CS70 Discrete Mathematics and Probability Theory, Spring 2009

Midterm 1 Solutions

Note: These solutions are not necessarily model answers. Rather, they are designed to be tutorial in nature, and sometimes contain more explanation (occasionally much more) than an ideal solution. Also, bear in mind that there may be more than one correct solution. The maximum total number of points available is 60. 2 points are deducted for a wrong answer in Q. 1

1. [Logic]

2pts

(a) **Valid:** We can see this by rewriting the implication and applying De Morgan's laws.

$$\begin{aligned} \forall n(\neg Q(n) \Rightarrow P(n)) &\equiv \forall n(Q(n) \vee P(n)) \\ &\equiv \forall n \neg(\neg P(n) \wedge \neg Q(n) \\ &\equiv \neg[\exists n(\neg P(n) \wedge \neg Q(n))] \end{aligned}$$

2pts

(b) **Invalid:** We can see this by looking at the right hand side of the equivalence. Note that the logical expression $(P \vee \neg P)$ is always going to be true. Therefore, we see that the expression

$$\forall n[(P(n) \vee \neg P(n)) \wedge (Q(n) \vee \neg Q(n))]$$

is always true. However, it is not true that the left hand side expression $\forall n(P(n) \Leftrightarrow Q(n))$ is always true, and so the equivalence is invalid.

2pts

(c) **Valid:** We can see this by rewriting the implication and applying De Morgan's laws.

$$\begin{aligned} &\forall m \forall n\ [R(m,n) \Rightarrow \neg(\forall l[R(m+l,n) \vee R(n,m+l)])] \\ \equiv\ &\forall m \forall n\ [\neg R(m,n) \vee \neg(\forall l[R(m+l,n) \vee R(n,m+l)])] \\ \equiv\ &\forall m \forall n\ [\neg R(m,n) \vee \exists l\ \neg(R(m+l,n) \vee R(n,m+l))] \\ \equiv\ &\forall m \forall n\ [\neg R(m,n) \vee \exists l\ (\neg R(m+l,n) \wedge \neg R(n,m+l))] \end{aligned}$$

2pts

(d) **Invalid:** We can see this just by coming up with a simple counterexample. In order for the equivalence to be valid, it needs to be valid for all possible $R(m,n)$. If we can find an proposition $R(m,n)$ such that the equivalence does not hold, then it must be invalid. Consider the proposition $R(m,n) = (m = n^2)$. We are looking at the equivalence

$$\forall n \exists m\ R(m,n) \equiv \exists m \forall n\ R(n,m)$$

Now, it is true that $\forall n, \exists m(m = n^2)$ - we can just pick $m = n^2$ which is a natural number, and so the left hand side of the equivalence is true with this particular choice of $R(m,n)$. However, it is not true that $\exists m \forall n(n = m^2)$. This should be obvious to see that all of the natural numbers n are not all the square of the same natural number m.

Note: This is obviously not the only possible counterexample that we can use. For example another counterexample, $R(m,n) = (m > n)$ would be valid as well.

2. [Induction]

Prove by induction that the sum of the interior angles of a convex polygon with n vertices is exactly $(n-2)\pi$.

Proof:

(a) **Base case:** For $n = 3$ we have a triangle. From elementary geometry we know that the sum of the interior angles of a triangle is $(3-2)\pi = \pi$. *3pts*

(b) **Inductive Step:** The inductive hypothesis is that for all polygons with up to n edges, we have that the sum of their interior angles is $(n-2)\pi$. Using this inductive hypothesis we will show this holds for polygons with $n+1$ edges. To prove this we will reduce the case of an $n+1$ polygon (polygon with $n+1$ edges) to the n polygon case. The idea of the proof is to show that any $n+1$ polygon can be represented as an n polygon and a triangle, s.t. adding the sum of the interior angles of the triangle and the n polygon will result the sum of the interior angles of the $n+1$ polygon. *7pts*

Formally, given an $n+1$ polygon, let A, B, C be three adjacent vertices, and let α, β, γ be the interior angles of the polygon which correspond to vertices A, B, C, respectively. Note that three such vertices exist since we are showing for all $n > 3$. Drawing an edge between A and C splits the polygon into two parts: a triangle ABC and the remaining polygon (always exists for $n > 3$, otherwise, we have the base case $n = 3$). Since the polygon is convex, the edge AC is inside the polygon, and therefore ABC is inside the $n+1$ polygon. Also, the remaining polygon is a polygon with n edges, since it is the original polygon with AC replacing AB and BC.

The interior degrees of ABC are $\angle BAC$, β and $\angle BCA$. The interior degrees of the n polygon are the same as in the $n+1$ polygon, except β is not in the n polygon (B is not a vertex in it), and the angles on A and C on the n polygon are simply $\alpha - \angle BAC$ and $\gamma - \angle BCA$. Therefore the sum of the interior angles of the n polygon plus the sum of the triangle's interior angles are exactly the sum of the interior angles of the $n+1$ polygon. We know that the sum of the interior angles of the triangle is π and, by the inductive hypothesis, the sum of the interior angles of the the n polygon is $(n-2)\pi$. Thus, together, we have that the sum of the interior angles of the $n+1$ polygon is $(n-1)\pi$, as required.

Notes: Perhaps the most common error was reducing in the other direction, i.e. taking an n polygon, adding an additional vertex, and connecting it to the polygon. The argument was that this gives a triangle and the original polygon and therefore proves the inductive hypothesis. Note that this is wrong, since this does not prove the statement for any $n+1$ polygon, but the specific one which was created using the n polygon. Other common errors involved using $n = 2$ as the base case. Some answers included statements like "Clearly, any $n+1$ polygon is an n polygon with a triangle" without any clarification or proof, which was the main idea here.

3. [Stable Marriage]

4pts

(a) Recall that the traditional marriage algorithm (propose and reject) that we discussed in class gives us a male-optimal stable matching. So, we run this with our given preference lists to get:

Day	Women	Men
1	a	A
	b	B
	c	-
	d	~~C~~, D
2	a	A
	b	B
	c	C
	d	D

So our male-optimal stable matching is (A, a), (B, b), (C, c), (D, d).

Now, in order to get the female-optimal stable matching, we can run the propose and reject algorithm with the roles reversed (i.e., the women propose). Running this with our preference lists gets:

Day	Men	Women
1	A	c
	B	-
	C	-
	D	~~a~~, ~~b~~, d
2	A	c
	B	a
	C	b
	D	d

So our female-otpimal stable matching is (A, c), (B, a), (C, b), (D, d). *2pts*

(b) Now, we need to find a stable matching which is neither male-optimal nor female-optimal. Now, since the male-optimal and female-optimal stable matchings are unique and have been found in part (a), what we basically have to do is to find a third stable matching. It turns out that such a matching does exist. The first thing we notice is that since D and d are on the top of each other's preference, lists, they must be paired together in any stable matching. So, we can now consider the preference list with just A, B, C, a, b, and c. We get

Men	Women		
A	a	b	c
B	b	c	a
C	c	a	b

Women	Men		
a	B	C	A
b	C	A	B
c	A	B	C

In the male-optimal matching, we ended up pairing all of the men with their most preferred woman among {a, b, c}. In the female-optimal matching, we ended up pairing all of the women with their most preferred man among {A, B, C}. We also notice that the most preferred woman for all of the guys is precisely the woman who dislikes him the most and vice versa. Combining these facts, it seems like a reasonable idea to give all of the people their middle choice. So combining with the fact that D and d must be together, a candidate matching we consider is (A, b), (B, c), (C, a), (D, d). In fact, it turns out that this is a stable matching (this can be done by verifying that there are no rogue couples) and since it is different from both matchings that we got from part (a), it is neither male-optimal nor female-optimal.

Notes: In general, people did well on this problem. However, there was some confusion on part (b). The main worry was that people were confused about what it means to have a stable matching - a number of people said that since neither the guys nor the girls would be getting their first choices, then the matching would no longer be stable. The thing to realize is that a matching is stable as long as no rogue couples exist - and that properties such as male-otpimality and female-optimality are additional properties on top of that.

4. [Modular Arithmetic]

4pts

(a) Following the extended gcd algorithm from the lecture notes, we obtain the following sequence of recursive calls (x, y) and corresponding triples of returned values (d, a, b):

$$\begin{array}{ccccccccc} \text{e-gcd}(48,5) & \longrightarrow & \text{e-gcd}(5,3) & \longrightarrow & \text{e-gcd}(3,2) & \longrightarrow & \text{e-gcd}(2,1) & \longrightarrow & \text{e-gcd}(1,0) \\ (1,2,-19) & \longleftarrow & (1,-1,2) & \longleftarrow & (1,1,-1) & \longleftarrow & (1,0,1) & \longleftarrow & (1,1,0) \end{array}$$

The final triple $(d, a, b) = (1, 2, -19)$ tells us that $\text{gcd}(48.5) = 1$, and that this value can be expressed as $48 \times a + 5 \times b)$, i.e., $1 = 48 \times 2 + 5 \times (-19)$. Hence the inverse of 5 mod 48 is $-19 = 29$.

Some people obtained the correct answer without using the extended gcd algorithm (essentially by guessing the answer, or trying various possibilities). They lost most of the credit: the point of this question was to use a systematic method (i.e., extended gcd) to find inverses.

4pts

(b) First note that, by subtracting 7 from both sides, the equation becomes

$$5x = 13 \bmod 48.$$

Multiplying both sides by $5^{-1} = 29$ we get

$$x = (13 \times 29) = 377 = 41 \bmod 48.$$

This is the unique solution mod 48. (Of course, over the integers any x of the form $41 + 48k$ for integer k is also a solution.)

Again, some people obtained the correct answer by trial-and-error rather than by the systematic method above. Again, they lost most of the credit.

4pts

(c) Since $\gcd(48, 6) = 6 \neq 1$, we know that 6 has no inverse mod 48. Hence we cannot use the approach of part (b) to obtain a unique solution. However, this does not necessarily mean that no solution exists (see below). To decide this, note that any solution must satisfy

$$6x = 13 + 48k$$

for some integer k. (This is an integer equation, not a modular one.) But since $6x$ and $48k$ are both divisible by 6, while 13 is not, we see that this equation can have no solutions.

Many people simply said that, because 6 has no inverse mod 48, the equation has no solution. This is not a valid implication. For example, the equation $6x + 7 = 19 \bmod 48$ *has many solutions; it is equivalent to* $6x = 12 \bmod 48$*, with solutions* $x = 2, 10, 18, 26, 34, 42$*. The reason it has solutions is that* $\gcd(6, 48)$ *also divides 12.*

5. [Divisibility Tests]

a) This problem was attempted in many ways. Below are three possible solutions to the problem: *5pts*

- **Simplifying using rules of modular arithmetic**

  Let n be a k-digit number for some $k \geq 1$, written as $a_{k-1}a_{k-2}\ldots a_0$. Then we know that

$$n \;=\; (10^{k-1} \times a_{k-1}) + (10^{k-2} \times a_{k-2}) + \ldots + (10^0 \times a_0) \;=\; \sum_{i=0}^{k-1}(10^i \times a_i)$$

  Using the rules of modular arithemetic, we can write $n \bmod 3$ as

$$\begin{aligned}
n \bmod 3 \;&=\; \sum_{i=0}^{k-1}(10^i \times a_i) \mod 3 \\
&=\; \sum_{i=0}^{k-1}((10^i \bmod 3) \times a_i) \mod 3 \\
&=\; \sum_{i=0}^{k-1}((10 \bmod 3)^i \times a_i) \mod 3 \\
&=\; \sum_{i=0}^{k-1}(1 \times a_i) \mod 3 \\
&=\; s \bmod 3 \qquad (\text{Since } s = \sum_{i=0}^{k-1} a_i)
\end{aligned}$$

  A slightly different (and somewhat more formal) version of this argument could be to use induction on the number of digits.

- **By considering $\mathbf{n - s}$ mod 3**
  Writing n and s as before, we can write $n - s$ as

$$\begin{aligned} n - s &= \sum_{i=0}^{k-1}(10^i \times a_i) - \sum_{i=0}^{k-1} a_i \\ &= \sum_{i=0}^{k-1}(10^i - 1) \times a_i \end{aligned}$$

  It remains to notice that for each $i \geq 0$, $10^i - 1$ is a multiple of 3 (it is 0 for $i = 0$ and a number consisting of i 9s for $i \geq 1$) and hence the right hand side in the above equation is divisible by 3. This gives $n - s = 0 \mod 3$, which implies $n = s \mod 3$.

- **By induction on the number $\mathbf{n}$**
  For the base case, we can consider $n = 0$ and note that $n = s = 0 \mod 3$. For a number n, let $s(n)$ denote the sum of digits of n. Assuming $n = s(n) \mod 3$, we would now like to prove that $n + 1 = s(n+1) \mod 3$.
  If the last digit of n is between 0 and 8, then all digits of $n + 1$ are the same as those in n, except for the last one which increases by 1. Hence in this case $s(n+1) = s(n) + 1$ and we get

$$n = s(n) \mod 3 \implies n + 1 = s(n) + 1 = s(n+1) \mod 3$$

  However, if the last digit of n is 9, then the digits of $n + 1$ may be very different from those of n. In particular, if the last k digits of n are 9, then they all change to 0, and the $(k+1)^{th}$ digit from the right (which is not 9) increases by 1. Hence $s(n+1) = s(n) - 9k + 1$. This also gives

$$s(n+1) \;=\; s(n) - 9k + 1 \;=\; s(n) + 1 \;=\; n + 1 \mod 3$$

The induction approach is somewhat harder to get right as compared to the others, while the first one (using rules of modular arithmetic) is the simplest. Many people who approached the problem by induction on n failed to realize that $s(n+1)$ may not be equal $s(n) + 1$, in which case no credit was given. Partial credit was given in the case when someone considered that $s(n+1)$ may be different, but did not fully specify how it can change.

b) This is an “if and only if” statement and hence to give a proof we need to give arguments for both the “if” and the “only if” directions. To prove the the “if” part, we note that if s is divisible by 3, then $s = 0 \mod 3$ which implies that $n = 0 \mod 3$ (since we know from part a) that $n = s \mod 3$) and hence n is divisible by 3. To prove the “only if” part we note that if n is divisible by 3, then $n = 0 \mod 3$. Using part a) this implies that $s = 0 \mod 3$ which shows that s is divisible by 3. *2pts*

c) One can give a test for divisibility by 9 identical to the one for 3. In particular, *3pts*

“A number n is divisible by 9 if and only if the sum of its digits is divisible by 9”

The correctness of the test can be verified by noting that each of the arguments in part a) also prove that $n = s \mod 9$. For example, in the first argument, we simply proved it using that $10 = 1 \mod 3$. Since it is also true that $10 = 1 \mod 9$ the argument also proves $n = s \mod 9$. It then follows by an argument identical to part b) that the test correctly checks divisibility by 9.

People who only gave the test without any justification received only 1 out of 3 points.

6. [Secret sharing]

7pts

(a) Lagrange interpolation:

$$\begin{aligned}
\Delta_1(x) &= \frac{(x-2)(x-4)}{(1-2)(1-4)} = 4x^2+9x+10 \mod 11. \qquad (3^{-1}=4 \mod 11) \\
\Delta_2(x) &= \frac{(x-1)(x-4)}{(2-1)(2-4)} = 5x^2+8x+9 \mod 11. \qquad ((-2)^{-1}=5 \mod 11) \\
\Delta_3(x) &= \frac{(x-1)(x-2)}{(4-1)(4-2)} = 2x^2+5x+4 \mod 11. \qquad (6^{-1}=2 \mod 11)
\end{aligned}$$

$$p(x) = p(1)\Delta_1(x) + p(2)\Delta_2(x) + p(4)\Delta_3(x) = 8x^2+5x+7 \mod 11$$

$$s = p(0) = 7.$$

Quite a few students leave the coefficients of the polynomials in factional form. They should be in between 0 and 11, (i.e. the inverses need to be explicitly calculated.)

5pts

(b) Instead of reporting the true value of $p(1)$, the cheater can report instead a such that $a\Delta_1(0) = p(1)\Delta(0) + 1 \mod 11$, so that player 2 and 4 will mistakenly calculate a value of s greater by 1 when they evaluate the polynomial at $x = 0$. Solving this equation using $\Delta_1(0) = 10$ yields $a = 8$. Note that the cheater can calculate this value of a without knowing a priori the values of $p(2)$ and $p(4)$.