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

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

(a) $(\forall x \in \mathbb{N})(\exists y \in \mathbb{N})(x = y)$.

(b) $(\forall x \in \mathbb{N})(\exists y \in \mathbb{N})(x^6 = y^2)$.

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

(d) For all $x, y \in \mathbb{N}$, if $9x \equiv y \pmod{26}$, then $x \equiv 3y \pmod{26}$.

(e) For all $x, y \in \mathbb{N}$, if $10x + 13 \equiv 14y + 7 \pmod{26}$, then $5x + 3 \equiv 7y \pmod{26}$.

(f) $\gcd(267, 368) = \gcd(101, 267)$.

(g) For all $x, y \in \mathbb{N}$, $\gcd(2x, 2y) = 2\gcd(x, y)$.

(h) For all $x, y \in \mathbb{N}$, $\gcd(2x, 3y) = \gcd(x, y)$.

Problem 2. [Propositional logic] (12 points)

(a) $P \implies Q$:

P	Q	$P \implies Q$
false	false	
false	true	
true	false	
true	true	

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

P	Q	$(P \wedge Q) \implies (P \wedge Q)$
false	false	
false	true	
true	false	
true	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	true	
true	false	
true	true	

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

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

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:

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

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?

(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?

(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?

(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)?

(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)?

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.)

(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.

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?

(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?

(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:
   [ ].
3. If degree($Q_j(x)$) $\leq$ [ ], then return the coefficients of $Q_j(x)$.

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

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