CS 70 Discrete Mathematics for CS
Fall 2003 Wagner

MT1 Solutions

PRINT your name: ______________________________, ______________________________
(last) (first)

SIGN your name: ____

PRINT your username on `cory.eecs`: ____

WRITE your section number (101 or 102): ___________________________

This exam is open-book, open-notes. No calculators are permitted. Do all your work on the pages of this examination. If you need more space, you may use the reverse side of the page, but try to use the reverse of the same page where the problem is stated.

You have 80 minutes. There are 4 questions, worth 25 points each (100 points total). The questions are of varying difficulty, so avoid spending too long on any one question.

Do not turn this page until the instructor tells you to do so.

Problem 1	
Problem 2	
Problem 3	
Problem 4	
Total	

Problem 1. [True or false] (25 points)

Circle TRUE or FALSE. You do not need to justify your answers on this problem.

$\mathbf{N}$ denotes the set of natural numbers, $\{0,1,2,\ldots\}$. $\mathbf{Z}$ denotes the integers, $\{\ldots,-2,-1,0,1,2,\ldots\}$.

(a) TRUE or $\boxed{\textbf{False}}$: If the implication $P \implies Q$ is true, then its converse is guaranteed to be true, too.

(b) $\boxed{\textbf{True}}$ or FALSE: $\forall w \in \mathbf{Z}.\ \exists x \in \mathbf{Z}.\ \forall y \in \mathbf{Z}.\ \exists z \in \mathbf{Z}.\ w+x=y+z$.

(c) $\boxed{\textbf{True}}$ or FALSE: $\exists x \in \mathbf{N}.\ \forall p \in \mathbf{Z}.\ p>5 \implies x^2 \equiv 1 \pmod{p}$.

(d) $\boxed{\textbf{True}}$ or FALSE: $\forall p \in \mathbf{Z}.\ p>5 \implies \exists x \in \mathbf{N}.\ x^2 \equiv 1 \pmod{p}$.

(e) $\boxed{\textbf{True}}$ or FALSE: If m is any natural number satisfying $m \equiv 1 \pmod{2}$, then the equation $2048x \equiv 1 \pmod{m}$ is guaranteed to have a solution for x.

Problem 2. [Proof by Induction] (25 points)

Prove by induction that

$$\sum_{i=1}^{n} \frac{i(i-1)}{2} = \frac{(n+1)n(n-1)}{6}$$

holds for all $n \in \mathbf{N}$.

Let $P(n) =$ "$\sum_{i=1}^{n} \frac{i(i-1)}{2} = \frac{(n+1)n(n-1)}{6}$". Then we prove by simple induction that $\forall n \in \mathbf{N}.\ P(n)$.

- Base case: $n = 0$.
  Then $\sum_{i=1}^{0} \frac{i(i-1)}{2} = 0 = \frac{(0+1)0(0-1)}{6}$, so $P(0)$.
- Inductive step: $P(n) \implies P(n+1)$.
  Then

$$\begin{aligned}
\sum_{i=1}^{n+1} \frac{i(i-1)}{2} &= \sum_{i=1}^{n} \frac{i(i-1)}{2} + \frac{n(n+1)}{2} && \text{(by definition of summation)} \\
&= \frac{(n+1)n(n-1)}{6} + \frac{n(n+1)}{2} && \text{(by inductive hypothesis)} \\
&= \frac{(n+1)n(n-1) + 3n(n+1)}{6} && \text{(combining terms)} \\
&= \frac{(n-1+3)(n+1)n}{6} && \text{(factoring)} \\
&= \frac{(n+2)(n+1)n}{6}. && \text{(completing the inductive step)}
\end{aligned}$$

Thus, by the principle of induction, $\forall n \in \mathbf{N}.\ P(n)$.

Problem 3. [Proofs] (25 points)

Definition: A 2-party cake-cutting protocol is called *equalizing* if it satisfies the following property: If a denotes the worth (by Alice's measure) of the piece Alice receives, and b denotes the worth (by Bob's measure) of the piece Bob receives, then $a = b$.

(a) TRUE or $\boxed{\textbf{False}}$: Every envy-free 2-party cake-cutting protocol is equalizing.

(b) Prove your answer to part (a).

Proof by counterexample. Consider the two-party cut-and-choose algorithm. Recall that this algorithm is envy-free. Suppose Alice cuts and Bob chooses. Alice values each of the two pieces exactly $\frac{1}{2}$. Now suppose Bob values one piece $\frac{3}{4}$ and the other $\frac{1}{4}$. The he will choose the former piece. But he receives $\frac{3}{4}$ by his measure, and Alice receives only $\frac{1}{2}$ by her measure, so cut-and-choose is not equalizing.

(c) Prove the following: If x is positive and irrational, then $\sqrt{x}$ is irrational, too.

We prove the contrapositive, that if $\sqrt{x}$ is rational, then x is also rational.
Consider an arbitrary rational $\sqrt{x}$. Then by definition of rational, $\sqrt{x} = \frac{a}{b}$ for some integers a and b. Now consider $x = \sqrt{x}^2 = \frac{a^2}{b^2}$. Since the integers are closed under multiplication, a^2 and b^2 are also integers. Thus x is rational, since it can be expressed as the quotient of two integers a^2 and b^2.

Problem 4. [Strings] (25 points)

Let $\{0,1\}^*$ denote the set of all binary strings. Write $y \cdot z$ for the concatenation of the strings y and z.

Prove that every string $x \in \{0,1\}^*$ can be written in the form $x = y \cdot z$ where the number of 0's in y is the same as the number of 1's in z. Empty strings are allowed.

(For instance, 01001 can be split as $01 \cdot 001$; $111011 = 11101 \cdot 1$; and $00000 = \cdot 00000$.)

Hint: It is possible to prove this using strong induction over $\mathbf{N}$.

We provide two solutions to this problem, one using simple induction and one using strong induction, both over the length of a string. Let $P(n) =$ "any string x of length n can be expressed as $x = y \cdot z$ as above."

1. Proof by simple induction.

   - Base case: $n = 0$.
     The only length 0 string is λ, the empty string, which can be expressed as $\lambda = \lambda \cdot \lambda$, satisfying $P(0)$.
   - Inductive step: $P(n) \implies P(n+1)$.
     Consider an arbitrary length $n+1$ string $x = x_1 x_2 \cdots x_{n+1}$. Then by the inductive hypothesis, the string $x' = x_1 x_2 \cdots x_n$ can be split as $x' = y'z'$ as required, where $y' = x_1 \cdots x_i$ and $z' = x_{i+1} \cdots x_n$ for some i. Let k be the number of 0's in y (and the number of 1's in z). Now there are two cases.

     (a) Case 1: $x_{n+1} = 0$.
     Then the split $x = y \cdot z$ where $y = y'$ and $z = z'x_{n+1}$ works, since y and z still have k 0's and 1's, respectively.

     (b) Case 2: $x_{n+1} = 1$.
     Again, there are two cases.

       i. Case 2a: $x_{i+1} = 0$.
       Then the split $x = y \cdot z$ where $y = x_1 \cdots x_{i+1}$ and $z = x_{i+2} \cdots x_{n+1}$ works, since y has $k+1$ 0's and z has $k+1$ 1's.

       ii. Case 2b: $x_{i+1} = 1$.
       Then the split $x = y \cdot z$ where $y = x_1 \cdots x_{i+1}$ and $z = x_{i+2} \cdots x_{n+1}$ works, since y has k 0's and z has k 1's (it loses one to y and gains one from x_{n+1}).

     In all cases, a valid split exists.

2. Proof by strong induction.

   - Base case: $n = 0$.
     The only length 0 string is λ, the empty string, which can be expressed as $\lambda = \lambda \cdot \lambda$, satisfying $P(0)$.
   - Inductive step: $P(0) \wedge \cdots \wedge P(n) \implies P(n+1)$.
     Consider an arbitrary length $n+1$ string $x = x_1 x_2 \cdots x_{n+1}$. There are three cases.

     (a) Case 1: $x_{n+1} = 0$.
     By the inductive hypothesis, the string $x' = x_1 \cdots x_n$ can be split into $x' = y'z'$ as required. Then the split $x = y \cdot z$ where $y = y'$ and $z = z'x_{n+1}$ works, since y has the same number of 0's as y' and z has the same number of 1's as z'.

(b) Case 2: $x_1 = 1$.
By the inductive hypothesis, the string $x' = x_2 \cdots x_{n+1}$ can be split into $x' = y'z'$ as required. Then the split $x = y \cdot z$ where $y = x_1 y'$ and $z = z'$ works, since y has the same number of 0's as y' and z has the same number of 1's as z'.

(c) Case 3: $x_1 = 0 \wedge x_{n+1} = 1$.
By the inductive hypothesis, the string $x' = x_2 \cdots x_n$ can be split into $x' = y'z'$ as required. Then the split $x = y \cdot z$ where $y = x_1 y'$ and $z = z' x_{n+1}$ works, since y has one more 0 than y' and z has one more 1 than z'.

In all cases, a valid split exists.