CS 70 Discrete Mathematics and Probability Theory
Fall 2010 Tse/Wagner MT 1 Soln

Problem 1. [True or false] (16 points)

(a) $\boxed{\text{TRUE}}$ or FALSE: $(\forall x \in \mathbb{N})(\exists y \in \mathbb{N})(x = y)$.

(b) $\boxed{\text{TRUE}}$ or FALSE: $(\forall x \in \mathbb{N})(\exists y \in \mathbb{N})(x^6 = y^2)$.
Comment: Simply take $y = x^3$.

(c) TRUE or $\boxed{\text{FALSE}}$: For all $x, y \in \mathbb{N}$, if $x + 9 \equiv y + 9 \pmod{26}$, then $x \equiv y - 9 \pmod{26}$.

(d) $\boxed{\text{TRUE}}$ or FALSE: For all $x, y \in \mathbb{N}$, if $9x \equiv y \pmod{26}$, then $x \equiv 3y \pmod{26}$.
Comment: Simply multiply both sides by 3, noting that $3 \times 9 \equiv 1 \pmod{26}$.

(e) TRUE or $\boxed{\text{FALSE}}$: For all $x, y \in \mathbb{N}$, if $10x + 13 \equiv 14y + 7 \pmod{26}$, then $5x + 3 \equiv 7y \pmod{26}$.
Comment: We cannot multiply both sides by the inverse of 2: 2 has no inverse, since $\gcd(2, 26) \neq 1$.

(f) $\boxed{\text{TRUE}}$ or FALSE: $\gcd(267, 368) = \gcd(101, 267)$.

(g) $\boxed{\text{TRUE}}$ or FALSE: For all $x, y \in \mathbb{N}$, $\gcd(2x, 2y) = 2\gcd(x, y)$.

(h) TRUE or $\boxed{\text{FALSE}}$: For all $x, y \in \mathbb{N}$, $\gcd(2x, 3y) = \gcd(x, y)$.
Comment: Consider $x = 3$, $y = 2$.

Problem 2. [Propositional logic] (12 points)

(a) $P \implies Q$:

P	Q	$P \implies Q$
false	false	$\boxed{\text{true}}$
false	true	$\boxed{\text{true}}$
true	false	$\boxed{\text{false}}$
true	true	$\boxed{\text{true}}$

(b) $(P \wedge Q) \implies (P \wedge Q)$:

P	Q	$(P \wedge Q) \implies (P \wedge Q)$
false	false	$\boxed{\text{true}}$
false	true	$\boxed{\text{true}}$
true	false	$\boxed{\text{true}}$
true	true	$\boxed{\text{true}}$

(c) $(P \wedge (\neg Q)) \vee ((\neg P) \wedge Q)$:

P	Q	$(P \wedge (\neg Q)) \vee ((\neg P) \wedge Q)$
false	false	false
false	true	true
true	false	true
true	true	false

Problem 3. [Grade this proof] (8 points)

Theorem. For all $n \in \mathbb{N}$ with $n \geq 1$, we have

$$10 + 20 + 30 + \cdots + 10n \leq 4n^2 + 6n + 20.$$

Proof: The proof is by induction.

Base case: for $n = 1$, the left-hand-side is 10, which is indeed less than $4 \times 1^3 + 6 \times 1^2 + 20 = 30$.

Induction hypothesis: Suppose $10 + \cdots + 10k \leq 4k^2 + 6k + 20$ for some k with $k \geq 1$.

Inductive step: We want to prove

$$10 + \cdots + 10(k+1) \leq 4(k+1)^2 + 6(k+1) + 20.$$

Expanding out the sum and manipulating arithmetic expressions, we get

$$\begin{aligned}
10 + \cdots + 10(k+1) &\leq 4(k+1)^2 + 6(k+1) + 20 \\
10 + \cdots + 10k + 10(k+1) &\leq 4(k+1)^2 + 6(k+1) + 20 \\
10 + \cdots + 10k &\leq 4(k+1)^2 + 6(k+1) + 20 - 10(k+1) \\
10 + \cdots + 10k &\leq (4k^2 + 8k + 4) + (6k + 6) + 20 - (10k + 10) \\
10 + \cdots + 10k &\leq 4k^2 + 4k + 20 \\
10 + \cdots + 10k &\boxed{\leq 4k^2 + 6k + 20}
\end{aligned}$$

which is true—where in the last step we used the fact that $4k \leq 6k$ for all $k \geq 1$. Therefore, the theorem follows by induction. □

You be the grader. Decide whether you think the proof is valid or not, and assign it either an A (valid proof) or an F (invalid proof).

(a) The grade you are giving it: F

(b) If you gave an F in part (a), circle the first erroneous step, and explain the logical error in the proof.

The error is reasoning backwards. You can't start by assuming what you want to prove. And if we try to read this in reverse order, then we find that there is a logical flaw: $10 + \cdots + 10k \leq 4k^2 + 6k + 20$ does not imply $10 + \cdots + 10k \leq 4k^2 + 4k + 20$.

Comment: This may illustrate why not to use "reasoning backwards." Working backwards may be easier for the person trying to find a proof (after all, when setting out on a long journey, it helps to know where you want to end up), but it is harder on the person reading the proof, because it makes it harder to spot errors like the one above.

Common errors (added 10/13): Some people suggested that you're not allowed to subtract $10(k+1)$ from both sides of an inequality. This is incorrect; it is fine to subtract a quantity from both sides of an inequality that's known to be true. (If $a \leq b$, then certainly $a - c \leq b - c$.)

Some folks suggested that in an induction step you have to start with one side of the goal and manipulate it; you're not allowed to manipulate both sides of an inequality. This is too sweeping. If you have an inequality that is known to be correct, it is fine to find alternate expressions for either or both sides of it, or to transform both sides (e.g., multiplying both sides by a positive number, or subtracting both sides by the same number).

Problem 4. [Counting] (20 points)

(a) How many ways are there to put capital letters in a 4×4 grid, if letters are allowed to appear more than once? $\boxed{26^{16}}$

(b) How many ways are there to put capital letters in a 4×4 grid, if no letter is allowed to appear more than once in the grid? $\boxed{\frac{26!}{10!}}$

Comment: There are 26 choices for the first grad square, 25 choices for the next grid square, and so on, so there are $26 \times 25 \times \cdots \times 11$ ways to do it.

(c) How many ways are there to put capital letters in a 4×4 grid, if we insist that no two rows of the grid be identical? $\boxed{26^4 \times (26^4 - 1) \times (26^4 - 2) \times (26^4 - 3)}$

Comment: There are 26^4 possibilities for the first row, $26^4 - 1$ for the second row (since it cannot be the same as the first row), and so on.

(d) How many ways are there to put capital letters in the 4×4 grid, if we insist that in each row, the letters must be in strictly increasing order (from left to right)? $\boxed{\binom{26}{4}^4}$

Comment: There are $\binom{26}{4}$ possibilities for each row: choose any subset of 4 of the 26 letters, and then create a row by listing them in order.

(e) How many ways are there to put capital letters in the 4×4 grid, if we insist that in each row, the letters must be in non-decreasing order (from left to right)? $\boxed{\binom{29}{4}^4}$

Comment: There are $\binom{29}{4}$ possibilities for each row. Choosing a row is the same as distributing 4 coins among 26 pirates, where each pirate is labelled with a different capital letter, and if a pirate receives some number of coins, then his letter appears that many times in the row. In other words, the number of ways to form a row is the number of solutions to $x_A + x_B + \cdots + x_Z = 4$ in the natural numbers, where $x_i \in \mathbb{N}$ counts the number of times that letter i should appear in the row.

Comment (added 10/13): Another way to compute the number of possibilities is to observe that a row may contain all one letter, for which there are $\binom{26}{1}$ possibilities. It may also contain exactly two

different letters, in which case there are $\binom{26}{2}$ choices for which letters to use. Then the two letters can be arranged in three different ways; for example, the three arrangements for A and B are AAAB, AABB, and ABBB. Thus, there are $3 \cdot \binom{26}{2}$ ways to fill a row with two letters. Similar arguments demonstrate that there are $3 \cdot \binom{26}{3}$ ways to fill a row with three different letters and $\binom{26}{4}$ for four letters. Thus, the total number of ways to fill a row is $\binom{26}{1} + 3 \cdot \binom{26}{2} + 3 \cdot \binom{26}{3} + \binom{26}{4}$, so the total number of ways to fill the grid is $(\binom{26}{1} + 3 \cdot \binom{26}{2} + 3 \cdot \binom{26}{3} + \binom{26}{4})^4$.

Common errors (added 10/13): A number of students came up with very complicated expressions for parts (d) and (e). If you end up with something very complicated, it is a strong hint that you are approaching the problem incorrectly and that a better approach exists.

Problem 5. [Modular arithmetic] (18 points)

Define the function $f : \{1,2,\ldots,2010\} \to \{0,1,\ldots,2010\}$ such that $f(x) \equiv x^{-1}(x+1) \pmod{2011}$.

(a) Prove that f is a one-to-one function, or in other words, that there does not exist $x, y \in \{1,2,\ldots,2010\}$ such that $f(x) \equiv f(y) \pmod{2011}$ and $x \not\equiv y \pmod{2011}$.

Hint: 2011 is prime. (You may assume this; you do not need to prove that 2011 is prime.)

Note that $f(x) \equiv x^{-1}(x+1) \equiv 1 + x^{-1} \pmod{2011}$. Suppose $f(x) \equiv f(y) \pmod{2011}$, or in other words, $1 + x^{-1} \equiv 1 + y^{-1} \pmod{2011}$. Subtract 1 from both sides to obtain

$$x^{-1} \equiv y^{-1} \pmod{2011}. \tag{1}$$

Multiplying both sides of the above equation by xy, we get $y \equiv x \pmod{2011}$. In other words, we have proved that $f(x) \equiv f(y) \pmod{2011}$ implies $x \equiv y \pmod{2011}$.

Comment: You could also observe that the inverse of x^{-1} is x and the inverse of y^{-1} is y, so taking inverses of both sides of the equation (1) yields $x \equiv y \pmod{2011}$.

Common errors (added 10/13): Many people cited the fact, proven in class, that if $x \not\equiv 0 \pmod{2011}$, then the inverse of x exists and is unique. This is correct, but be careful: it might not mean what you think it means. In this context, "unique" means that there is only one inverse of x (we don't have two different numbers which both have a valid claim to be the inverse of x). Thus, uniqueness ensures that the function $g(x) \equiv x^{-1} \pmod{2011}$ is indeed a well-defined function (which is already implicitly assumed in the question; otherwise the notation x^{-1} doesn't even make sense). However, uniqueness says nothing about whether g is one-to-one, or in other words, whether there might exist x, y such that $x^{-1} \equiv y^{-1} \pmod{2011}$ but $x \not\equiv y \pmod{2011}$. In fact, it is true that if $x^{-1} \equiv y^{-1} \pmod{2011}$, then we necessarily have $x \equiv y \pmod{2011}$, but this fact requires justification as described above. Simply saying that the inverse is unique isn't sufficient justification.

Unfortunately, the sample proof handed out immediately after the exam shared this flaw (thereby revealing that one of us—DW—would have received strictly less than a 100 on this exam). The boxed proof above has been corrected to fix this flaw.

(b) There is a number $n \in \{0,1,\ldots,2010\}$ such that, for every $x \in \{1,2,\ldots,2010\}$, $f(x) \not\equiv n \pmod{2011}$. Find the number n. You do not need to prove your answer. Circle your final answer.

$\boxed{n = 1}$

Comment: Note that $f(x) \equiv 1 + x^{-1} \pmod{2011}$. The only number that cannot be expressed as the inverse of something (modulo 2011) is 0 (i.e., $x^{-1} \equiv 0 \pmod{2011}$ has no solution for x), so $f(x) \equiv 1 \pmod{2011}$ has no solution for x.

Problem 6. [Error-correcting codes] (12 points)

(a) Suppose that we know that at most one encoded packet will be lost during transmission, and that no packet will be corrupted. (In other words, every packet is either received correctly by the recipient, or is not received at all. Also, if any packet is lost, the recipient can tell which one was lost.)

Is it sufficient to send $n+1$ encoded packets? In other words, is there a way to encode the message $m_1, \ldots, m_n$ into the encoded packets $c_1, \ldots, c_{n+1}$ such that if any one encoded packet c_i is lost, the recipient can still uniquely recover the original message $m_1, \ldots, m_n$? Briefly, why or why not?

Yes. The scheme we saw in class achieves this.

(b) Now let's change the error model. Suppose that no packet will ever be lost, but at most one encoded packet might be corrupted during transmission. (In other words, at most one packet is received incorrectly by the recipient.) Suppose also that the recipient can somehow tell which packet (if any) was received incorrectly.

Is it sufficient to send $n+1$ encoded packets? In other words, is there a way to encode the message $m_1, \ldots, m_n$ into the encoded packets $c_1, \ldots, c_{n+1}$ such that if any one encoded packet c_i is corrupted and the recipient knows which one was corrupted, the recipient can still uniquely recover the original message $m_1, \ldots, m_n$? Briefly, why or why not?

Yes. Treat the corrupted packet as though it were lost, then see part (a).

(c) It is not very realistic to assume that the recipient can tell which packet was received incorrectly. So let's assume that, as in part (b), at most one packet might be received incorrectly, but now the recipient has no way to tell which packet (if any) was received incorrectly.

Professor Auburn claims that $n+2$ encoded packets suffice to ensure the recipient can always uniquely recover the original message, as long as at most one packet is received incorrectly (even though the recipient does not know which packet was corrupted). He suggests that the sender generate encoded packets using polynomials: namely, $c_i = P(i)$ for $i = 1, 2, \ldots, n+2$, where $P(x) = m_1 + m_2 x + \cdots + m_n x^{n-1}$. Then, when the recipient receives $n+2$ values $\hat{c}_1, \ldots, \hat{c}_{n+2}$, Professor Auburn suggests that the recipient use the following algorithm to recover the original message.

AuburnDecoder($\hat{c}_1, \ldots, \hat{c}_{n+2}$):
1. For each $j \in \{1, 2, \ldots, n+2\}$, do:
2. Use Lagrange interpolation to find the unique polynomial $Q_j(x)$ of degree $\leq n$ that passes through the following $n+1$ points:
   $\boxed{(1, \hat{c}_1), \ldots, (j-1, \hat{c}_{j-1}), (j+1, \hat{c}_{j+1}), \ldots, (n+2, \hat{c}_{n+2})}$.
3. If degree($Q_j(x)$) $\leq \boxed{n-1}$, then return the coefficients of $Q_j(x)$.

Comment: This is guaranteed to recover $P(x)$ uniquely. Here's why. Obviously, when we choose j to be the index of the corrupted packet, the check on line 3 succeeds (since then $Q_j(x) = P(x)$, and $P(x)$ has degree at most $n-1$), so the check will succeed for at least one value of j. Is it possible that the check

succeeds for some other index, say i? That would mean $\deg Q_i(x) \leq n-1$ and $\deg Q_j(x) \leq n-1$. But $Q_i(x)$ and $Q_j(x)$ agree on n points (namely, all the points in $1,2,\ldots,i-1,i+1,\ldots,j-1,j+1,\ldots,n+2$), and we can't have two different polynomials of degree at most $n-1$ that agree on n points (by the fact from class). So there is a single value of j for which the check will pass—the index of the corrupted packet.

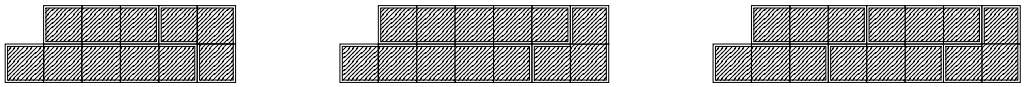
Common errors (added 10/13): Many students did not specify points for the first box, e.g., they answered $1,\ldots,j-1,j+1,\ldots n+2$ or $\hat{c}_1,\ldots,\hat{c}_{j-1},\hat{c}_{j+1},\ldots,\hat{c}_{n+2}$.

Problem 7. [Cory Hall renovation] (14 points)

Prove that, for all $n \geq 6$, it is possible to tile the hallway.

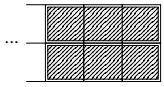
Proof by (strong) induction.

Base cases: For $n = 6$, $n = 7$, and $n = 8$, the hallway can be tiled like this:



Induction hypothesis: Suppose that the hallway can be tiled for lengths $6,7,8,\ldots,k$, for some $k \geq 8$.

Inductive step: Since $k \geq 8$, we know that $k-2 \geq 6$, so by the induction hypothesis, the hallway can be tiled for length $k-2$. It follows that the hallway can be tiled for length $k+1$ simply by adding two 1×3 pieces to the right side of the tiling for length $k-2$, like this:



Common errors (added 10/13): A number of students described the basic idea of the solution above, but didn't provide a formal induction proof (or claimed to have proved the statement, even though they were in fact implicitly relying upon induction). We gave significant partial credit for such an answer, but not full credit.

The most common mistake was to implicitly assume that if it is possible to find a collection of tiles whose total area is $2n-1$, then the hallway of length n can be tiled. This does not follow, because there is no guarantee that those pieces can be fit together into the necessary shape.

Some people tried to prove the statement by simple induction on n, i.e., proving $(\forall k)(P(k) \implies P(k+1))$, where $P(k)$ is the claim that a hallway of length k can be tiled. It is possible, but vastly harder, to make such a proof work. Most attempts failed at various points along the way. The correct proofs of this form involved strengthening the hypothesis, to claim not only that a tiling exists but to describe some of its properties.

Some people used strong induction to tile a hallway of length n by combining a tiling for a hallway of length k, a hallway of length ℓ, and an L-shaped piece, where k,ℓ were chosen so that $k+\ell = n-1$ and $k,\ell \geq 6$. This proof strategy can work, given sufficiently many base cases.

Comment: Want a fun (easy) puzzle? Prove that there exists a threshold $t \in \mathbb{N}$ such that the hallway can be tiled for all lengths $n \geq t$, using only the 1×3 and 1×5 tiles (i.e., without access to the L-shaped tile).

Want a harder puzzle? Try to prove that 3 and 5 aren't special: for every pair of lengths ℓ, m, there exists a threshold t such that it is possible to tile all hallways of length $n \geq t$ using only $1 \times \ell$ and $1 \times m$ tiles.

Hint on puzzle (added 10/13): I should have specified that $\gcd(\ell, m) = 1$. (Otherwise, there is no hope.)