Massachusetts Institute of Technology
6.042J/18.062J: Mathematics for Computer Science
Professors David Karger and Nancy Lynch

Handout 4
February 4, 2000

Mini-Quiz 1

1. Write your name:

2. (Rosen 1.2.13). Determine whether $(\neg q \wedge (p \implies q)) \implies \neg p)$ is a tautology.

3. Determine the truth value of the following propositions, where the universe of discourse is the natural numbers.

   (a) $\forall n \exists m (n^2 < m)$

   (b) $\exists m \forall n (n^2 < m)$

   (c) $\exists n \exists m (n^2 + m^2 = 5)$

   (d) $\forall n, m \exists p (p = (m + n)/2)$

Tutorial 1 Problems

Problem 1. Identify *precisely* what the bugs are in each of the following false proofs.

(a)

$$\begin{gathered} 3 > 2 \\ 3\log_{10}(1/2) > 2\log_{10}(1/2) \\ \log_{10}(1/2)^3 > \log_{10}(1/2)^2 \\ (1/2)^3 > (1/2)^2 \\ \text{Therefore, } 1/8 > 1/4! \end{gathered}$$

Solution:
$\log x < 0$, for $0 < x < 1$, so since both sides of the inequality "$3 > 2$" are being multiplied by the negative quantity $\log_{10}(1/2)$, the inequality in the second line should have been the reverse of the first line, that is, $<$ instead of $>$.

(b) You are richer than you think:

$$1\cent = \$0.01 = (\$0.1)^2 = (10\cent)^2 = \$1.$$

Solution:
$\$0.01 = \$(0.1)^2 \neq (\$0.1)^2$ because the units $\$^2$ and $\$$ don't match (just as in physics the difference between sec^2 and sec indicates the difference between acceleration and velocity).

(c) Consider the following scheme to make millions. Obtain a slab of gold $10'' \times 11'' \times 1''$. Then cut out two little one-inch triangles at the corners. These triangles are the profit. Finally, slide the two slabs together again and note that the rectangle is now $11'' \times 10'' \times 1''$—the same size as it was before we removed the small triangles. By repeating the process, we can produce an unlimited supply of gold!

Solution:
The picture makes the little triangles look like right triangles, but they aren't. So when the two large pieces left after the little triangles are removed are slid together, they do not form a rectangle, which means the resulting shape is not the same as the original figure. (This illustrates why "proof by diagram" is mathematically suspicious.)

(d) Claim: Every polynomial $p(x) = ax^2 + bx + c$ over $\mathbb{C}$ (the complex numbers) has two roots.

Sounds good, but the claim is false. Find the counterexamples and then restate the claim so it is correct.

Proof. Using the usual formulas for the roots of a quadratic, let

$$\begin{aligned} r_1 &::= \frac{-b+\sqrt{D}}{2a}, \text{ and} \\ r_2 &::= \frac{-b-\sqrt{D}}{2a}, \text{ where} \\ D &::= b^2 - 4ac. \end{aligned}$$

To verify that r_1 is a root, note that

$$\begin{aligned} a{r_1}^2 &= a(\frac{-b+\sqrt{d}}{2a})^2 \\ &= a\frac{b^2 - 2b\sqrt{D} + D}{4a^2} \\ &= \frac{b^2 - 2b\sqrt{D} + b^2 - 4ac}{4a} \\ &= \frac{2b^2 - 2b\sqrt{D} - 4ac}{4a} \\ &= \frac{b^2 - b\sqrt{D} - 2ac}{2a} \end{aligned}$$

and

$$\begin{aligned} br_1 &= b\frac{-b+\sqrt{D}}{2a} \\ &= \frac{-b^2 + b\sqrt{D}}{2a} \end{aligned}$$

so

$$\begin{aligned} p(r_1) &= {r_1}^2 + br_1 + c \\ &= \frac{b^2 - b\sqrt{d} - 2ac}{2a} + \frac{-b^2 + b\sqrt{d}}{2a} + c \\ &= \frac{-2ac}{2a} + c = -c + c = 0, \end{aligned}$$

as claimed. A similar calculation confirms that $p(r_2) = 0$. ∎

Solution:

The polynomial $0x^2 + 0x + 1$ has no roots. The proof failed for this case since it divides by a, which is unsound when $a = 0$.

The polynomial $x^2 + 2x + 1$ has only one root. For $a \neq 0$, the algebra is ok, but the proof assumes that $r_1 \neq r_2$, which will be false when $D = 0$.

The proof is correct for polynomials with $a \neq 0 \neq D$ (even though when $D < 0$, the meaning of $\sqrt{D}$ is ambiguous as we saw in lecture). So these two conditions are required to make the claim correct.

Problem 2. A *group* is a set G together with a binary operation $\cdot : G \times G \to G$ that satisfies the following axioms.

Identify at least two "normal" sets and operations on them that satisfy the group axioms.

1. $\forall a, b, c \in G, (a \cdot b) \cdot c = a \cdot (b \cdot c)$.
2. $\exists e \in G$ (called the *identity*) such that $\forall a \in G, a \cdot e = e \cdot a = a$.
3. $\forall a \in G, \exists a^{-1} \in G$ (called the *inverse* of a), such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

So addition defines a group on the integers, and multiplication a group on the positive rationals.

Using the three group axioms prove the following propositions.

(a) Show, by contradiction, that the identity element is unique.

Solution:
Proof by Contradiction. Suppose there are two identities e and f. Then $ef = e$ since f is an identity, but $ef = f$ since e is an identity. Thus $e = f$, a contradiction.

(b) Show that for every $a \in G$, the inverse of a is unique. We can therefore write the inverse element as a^{-1} with no fear of ambiguity.

Solution:
Proof by Contradiction. Suppose there are two inverses b and c. Then $ab = e$, which implies that $c(ab) = ce = c$. But also $c(ab) = (ca)b = eb = b$ since c is an inverse. So $b = c$, a contradiction.

(c) Show $\forall a \in G, (a^{-1})^{-1} = a$

Solution:
Direct Proof. Write $b = a^{-1}$. By definition of a^{-1}, we have $ba = ab = e$. Therefore, a satisfies the "inverse" definition for b—that is, $a = b^{-1} = (a^{-1})^{-1}$.

(d) Show $\forall a, b \in G, (a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$

Solution:
We have

$$(b^{-1}a^{-1})(ab) = (b^{-1})(a^{-1}a)b = b^{-1}eb = b^{-1}b = e.$$

Therefore $(b^{-1}a^{-1})$ satisfies the inverse definition for ab.

Problem 3. Use induction on n to prove that the following inequality holds for all integers $n \geq 1$ and for all non-negative real numbers $x_1, \ldots, x_n$.

$$(x_1 + x_2 + \ldots + x_n)^2 \quad \geq \quad x_1^2 + x_2^2 + \ldots + x_n^2$$

Problem 4. *Handshakes.* I recently went to a party with my spouse; there were 11 other married couples there. A lot of handshaking happened (but of course no one shook hands with their spouse). At the end, it turned out that for every k from 0 to 22, someone other than me had shaken hands with exactly k people. How many people did I shake hands with? Prove your answer.

Note that there are 24 people (12 couples) in this case.

Solution:
We will prove the following for a set of n couples:

Theorem 0.1. *Suppose at a party for n couples (total) it turns out that someone other than me has shaken k hands for every k from 0 to $2n-2$. Then I must have shaken $n-1$ hands.*

Proof. By induction on n.

I.H. $P(n)$: At an n couple party, if someone other than me shakes k hands for every k from 0 to $2n-2$ then I must have shaken $n-1$ hands.

Base: $n = 1$. There are no other couples. My wife has shaken 0 hands (can't shake with me). I have shaken 0 hands ($= n-1$). (some party!)

I.H. Assume $P(n-1)$ is true. To prove $P(n)$, consider a party with n couples.

Someone has shaken $2n-2$ hands, i.e., with everyone in the room except themselves and their spouse. Therefore everyone else but this couple has shaken hands at least once. So the one who hasn't shaken hands at all must be this person's spouse. $2n-2$ is paired with 0. Consider the subparty of the remaining $n-1$ couples. I must be in this group since there cannot be two people who shook hands $2n-2$ times or 0 times. Consider the number of times this group of people has shaken hands among themselves, i.e., not counting handshakes with the $2n-2, 0$ couple. Then the number of handshakes I see is every number between 0 and $2n-4$. This is because this group of people has original handshake counts of $1, 2, 3, \ldots, 2n-3$. Since everyone shakes the $2n-2$ person's hand once, we are left with handshake counts of $0, 1, \ldots, 2n-4$. This is exactly the premise of $P(n-1)$. So by the I.H. I must have shaken $n-2$ hands within this group. Adding the one handshake with the $2n-2, 0$ couple, I must have shaken a total of $n-1$ hands. ∎

For $n = 12$, the answer is that I shook 11 hands.