that one could come up with an algorithm for breaking RSA that does not involve factoring.)

Problem 5 (10 points):

Use rules of inference to show that if the premises $\forall x(P(x) \rightarrow Q(x))$, $\forall x(Q(x) \rightarrow R(x))$, and $\neg R(a)$, where a is in the domain, are true, then the conclusion $\neg P(a)$ is true. (Note: You do not need to give the names for the rules of inference.)

Here is a proof based on using hypothetical syllogism to combine the implications. Another approach is to apply Modus Tollens twice.

1)	$\forall x(P(x) \rightarrow Q(x))$	Hypothesis
2)	$P(a) \rightarrow Q(a)$	Universal Instantiation of 1
3)	$\forall x(Q(x) \rightarrow R(x))$	Hypothesis
4)	$Q(a) \rightarrow R(a)$	Universal Instantiation of 3
5)	$P(a) \rightarrow R(a)$	Hypothetical Syllogism of 2 and 4
6)	$\neg R(a)$	Hypothesis
7)	$\neg P(a)$	Modus Tollens of 5 and 6

Problem 6 (10 points):

Prove that if n is even and m is odd, then $(n+1)(m+1)$ is even.

Let n be even and m be odd. By definition of odd, $m = 2k+1$ for some $k \in \mathcal{Z}$. Then $(n+1)(m+1) = (n+1)(2k+1+1) = (n+1)(2k+2) = 2((n+1)(k+1))$. By definition of even, $(n+1)(m+1)$ is even.

Problem 7 (10 points):

Prove or disprove:

a) For positive integers x, p, and q, $(x \bmod p) \bmod q = x \bmod pq$.

False. Let $x = 10$, $p = 7$, $q = 3$. $(10 \bmod 7) \bmod 3 = 0$, $10 \bmod 21 = 10$.

b) For positive integers x, p, and q, $(x \bmod p) \bmod q = (x \bmod q) \bmod p$.

False. Let $x = 10$, $p = 7$, $q = 3$. $(10 \bmod 7) \bmod 3 = 0$, $(10 \bmod 3) \bmod 7 = 3$.