# Problem Set 3: Proof Techniques

**CS 198-087: Introduction to Mathematical Thinking**
UC Berkeley EECS
Fall 2018

This homework is due on Monday, September 24th, at 6:30PM, on Gradescope. As usual, this homework is graded on participation, but it is in your best interest to put full effort into it. This is a good opportunity to learn how to use LaTeX.

---

1. Prove that if $x^2 - 6x + 5$ is odd, then $x$ is even, using:

   a. Proof by Contraposition

   b. Direct Proof

**Solution:**

a. The contrapositive of this statement is, "if $x$ is odd, then $x^2 - 6x + 5$" is even. If $x$ is odd, we can write $x = 2k + 1$ for $k \in \mathbb{Z}$. Then:

$$\begin{aligned} x^2 - 6x + 5 &= (2k+1)^2 - 6(2k+1) + 5 \\ &= 4k^2 + 4k + 1 - 12k - 6 + 5 \\ &= 2(2k^2 - 4k) \end{aligned}$$

We've shown that when $x$ is odd, $x^2 - 6x + 5$ can be written as $2 \cdot$ (some integer), therefore by contraposition, the original statement holds.

b. There are several ways to do this directly.

- We can factor $x^2 - 6x + 5$ into $(x-1)(x-5)$. If this product is odd, then each of $x - 1$ and $x - 5$ has to be odd (the only way for a product of two integers to be odd is if both integers are odd). But if $x - 1$ is odd, then $x$ has to be even (same with $x - 5$), as adding one to any odd integer makes it even.
- We can break this into two cases: when $x$ is even and when $x$ is odd. For each, we can evaluate $x^2 - 6x + 5$; this will show that when $x$ is even, $x^2 - 6x + 5$ is odd, and when $x$ is odd, $x^2 - 6x + 5$ is even. This also proves the original statement.

2. Prove that if $P \implies Q$ and $R \implies \neg Q$, then $P \implies \neg R$, using:

a. Proof by Contradiction

b. Proof by Contraposition *(Hint: You may need to use the fact that $A \implies B \equiv \neg A \vee B$.)*

**Solution:** It may help to think of the statement "$P \implies Q$ and $R \implies \neg Q$" as $A$, and "$P \implies \neg R$" as $B$.

a. The negation of the statement $A \implies B$ is $A \wedge \neg B$ (this was seen in lecture, but you should prove it to yourself). So, the negation of our statement is that $P \implies Q$ and $R \implies \neg Q$, but $\neg(P \implies \neg R)$. We can rewrite $\neg(P \implies \neg R)$ as $\neg(\neg P \vee \neg R) \equiv P \wedge R$. In other words, we are now assuming that all of the following are true:

   - $P \implies Q$
   - $R \implies \neg Q$
   - $P \wedge R$

   From the statement $P \wedge R$, we know that $P$ and $R$ both must be true. If $P$ is true, then $Q$ must be true in order for $P \implies Q$ to be true. However, this means the statement $R \implies \neg Q$ is false, as a true value ($R$) does not imply a false value ($\neg Q$). This is a contradiction.

   This means that the negation of our original statement cannot be true, and therefore our original statement was true.

b. The contraposition of our original statement is

$$\begin{aligned} \neg(P \implies \neg R) &\implies \neg((P \implies Q) \wedge (R \implies \neg Q)) \\ (P \wedge R) &\implies \neg((\neg P \vee Q) \wedge (\neg R \vee \neg Q)) \\ (P \wedge R) &\implies ((P \wedge \neg Q) \vee (R \wedge Q)) \end{aligned}$$

   We now need to show that this implication has a true value. This implication is true when:

   - $P \wedge R$ is true **and** $((P \wedge \neg Q) \vee (R \wedge Q))$ is true
   - $P \wedge R$ is false

   There isn't a whole lot to prove when $P \wedge R$ is false (as "false" $\implies$ "true" and "false" $\implies$ "false" are both true).

   Suppose $P \wedge R$ is true, meaning $P$ and $R$ are both true. We have to consider both cases of $Q$: $Q$ could either be true or false.

| $P$ | $R$ | $Q$ | $(P \wedge \neg Q) \vee (R \wedge Q)$ |
|---|---|---|---|
| $T$ | $T$ | $T$ | $T$ |
| $T$ | $T$ | $F$ | $T$ |

You should verify the above two cases yourself. In short, when $Q$ is true, $P \wedge \neg Q$ is false and $R \wedge Q$ is true. When $Q$ is false, $P \wedge \neg Q$ is true and $R \wedge Q$ is false. Since these two conditions are joined by a disjunction, only one needs to be true for the entire expression to be true. Therefore, by contraposition, the original statement holds true.

Which of these methods do you think was more straightforward?

3. In the previous problem set, we had you prove De Morgan's Laws for conjunctions and disjunctions.

$$\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$$
$$\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q)$$

a. *(Optional)* Using truth tables, prove both of the statements above.

b. In terms of the symbols $\vee, \wedge, \neg$, re-write the *negation* of $P \implies Q$. *(Hint: We did this in lecture, but try and derive it on your own.)*

c. Now, let's consider the statement "if $a \cdot b$ is even, then $a$ is even or $b$ is even." First, rewrite this statement using mathematical notation. *(Hint: you will need the implication symbol.)*

d. Find the contrapositive of the statement in (c), and write it using mathematical notation.

e. Prove the statement in (c) by contraposition.

f. Prove the statement in (c) using a direct proof. *(Hint: You may need to consider multiple cases.)*

g. Why do you think we included this problem?

**Solution:**

a. Done in lecture.

b. $\neg(P \implies Q) \equiv P \wedge \neg Q$

c. $(\exists k \in \mathbb{N} : a \cdot b = 2k) \implies (\exists k_1 \in \mathbb{N} : a = 2k_1) \vee (\exists k_2 \in \mathbb{N} : a = 2k_2)$ Note: We could've used $k$ instead of $k_1$ and $k_2$, as in this case, the $k$s are local to the parenthesis.

d. $(\forall k_1 \in \mathbb{N} : a \neq 2k_1) \wedge (\forall k_2 \in \mathbb{N} : a \neq 2k_2) \implies (\forall k \in \mathbb{N} : a \cdot b \neq 2k)$

e. Suppose $a = 2k + 1$ and $b = 2l + 1$ (meaning they're both odd). Then, $a \cdot b = (2k+1)(2l+1) = 4kl + 2(k+l) + 1 = 2(2kl + k + l) + 1$. Since we wrote $a \cdot b$ as an even number plus one, we know the product has to be odd. Therefore, by contraposition, the original statement holds.

f. $a$ and $b$ can each be either even, or odd. Let's look at all four possibilities:

- $a$ even, $b$ even: $a \cdot b$ is even

- $a$ even, $b$ odd: $a \cdot b$ is even
- $a$ odd, $b$ even: $a \cdot b$ is even
- $a$ odd, $b$ odd: $a \cdot b$ is odd

In all cases where $a \cdot b$ is even, at least one of $a$ or $b$ is even, proving the statement.

g. For two reasons: (1) to illustrate that the negation of a "for all" is a "there exists" (and vice versa) and the fact that the negation of a conjunction is a disjunction (and vice versa), and (2) to show that there are usually multiple ways to prove any statement.

4. In this problem, we'll look at how to prove statements of the form "$P$ if and only if $Q$." Recall, the statement $P \iff Q$ is equivalent to $(P \implies Q) \wedge (Q \implies P)$. To show that $P$ is true if and only if $Q$ is true, we need to prove both directions of the implication, i.e. that $P$ implies $Q$ and that $Q$ implies $P$. We can use any proof technique we like for each of the two sub-proofs.

   For example: Suppose we want to prove that $|A \cup B| = |A| + |B|$ if and only if $A$ and $B$ are disjoint. We need to prove two directions: if $|A \cup B| = |A| + |B|$, then $A$ and $B$ are disjoint (1), and if $A$ and $B$ are disjoint, then $|A \cup B| = |A| + |B|$ (2).

   a. Complete the proof above.

   b. We say $(a, b, c)$ is a *Pythagorean triplet* if $a^2 + b^2 = c^2$. Prove that $(a, b, c)$ can only be Pythagorean triplet if and only if at least one of $a, b, c$ are even. *(This question originally had a significant typo, which made this proof impossible, but that has now been fixed.)*

**Solution:**

a. First, let's prove the statement "if $|A \cup B| = |A| + |B|$, then $A, B$ are disjoint." We know that normally, $|A \cup B| = |A| + |B| - |A \cap B|$. By what we are allowed to assume, we have that $|A| + |B| - |A \cap B| = |A| + |B|$, implying that $|A \cap B| = 0$. However, this is only true when $A, B$ are disjoint.

   Now, let's prove the statement "if $A, B$ are disjoint, then $|A \cup B| = |A| + |B|$". If $A, B$ are disjoint, we know that $|A \cap B| = 0$. Then, $|A \cup B| = |A| + |B| - |A \cap B| = |A| + |B|$, as required.

   Since both directions hold, we have that the entire statement holds. QED.

b. First, let's prove the statement "$(a, b, c)$ can only be a Pythagorean triplet if at least one of $a, b, c$ are even." Let's do this by contradiction, that is, let's assume that there exists a triplet of odd integers $a, b, c$ such that $a^2 + b^2 = c^2$ (the negation of "at least one of $a, b, c$ is even" is "all $a, b, c$, are odd").

   Then, we can say $a = 2k + 1$, $b = 2l + 1$ and $c = 2m + 1$.

$$\begin{aligned}
c^2 &= a^2 + b^2 \\
(2m+1)^2 &= (2k+1)^2 + (2l+1)^2 \\
2(2m^2+2m)+1 &= 4k^2+4k+1+4l^2+4l+1 \\
2(2m^2+2m)+1 &= 2(2k^2+2k+2l^2+2l+1)
\end{aligned}$$

Here, we have a contradiction, as on the left side we have an odd number and on the right side we have an even number. Therefore, by contradiction, we've shown that $(a, b, c)$ can only be a Pythagorean triplet if at least one of $a, b, c$ are even.

Now, let's prove the statement "if at least one of $a, b, c$ are even, then $a, b, c$ can be a Pythagorean triplet". Since we're simply being asked to show the existence of such a triplet ("**can** be a Pythagorean triplet"), we can just give one example, i.e. $(3, 4, 5)$.

We've shown both directions of our if and only proof, therefore the entire statement holds.

5. When we are presented with the task of proving the uniqueness of two elements (where elements could be numbers, sets, vectors, etc.) we usually use a proof by contradiction. We assume that there exist two different instances of such an element, and show that they must be the same.

   For example, suppose we want to prove that additive inverses are unique. (The inverse of some real number $x$ for the operation of addition is $-x$, as $x + (-x) = 0$.) We could start by assuming that there exist two inverses, $a$ and $b$, such that $a \neq b$. This means that $x + a = 0$ and $x + b = 0$. Then:

$$\begin{aligned}
a &= a \\
&= a + (x + b) \\
&= (a + x) + b \\
&= 0 + b \\
&= b
\end{aligned}$$

   We started by assuming $a \neq b$, but showed that $a = b$, disproving the notion that additive inverses are unique.

   Sometimes, the notation $\exists!$ is used to mean "there exists a unique" / "there exists exactly one." For example, $\exists!\ x \in \mathbb{R} \mid x^2 - 4x + 4 = 0$ translates to "there exists a unique real solution to $x^2 - 4x + 4 = 0$."

   a. Prove, using a technique similar to that above, that there only exists a single positive integer solution to $a^2 + 4^2 = 5^2$.

   b. Prove that $(\forall x \in \mathbb{R}, x \neq 0)(\exists!\ y \in \mathbb{R})(x \cdot y = 1)$.

**Solution:**

a. Suppose there are two positive integer solutions $x, y$, such that $x \neq y$. They must both satisfy $a^2 = 5^2 - 4^2 = 9$. Suppose $x^2 = y^2$. Then, either $x = y$ or $x = -y$. The latter case cannot be true, as it implies either $x$ or $y$ is negative. That means $x = y$, which contradicts what we assumed in the beginning. Therefore, there is only one such $a$.

b. Suppose there exist two such values of $y$, $y_1$ and $y_2$, such that $y_1 \neq y_2$, and that $x, y_1, y_2 \neq 0$. Then:

$$x \cdot y_1 = 1 \implies y_1 = \frac{1}{x}$$
$$x \cdot y_2 = 1 \implies y_2 = \frac{1}{x}$$
$$\implies y_1 = y_2$$

which again contradicts what we assumed in the beginning. Therefore, multiplicative inverses are unique.

6. Over the summer, Billy spent all day thinking about math (same!) and trying to come up with the next big proof. After a few months, he presents this proof to you to proofread. Verify that his proof is correct, or explain the error.

*Theorem:* If $n$ is an integer and $2n + 2$ is even, then $n$ is odd.

**Proof:** Proceed by contraposition. Assume that $n$ is odd. We will now prove that $2n + 2$ is even. Clearly, $2n$ must be an even number, since it is divisible by 2. Furthermore, 2 is an even number, so $2n + 2$ must be even. This concludes the proof.

**Solution:** This is a statement that is false. For example, when $n = 4$, $2n + 2 = 10$ which is even, but $n$ is still an even number. Bob attempted to prove this statement by contraposition, but instead of taking the contrapositive, he took the converse.

In general, an implication $P \to Q$ is not logically equivalent with its contrapositive, $Q \to P$.

7. The following problems involve parity arguments  that is, reasoning about whether some combinations of integers are even or odd.

   a. Prove that if $a, b$ and $c$ are odd integers, then there are no integer solutions to $ax^2+bx+c = 0$. *(Hint 1: You should consider two different cases for $x$. Hint 2: Negative integers can still be even or odd. Hint 3: Is it possible for the sum of a few integers to be a non-integer?)*

   b. Prove that there are no integer solutions to $a^2 - 4b = 2$.

**Solution:**

a. We will actually prove a stronger statement: that if $a, b, c$ are odd integers, then there are no **rational** solutions to $ax^2 + bx + c = 0$. Since all integers are rational numbers, if we prove this statement for all rationals, we've proven it for all integers as well.

   Let's proceed by contradiction, by assuming that there are rational solutions to $p(x) = ax^2 + bx + c = 0$ with all $a, b, c$ odd. This would mean we can factor $p(x)$ into $p(x) = (Ax+B)(Cx+D)$. Expanding this out yields $p(x) = ACx+(AD+BC)x+BD$, where $a = AC$, $b = AD + BC$ and $c = BD$.

   Since $a$ and $c$ are both odd, we have that $A, C, B$ and $D$ must all also be odd. If that's the case, though, then that would mean $b = AC + BD$ is even, as it is the sum of two odd numbers. This contradicts our initial assumption that all $a, b, c$ are odd, and therefore the original statement holds by proof by contradiction.

b. We will proceed by contradiction. Let's assume there are integral solutions for $a, b$.

   We can rearrange to have $a^2 = 2 + 4b = 2(1 + 2b)$. This means that $a^2$ is even, and thus $a$ is even, meaning we can say $a = 2k$.

   Then,

$$
\begin{aligned}
(2k)^2 &= 2(1 + 2b) \\
4k^2 &= 2(1 + 2b) \\
2k^2 &= 1 + 2b
\end{aligned}
$$

   Here, we have a contradiction, as $2k^2$ is even, but $1 + 2b$ must be odd. Therefore, there cannot be any integer solutions for $a, b$.

8. Prove that $\sqrt{2}^{\sqrt{2}^{\sqrt{2}^{\sqrt{2}^{\cdots}}}} = 2$. *(This is a challenging problem. Try not to search for it online. Hint: Define some variable $x$ recursively.)*

**Solution:** Let $x = \sqrt{2}^x$. Then:

$$
\begin{aligned}
\ln x &= x \ln 2^{\frac{1}{2}} \\
\frac{1}{x} \ln x &= \frac{1}{2} \ln 2
\end{aligned}
$$

It now becomes clear that $x = 2$ satisfies the above relationship. However, it isn't necessarily the only solution. Suppose that $g(x) = \frac{\ln x}{x}$.

By differentiating $g(x)$ it becomes clear that $g(x)$ has a local maximum at $x = e$ and begins decreasing after, implying that there are two solutions potential values of $x$ that could satisfy this equation. It turns out that $x = 4$ is also a solution to $g(x)$.

How do we know that $x = 4$ is not the correct answer?

Suppose we consider some recursive sequence defined by $a_0 = \sqrt{2}$, $a_n = \sqrt{2}^{a_{n-1}}$, it can be shown by induction that $a_n \leq 2$. Do this as an exercise!