Proof techniques: 2

In this lecture, we will continue our work on proof techniques. The majority of the material is simply a set of *examples* from which you can develop your proof skills, and use as possible templates for similar proofs. There is very new little technical material.

1 Proof by Contradiction

A proof by contradiction can be used to prove almost any kind of statement. The basic idea is to assume that the statement we want to prove is **false**, and then show that this leads to "nonesense". We must then conclude that we were **wrong** to assume the statement was false, and thus the statement **must be true**. One of the most famous proofs by contradiction is given below:

Example 1. *Prove that $\sqrt{2}$ is irrational. **also shown in chalkboard lecture*

Solution: The statement we are asked to prove is that "$\sqrt{2}$ is irrational". To proceed with a proof by contradiction, we assume that this statement is **false**, in other words, we assume that $\sqrt{2}$ is *rational*. We will show that this leads to a some kind of mathematical nonsense (i.e. a contradiction). Then we conclude that the *only* possibility is that $\sqrt{2}$ is irrational. If $\sqrt{2}$ is rational, then there exist integers p, q, $q \neq 0$ such that $\sqrt{2} = p/q$. We will assume that the fraction is written in lowest terms, in other words that the p and q have no common factors. By squaring both sides:

$$2 = \frac{p^2}{q^2}$$

Hence

$$2q^2 = p^2$$

Now the left hand side is an *even* number, which means that the right hand side should also be even. So p^2 is even. But if p^2 is even, then p is also even, and as usual, this means that $p = 2k$ for some integer k. Then we can use this to replace the p in the above equation:

$$2q^2 = p^2 = 4k^2$$

which simplifies to $q^2 = 2k^2$. But now this means q^2 is *also* an even number, which means q is an even number. But now our deductions have lead to the fact that p is even *and* q is even... which is *impossible* since we assumed that the fraction p/q was written in lowest terms. So we have arrived at a **contradiction**, and thus the statement "$\sqrt{2}$ is rational" must be false, in other words, "$\sqrt{2}$ is irrational" is true.

Example 2. *If you select 15 days out of the year, at least two of the days fall in the same month*

Solution: There are many different cases to analyze if we were to proceed with a direct proof - imagine *all* the different way the days can fall into the calendar. A proof by contradiction takes the negation of the above statement: "*it is **not** true that at least two days fall in the same month*" which is equivalent to "*all 15 days fall in different months*". This statement is much easier to work with. In fact, immediately one might notice that this is impossible: there are only 12 months of the year, making it impossible to have 15 different months. Therefore, the negation is impossible, and thus we must conclude that the original statement is true: at least two of the days fall in the same month.

Example 3. *If a and b are integers, then $a^2 - 4b - 2 \neq 0$*

Solution: For a proof by contradiction, we assume the negation of the above statement: in other words that $a^2 - 4b - 2 = 0$. As above, we use this to find some kind of contradiction, so that we can conclude that actually $a^2 - 4b - 2 \neq 0$. To begin, we take the assumption $a^2 - 4b - 2 = 0$, and note that this means that $a^2 = (4b + 2) = 2(2b + 1)$. Thus a^2 is a multiple of 2 (and thus an even number), and so a is even. This means we can write $a = 2k$. We can replace this in the equation above and get:

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

But the last line has a problem: the left side is an *even* number, and the right side is an *odd* number. This is impossible! Thus we have arrived at a contradiction, and therefore we must conclude that actually $a^2 - 4b - 2 \neq 0$.

1.1 Proofs by Contradiction involving implications

Suppose we want to prove $P \Rightarrow Q$. We saw in the previous section that this could be done using the contrapositive: $\neg Q \Rightarrow \neg P$. However, we could *also* prove $P \Rightarrow Q$ using a **contradiction**. We assume $P \Rightarrow Q$ is false, which is equivalent to $\neg(P \Rightarrow Q) \equiv P \wedge \neg Q$ (recall our section on Logic). Again, we continue with a sequence of deductions until we arrive at a contradiction, which enables us to conclude that $P \Rightarrow Q$. In the following examples, we show how to take an implication and apply the contradiction, and arrive at a contradiction.

Example 4. *Suppose that $a, b \in \mathbb{R}$. If a is rational and ab is irrational, then b is irrational.*

Solution: This is an implication of the form $P \Rightarrow Q$ where P : a is rational and ab is irrational, $Q : b$ is irrational. We assume the contradiction, $P \wedge \neg Q$: that is that a is rational, ab is irrational, and b is *rational*. Then a and b can both be written as fractions of integers, p, q, r, s where $q, s \neq 0$:

$$a = \frac{p}{q}, b = \frac{r}{s}$$

but then

$$ab = \frac{pr}{qs}$$

which means that ab is also rational. This is a contradiction (since in the above statement ab was assumed to be irrational). Therefore, we can conclude that the original statement must be true: if a is rational and ab is irrational, then b is irrational.

2 Proofs involving sets

The techniques we developed in the previous sections, namely the direct proof, contrapositive proof, and proof by contradiction, can be applied to proofs involving sets. In this section we will work through several examples to get a feeling of how they are applied to the notions of set theory.

2.1 Proving $A \subseteq B$

In our lecture on subsets, we defined $A \subseteq B$ to mean that for all $x \in A$, we have $x \in B$. In order to *prove* that $A \subseteq B$, we must assume that we are given **any arbitrary** $x \in A$ and we need to show that this implies that that $x \in B$.

Example 5. *Suppose that $A \subseteq B$. Prove that $A - C \subseteq B - C$.*

Solution: Assume that we are given an arbitrary $a \in A - C$. Then $a \in A$ and $a \notin C$. Since $A \subseteq B$, then $a \in B$. Thus we have that $a \in B$ and $a \notin C$, so $a \in B - C$. Therefore $A - C \subseteq B - C$.

2.2 Proving $A \subset B$

To prove that $A \subset B$, which is called a *proper subset*, then one proceeds as in the previous section to show that $A \subseteq B$, and then next one shows that the sets are not equal by finding an element $b \in B$ where $b \notin A$.

Example 6. *Suppose that $A = \{n \in \mathbb{Z} | n = 12k + 7$ for some integer $k\}$ and $B = \{m \in \mathbb{Z} | m = 4l + 3$ for some integer $l\}$. Prove that $A \subset B$.*

Solution: Assume we are given an element $a \in A$. There there exists an integer k such that $a = 12k+7$. We can rewrite this as:

$$a = 12k + 7 = 4(3k) + 4 + 3 = 4(3k + 1) + 3$$

So letting $l = 3k + 1$, we have that $a = 4l + 3$. Thus $a \in B$. We have shown $A \subseteq B$. It remains to show that it is a *proper* subset. We need to find an element that is in B but that is not in A. Notice that the element 11 is in B, since $11 = 4(2) + 3$. However, if $11 \in A$, then $11 = 12k + 7$ implies that $4 = 12k$ for some integer k, which has no solution. Thus $A \neq B$, so we can conclude that $A \subset B$.

2.3 Proving $A = B$

In our section on sets, we learned that set equality was defined as $A \subseteq B$ and $B \subseteq A$. This definition is used directly when asked to prove that two sets are equal. Thus the proof involves two steps: we first prove $A \subseteq B$ and then prove $B \subseteq A$.

Example 7. *Suppose A,B,C are sets, and $C \neq \emptyset$. Prove that if $A \times C = B \times C$, then $A = B$.*

Solution: We start by showing that $A \subseteq B$. Suppose $a \in A$. Since $C \neq \emptyset$, then there must be at least one element in C. Let's call that element c. Then $(a, c) \in A \times C$, and so (a, c) is *also* in $B \times C$, since the two sets are equal. So the element $a \in B$ by the definition of the Cartesian product. Thus $a \in A$ has lead to $a \in B$, so we conclude that $A \subseteq B$. Next we proceed to show that $B \subseteq A$. The steps are identical. We assume $b \in B$. Then $(b, c) \in B \times C$, and so $(b, c) \in A \times C$, thus $b \in A$. Therefore $B \subseteq A$. Both facts together imply $A = B$.

3 Existence proofs and constructive proofs

Often one is asked to prove that objects of a particular type *exist*, in other words, we are asked to prove a statement which is equivalent to $\exists x P(x)$. These proofs are called **existence proofs**. They are based on the fact that it is up to "us" to *find* or *prove* that there exists some x for which the statement is true. This can be done in two different ways. One can either *find* such an element x, in which case the proof is called **constructive**. In other cases, it is possible to show that the element x exists, without actually stating what it is, which is called a **nonconstructive** proof.

3.1 Constructive proofs

Example 8. *Prove that there exists a pair of consecutive integers such that one of these integers is a perfect square and the other is a perfect cube*

Solution: A direct approach would consider the perfect cubes, and for each one check if the previous or next consecutive integer is a perfect square. The perfect cubes are $1, 8, 27, 64, 125...$, and right away we can identify $8 = 2^3$ which is a perfect cube, and $9 = 3^2$ which is a perfect square. Thus we have found the pair of integers that satisfy the statement. They are 8 and 9.

Example 9. *In a game of two players, each person takes a turn removing either 1,2 or 3 stones from a pile of stones. The original pile contains 15 stones. The last player to take a turn is the winner. Show that the first player has a way to win the game, no matter what the second player does.*

Solution: In order to prove that a winning strategy *exists*, we simply describe the strategy that is guaranteed to win.

- On the first turn, the first player will remove 3 stones, leaving exactly 12 stones in the pile for the second player
- The second player will remove 1,2 or 3 stones, which means that there are now either 9,10,or 11 stones left.
- If the pile was size 11, the first player removes 3 stones. If it was size 10, the first player removes 2 stones. If it was size 9, the first player removes 1 stone. In all 3 cases, the first player leaves a pile with exactly 8 stones left
- The second player will remove 1,2 or 3 stones, which means that there are now either 5,6 or 7 stones left.
- If the pile was size 7, the first player removes 3 stones, if it was size 6, the first layer removes 2 stones, if it was size 5, the player removes 1 stone. In all 3 cases, the first player leaves a pile with exactly 4 stones left.
- The second player will now remove 1,2 or 3 stones. There will be either 1,2 or 3 stones left.
- The first player removes the remaining stones and **wins**.

Example 10. *Prove that between any two rational numbers, there is an irrational number*

Solution: We need to prove there this is true not matter what two rational numbers we start with. Suppose they are p and q, where $p < q$. We need to construct an irrational number between p and q. Recall that $\sqrt{2}$ is a known irrational, and any product of $\sqrt{2}$ with a rational number will be irrational. The difference bewteen p and q is $(q - p)$, and so

$$p + \sqrt{2}\left(\frac{q-p}{2}\right)$$

is an irrational number that lies between p and q. One can test this out with two rationals. Suppose $p = 0.54$ and $q = 0.55$. Then

$$0.54 + \sqrt{2}\left(\frac{0.01}{2}\right) = 0.54 + 0.005\sqrt{2} \approx 0.5470710678...$$

is an irrational number between 0.54 and 0.55.

3.2 Nonconstructive proofs

In a nonconstructive proof, one can argue that an element exists which validates the statement $\exists x P(x)$, without actually explicitly describing x. A well known example based on the game of **Chomp** is described and illustrated in the chalkboard lecture.

3.3 Uniqueness proofs

Sometimes we are asked to prove that there is a *unique* element that has a certain property. In this case, it is not enough to simply use a constructive proof to demonstrate such an element **exists** - we would *also* need to prove that **no other element has this property**.

Example 11. *Suppose that n is an odd integer. Prove that there is a unique integer k such that n is the sum of $k-2$ and $k+3$*

Solution:

Since n is an odd integer, then it can be expressed as $n = 2m+1$ for some integer m. Note that $m = \frac{n-1}{2}$. We will first show that the integer k *exists* where $(k-2)+(k+3) = n$. Set $k = \frac{n-1}{2}$, then we have exactly:

$$\frac{n-1}{2} - 2 + \frac{n-1}{2} + 3 = (n-1) + 1 = n$$

and thus we have shown that the integer k *exists*, in fact it is $k = \frac{n-1}{2}$. For example, if $n = 11$, then $k = 5$ since $(5-2)+(5+3) = 11$. Next we need to show that *no other* integer exists. Suppose that another integer, l satisfies $(l-2)+(l+3) = n$. Then

$$l - 2 + l + 3 = 2l + 1$$

and if this is equal to n, then $2l+1 = n$. Yet $n = 2m+1$. Setting these two equal, we have $2l+1 = 2m+1$ and thus $l = m = \frac{n-1}{2}$. So we have shown that *if* another integer, l, exists which satisfies the statement, then the only way this is possible is if $l = \frac{n-1}{2}$. Thus the unique element that satisfies the statement is $m = \frac{n-1}{2}$.

4 Disproofs

To disprove a statement, we are simply being asked to prove the *negative* of a statement. In other words, if one is asked to **disprove** the statement P, then our job is to **prove** the statement $\neg P$. The approach is therefore very simple, and can then proceed as a direct proof, or a contrapositive proof, or contradiction, etc.

Often one is asked to disprove a universally quantified statement, such as $\forall x P(x)$. To disprove such a statement, the negative is $\exists x \neg P(x)$. Therefore we need to show that there *exists* an x for which the statement is not true. There is a special name for an example that disproves a statement. It is called a **counterexample**.

Example 12. *Prove or disprove that for every natural number n, the integer $f(n) = n^2 - n + 11$ is prime.*

To start things off, it's a good idea to gather some information about the statement. One could evaluate $f(n)$ for some values of n and determine whether or not it would be a good idea to attempt a *proof* or to start looking for a counterexample, which would then be a *disproof*. Starting with $n = 0$, the list below shows the values of $f(n)$ as n increases by 1:

$$11, 11, 13, 17, 23, 31, 41, 53, 67, 83, 101, 121...$$

Note that most of these are primes, but suddenly we fall on $f(11) = 121$, and 121 is not a prime number. We have found a case where the statement is *not* true: $f(11)$ is *not* prime. Thus the statement is **false** and the counterexample is $n = 11$.

Example 13. *Prove or disprove that if A, B, C are sets and $A \times C = B \times C$ then $A = B$.*

Solution: This is false. A counter example is $A = \{a\}$, $B = \{b\}$, and $C = \emptyset$. Then $A \times C = \emptyset$ and $B \times C = \emptyset$. Yet $A \neq B$.

5 Bad Proofs

Some of the biggest mistakes made in proofs are listed below:

- *Assuming* something to be true
- Using an example to *prove* something is true in general
- Making Mathematical or logical errors

Let's take an example of something that we know is false, see how it is nevertheless possible to fall into a trap of constructing a bogus proof:

Prove: *If $a = b$, where a, b are real numbers, then $a = 0$.*

Bogus proof:

$$\begin{aligned} a &= b \\ a^2 &= ab \\ a^2 - b^2 &= ab - b^2 \\ (a-b)(a+b) &= (a-b)b \\ a+b &= b \\ a &= 0 \end{aligned}$$

Make sure you can identify the error in the above proof!