CS103 Handout 05S
Fall 2013 October 7, 2013

Problem Set 1 Solutions

Problem One: Set Theory Warmup (4 points)

Consider the following sets:

$W = \{ 1, 2, 3, 4 \}$

$X = \{ 2, 2, 2, 1, 4, 3 \}$

$Y = \{ 1, \{2\}, \{\{3, 4\}\} \}$

$Z = \{ 1, 3 \}$

i. Which pairs of the above sets, if any, are equal to one another?

W and X are equal to one another, and no other sets are. These sets are equal because they contain precisely the same *elements*. Remember that sets do not care about repetition or ordering.

Note that W and Y are not the same set, because $\{2\} \in Y$, but $\{2\} \notin W$.

ii. Is $Z \in W$? Is $Z \subseteq W$?

$Z \notin W$ because W does not contain an element equal to the set $\{1, 3\}$. However, $Z \subseteq W$, because every element of Z is also in W.

iii. Is $Z \in \wp(W)$? Is $Z \subseteq \wp(W)$?

Since $Z \subseteq W$, it is true that $Z \in \wp(W)$. However, Z is not a subset of $\wp(W)$. Since 1 isn't a set, 1 isn't a subset of W, so $1 \notin \wp(W)$. Thus Z is not a subset of $\wp(W)$ because $1 \in Z$ but $1 \notin \wp(W)$.

iv. What is $W \cap Y$? How about $W \cup Y$? How about $W \Delta Y$?

$W \cap Y = \{ 1 \}$, since 1 is their only common element. $W \cup Y = \{1, 2, 3, 4, \{2\}, \{\{3, 4\}\}\}$, the set of all elements in at least one of W and Y. $W \Delta Y = \{2, 3, 4, \{2\}, \{\{3, 4\}\}\}$.

v. What is $|X|$?

$|X| = 4$, since there are four distinct elements in X.

Why did we ask this question? We introduced a lot of notation in the first lecture (inclusion, subset, power set, cardinality, and set operators) and wanted to make sure everyone was comfortable with them before moving on. Typically, we don't ask questions that just test whether you understand the notation, but in this case we felt it would be good to "stress-test" it in isolation to make sure that everyone had a firmer grasp of set theory before jumping into the next problem.

Problem Two: Properties of Sets (28 points)

i. If $A \in B$ and $B \in C$, then $A \in C$.

This statement is neither always true nor always false. Take $A = \emptyset$, $B = \{\emptyset\}$, and $C = \{\emptyset, \{\emptyset\}\}$. In this case, $A \in B$ and $B \in C$, and it's also true that $A \in C$. However, if you consider the sets $A = \emptyset$, $B = \{\emptyset\}$, and $C = \{\{\emptyset\}\}$, then $A \in B$ and $B \in C$, but $A \notin C$. Remember – the element-of relation $\in$ and the subset-of relation $\subseteq$ aren't the same!

ii. If $\wp(A) = \wp(B)$, then $A = B$.

This statement is always true.

***Theorem**:* If $\wp(A) = \wp(B)$, then $A = B$.

Proof: Let A and B be arbitrary sets with $\wp(A) = \wp(B)$. Since every set is a subset of itself, this means $A \subseteq A$ and $B \subseteq B$, so we have $A \in \wp(A)$ and $B \in \wp(B)$. Because $\wp(A) = \wp(B)$ and $A \in \wp(A)$, we know $A \in \wp(B)$ and so $A \subseteq B$. Similarly, since $B \in \wp(B)$ and $\wp(B) = \wp(A)$, we have $B \in \wp(A)$ and so $B \subseteq A$. Since $A \subseteq B$ and $B \subseteq A$, we have that $A = B$. ■

Another way to prove this is by contrapositive:

***Proof**:* By contrapositive; we show that if $A \neq B$, then $\wp(A) \neq \wp(B)$. If $A \neq B$, then there must be an element x such that either $x \in A$ and $x \notin B$ or $x \notin A$ and $x \in B$. Without loss of generality, assume it's the former case. In that case, since $x \in A$, we know $\{x\} \subseteq A$, and since $x \notin B$, we know that $\{x\}$ is not a subset of B. Thus $\{x\} \in \wp(A)$ and $\{x\} \notin \wp(B)$. Consequently, $\wp(A) \neq \wp(B)$. ■

iii. $(A - B) \cup B = A$.

This statement is neither always true nor always false. If we take $A = \mathbb{N}$ and $B = \emptyset$; then we see $(A - B) \cup B = (\mathbb{N} - \emptyset) \cup \emptyset = \mathbb{N} \cup \emptyset = \mathbb{N} = A$. However, if we instead let $A = \emptyset$ and $B = \mathbb{N}$, then $(A - B) \cup B = (\emptyset - \mathbb{N}) \cup \mathbb{N} = \emptyset \cup \mathbb{N} = \mathbb{N} \neq \emptyset = A$.

Can you find a criterion by which you can determine when this statement will be true?

iv. $A \cap (B - A) \neq \emptyset$.

This statement is always false.

***Theorem**:* $A \cap (B - A) = \emptyset$.

***Proof**:* We need to show that for any x, that $x \notin A \cap (B - A)$. To do this, we proceed by contradiction; assume that there exists an x such that $x \in A \cap (B - A)$. This means that $x \in A$ and $x \in B - A$. Since $x \in B - A$, we have $x \in B$ and $x \notin A$. This means $x \in A$ and $x \notin A$, which is impossible. We have reached a contradiction, so our initial assumption must have been wrong. Thus for any x, we know $x \notin A \cap (B - A)$. Therefore, $A \cap (B - A) = \emptyset$. ■

Why did we ask this question? There are two main reasons we asked this problem. First, we hoped that this would give you experience writing proofs that call back to underlying definitions. Second, this problem contains two statements that might seem "obviously" true but actually depend on the underlying sets. By leaving it up to you to determine the truth of each statement, we hoped to help you build a better mathematical intuition.

Problem Three: Venn Diagrams (4 Points)

In the second Venn diagram, there is no region that represents the intersection of just A and D or of just B and C. This means that the sets $A = \{1\}$, $B = \{2\}$, $C = \{2\}$, $D = \{1\}$ cannot be represented in the second Venn diagram. For a challenge, try showing that no matter how you draw four circles, you can *never* get a valid Venn diagram!

Why did we ask this question? Venn diagrams are often taught in elementary school for two sets or three sets, but rarely does anyone explore four sets. The actual Venn diagram for four sets is by no means obvious, and the natural generalization of Venn diagrams for two and three sets turns out not to work. We hoped that this question would help you see why this is the case.

Problem Four: Two Is Irrational? (12 points)

The problem with this proof is that it incorrectly claims that if n^2 is a multiple of four, then n is a multiple of four as well. This reasoning is used twice – once to claim that since p^2 is a multiple of four, p is a multiple of four, and once to claim that since q^2 is a multiple of four, q is a multiple of four. But this claim is false – for example, $36 = 6^2$ is a multiple of four, but 6 is not a multiple of four. In fact, this is how the proof breaks down. Rather than being able to claim that since p^2 is a multiple of four, p is a multiple of four, we can only claim that since p^2 is a multiple of four, p must be even (since p^2 is even).

If we substitute this logic in and propagate it, we'd end up getting that $p = 2k$ for some integer k. This would mean that, since $p^2 = 4q^2$, then we have that $4q^2 = (2k)^2 = 4k^2$, so $q^2 = k^2$. In other words, $|q| = |k|$. Since $p = 2k$, this means that $p / q = 2$ or $p / q = -2$. We fail to find a contradiction because we instead explicitly find a p and q that work!

Why did we ask this question? The proof that the square root of two is irrational was our first nontrivial proof. It used a proof by contradiction, leveraged a complex definition, and relied on an intermediary result we proved in multiple pieces. We asked this question to get you to review the proof in detail to see exactly why it worked and what assumptions it made. As you probably saw in this problem, the proof is a lot more subtle than it might initially seem!

We also asked this problem so that you could better appreciate the complexities involved in writing a good mathematical proof. Everything in the proof seems perfectly reasonable at first glance, and only by carefully working through it can you discover where the logic breaks down. Going forward, we encourage you to look over proofs you don't understand in more detail and try to see how they work. Some of the results we'll be proving are by no means obvious, but by playing around with the proofs and asking why the same reasoning would or would not work in other areas you'll gain a much deeper understanding of their inner workings.

Problem Five: Pythagorean Triples (12 points)

Theorem: If (a, b, c) is a Pythagorean triple, then $(a + 1, b + 1, c + 1)$ is not a Pythagorean triple.

Proof: By contradiction; assume there are positive natural numbers a, b, and c such that (a, b, c) is a Pythagorean triple and $(a + 1, b + 1, c + 1)$ is a Pythagorean triple. Then $a^2 + b^2 = c^2$ and $(a + 1)^2 + (b + 1)^2 = (c + 1)^2$. Expanding out this second equality, we get

$$a^2 + 2a + 1 + b^2 + 2b + 1 = c^2 + 2c + 1$$

Rearranging, we get

$$a^2 + b^2 - c^2 + 1 = 2c - 2a - 2b = 2(c - a - b)$$

Since $a^2 + b^2 = c^2$, we have $a^2 + b^2 - c^2 = 0$. Combined with the above, we have that

$$1 = 2(c - a - b)$$

But this is impossible, since 1 is odd and $2(c - a - b)$ is even. We have reached a contradiction and therefore our assumption was wrong, so if (a, b, c) is a Pythagorean triple, then $(a + 1, b + 1, c + 1)$ is not. ■

Why did we ask this question? We asked this question for several reasons. First, this is a proof by contradiction of a statement involving an implication: *if* (a, b, c) is a Pythagorean triple, *then* $(a + 1, b + 1, c + 1)$ is not. One of the things we look for when grading this problem is whether you correctly took the negation of this statement and assumed that (a, b, c) is a Pythagorean triple *and* $(a + 1, b + 1, c + 1)$ is a Pythagorean triple.

Second, many proofs of complicated facts rely on simple observations. In this case, our solution works using the fact that no number is both odd and even. You might have proven this result by taking the expression

$$1 = 2(c - a - b)$$

and dividing both sides by two to get

$$\tfrac{1}{2} = c - a - b$$

and from there getting a contradiction because a, b, and c are integers and ½ is not. We hoped that you would recognize the contradiction of a simple mathematical fact when you saw it and could use it to conclude that the premise, which had nothing to do with odd and even numbers or with integers and rational numbers, would imply an inconsistency with them.

Problem Six: Modular Arithmetic (24 points)

i. Prove that for any integer x and any integer k, $x \equiv_k x$.

Proof: Let x and k be arbitrary integers. Then $x - x = 0 = 0 \cdot k$. Thus there exists a q, namely 0, such that $x - x = qk$, so $x \equiv_k x$. ■

ii. Prove that for any integers x and y and any integer k, that if $x \equiv_k y$, then $y \equiv_k x$.

Proof: Let x, y, and k be arbitrary integers such that $x \equiv_k y$. Since $x \equiv_k y$, there exists a q such that $x - y = kq$. Consequently, $y - x = -kq = (-q)k$. Thus there exists an integer r, namely, $-q$, such that $y - x = kr$, so $y \equiv_k x$. ■

iii. Prove that for any integers x, y, and z and any integer k, that if $x \equiv_k y$ and $y \equiv_k z$, then $x \equiv_k z$.

Proof: Let x, y, z, and k be arbitrary integers such that $x \equiv_k y$ and $y \equiv_k z$. This means that there exists integers q_0, q_1 such that $x - y = kq_0$ and $y - z = kq_1$. Thus $x - z = x - y + y - z = kq_0 + kq_1 = k(q_0 + q_1)$. This means that there exists an integer q (namely, $q_0 + q_1$) such that $x - z = kq$, so $x \equiv_k z$. ■

iv. Prove that for any integers w, x, y, z, and k, that if $x \equiv_k w$ and $y \equiv_k z$, then $x + y \equiv_k w + z$.

Proof: Let x, y, z, w, and k be arbitrary integers such that $x \equiv_k w$ and $y \equiv_k z$. This means that there exists integers q_0, q_1 such that $x - w = kq_0$ and $y - z = kq_1$. Thus $(x + y) - (w + z) = x + y - w - z = (x - w) + (y - z) = kq_0 + kq_1 = k(q_0 + q_1)$. Thus there exists a q, namely $q_0 + q_1$, such that $(x + y) - (w + z) = kq$, so $x + y \equiv_k w + z$. ■

v. Prove that for any integers w, x, y, z, and k, that if $x \equiv_k w$ and $y \equiv_k z$, then $xy \equiv_k wz$.

Proof: Let x, y, z, w, and k be arbitrary integers such that $x \equiv_k w$ and $y \equiv_k z$. This means that there exists integers q_0, q_1 such that $x - w = kq_0$ and $y - z = kq_1$. This means that $x = kq_0 + w$ and $y = kq_1 + z$. Therefore, $xy - wz = (kq_0 + w)(kq_1 + z) - wz = k^2q_0q_1 + wkq_1 + zkq_0 + wz - wz = k^2q_0q_1 + wkq_1 + zkq_0 = k(kq_0q_1 + wq_1 + zq_0)$. Thus there is an integer q, namely $kq_0q_1 + wq_1 + zq_0$, such that $xy - wz = kq$, so $xy \equiv_k wz$. ■

Why did we ask this question? This question is tricky because it involves so many existential statements. Proving these results are true requires you to assume that many unknown quantities with various properties must exist and reasoning about them to show that *other* unknown quantities with various properties must exist as well. Additionally, this problem involves a lot of calculation, but in the context of a mathematical proof. We hoped that this would help you explore how to write proofs that at their core are mathematical arguments, but which require external structure.

We also asked this question because the $\equiv_k$ relation will come up a few more times in the course. It's a great example of an *equivalence relation*, which we'll study this week.

Problem Seven: Subverting XOR Encryption (16 Points)

One possible procedure is the following: given the intercepted $M \oplus K$ and the values of M_1 and M_2, compute $(M \oplus K) \oplus (M_1 \oplus M_2)$. We claim that this leaves $M' \oplus K$, where M' is the message other than the one Alice sent.

Proof: We consider two cases.

Case 1: $M = M_1$. Then $(M \oplus K) \oplus (M_1 \oplus M_2) = (M_1 \oplus K) \oplus (M_1 \oplus M_2)$. Since $\oplus$ is associative and commutative, $(M_1 \oplus K) \oplus (M_1 \oplus M_2) = (M_1 \oplus M_1) \oplus (M_2 \oplus K)$. Since $\oplus$ is self-inverting and has 0 as an identity, we in turn have $(M_1 \oplus M_1) \oplus (M_2 \oplus K) = M_2 \oplus K$. Therefore, this procedure ends with $M_2 \oplus K$.

Case 1: $M = M_2$. Then $(M \oplus K) \oplus (M_1 \oplus M_2) = (M_2 \oplus K) \oplus (M_1 \oplus M_2)$. Since $\oplus$ is associative and commutative, $(M_2 \oplus K) \oplus (M_1 \oplus M_2) = (M_2 \oplus M_2) \oplus (M_1 \oplus K)$. Since $\oplus$ is self-inverting and has 0 as an identity, we in turn have $(M_2 \oplus M_2) \oplus (M_1 \oplus K) = M_1 \oplus K$. Therefore, this procedure ends with $M_1 \oplus K$.

Thus in both cases, the procedure ends with $M' \oplus K$, where M' is the message Alice didn't send. ■

Cryptography is hard! It's extremely difficult to implement a cryptographic system correctly – you need to make sure the keys stay secret, the keys are random, the keys never get reused, the system is secured against attacks like the one above, etc. A good general piece of advice is that ***you should never try to implement your own cryptography***. For more information on how to do cryptography properly, consider taking CS255 or CS155.

Why did we ask this question? This question shows how you can use the four major properties of the XOR operator (commutativity, associativity, identity elements, and self-invertibility) in order to attack a seemingly secure cryptographic system. Additionally, it requires some creativity to solve and is a great example of a proof by cases.

Problem Eight: Tiling a Chessboard (20 Points)

i. Prove that it is impossible to tile an 8×8 chessboard missing two opposite corners with right triominoes.

Proof: An 8×8 chessboard missing two opposite corners has 62 squares. If we were to tile it with right triominoes, the total number of squares covered would have to be a multiple of three. Since 62 is not a multiple of three, it is therefore impossible to tile it with right triominoes. ■

ii. For $n \geq 3$, is it *ever* possible to tile an $n \times n$ chessboard missing two opposite corners with right triominoes? If so, find a number $n \geq 3$ such that it's possible show how to tile such a chessboard with right triominoes. If not, prove that for every $n \geq 3$, it's impossible to tile an $n \times n$ chessboard missing two opposite corners with right triominoes.

***Theorem**:* For all $n \geq 3$, it is impossible to tile an $n \times n$ chessboard missing two opposite corners with right triominoes.

***Proof**:* For any $n \geq 3$, there are $n^2 - 2$ squares in an $n \times n$ chessboard missing two opposite corners. As in part (i), we can only tile a surface with right triominoes if the total number of squares is a multiple of three. We will therefore prove that $n^2 - 2$ is never a multiple of three to conclude that we can never tile an $n \times n$ chessboard missing two opposite corners using right triominoes. To do so, we consider three cases for n:

Case 1: n is a multiple of three. Then $n = 3k$ for some integer k. Therefore, we have that $n^2 - 2 = 9k^2 - 2 = 3(3k^2 - 1) + 1$, so $n^2 - 2$ is congruent to one modulo three and therefore not a multiple of three.

Case 2: n is congruent to one modulo three. Then $n = 3k + 1$ for some integer k. Therefore, we have $n^2 - 2 = (3k + 1)^2 - 2 = 9k^2 + 6k - 1 = 3(3k^2 + 2k - 1) + 2$, so $n^2 - 2$ is congruent to two modulo three and therefore not a multiple of three.

Case 3: n is congruent to two modulo three. Then $n = 3k + 2$ for some integer k. Therefore, we have $n^2 - 2 = (3k + 2)^2 - 2 = 9k^2 + 12k - 1 = (3k^2 + 4k - 1) + 2$, so $n^2 - 2$ is congruent to two modulo three and therefore not a multiple of three.

Thus in all cases, $n^2 - 2$ is not a multiple of three, from which the theorem follows. ■

Why did we ask this question? This question asks you to prove that a certain task is impossible. The proof we have above (which is the line of reasoning we hoped you would follow) works by abstracting away from the particulars of the problem (2D grids, L-shaped tiles) to a broader context (properties of numbers modulo three). Moreover, this proof builds off of the result from the checkpoint problem and helps provide some context about why that line of reasoning is worth pursuing at all.

Extra Credit Problem: Symmetric Latin Squares

We tend not to put the solutions to extra credit problems in the solution sets. However, if you have any questions about this problem, please feel free to stop by office hours and ask!