Proof Techniques

Jessica Su

November 12, 2016

1 Proof techniques

Here we will learn to prove universal mathematical statements, like "the square of any odd number is odd". It's easy enough to show that this is true in specific cases – for example, $3^2 = 9$, which is an odd number, and $5^2 = 25$, which is another odd number. However, to prove the statement, we must show that it works for *all* odd numbers, which is hard because you can't try every single one of them.

Note that if we want to *disprove* a universal statement, we only need to find one counterexample. For instance, if we want to disprove the statement "the square of any odd number is even", it suffices to provide a specific example of an odd number whose square is not even. (For instance, $3^2 = 9$, which is not an even number.)

Rule of thumb:

- To **prove** a universal statement, you must show it works in all cases.
- To **disprove** a universal statement, it suffices to find one counterexample.

(For "existence" statements, this is reversed. For example, if your statement is "there exists at least one odd number whose square is odd, then proving the statement just requires saying $3^2 = 9$, while disproving the statement would require showing that none of the odd numbers have squares that are odd.)

1.0.1 Proving something is true for all members of a group

If we want to prove something is true for all odd numbers (for example, that the square of any odd number is odd), we can pick an arbitrary odd number x, and try to prove the statement for that number. In the proof, we cannot assume anything about x other than that it's an odd number. (So we can't just set x to be a specific number, like 3, because then our proof might rely on special properties of the number 3 that don't generalize to all odd numbers).

Example: Prove that the square of any odd number is odd.

Proof: Let x be an arbitrary odd number. By definition, an odd number is an integer that can be written in the form $2k + 1$, for some integer k. This means we can write $x = 2k + 1$, where k is some integer. So $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Since k is an integer, $2k^2 + 2k$ is also an integer, so we can write $x^2 = 2\ell + 1$, where $\ell = 2k^2 + 2k$ is an integer. Therefore, x^2 is odd.

Since this logic works for *any* odd number x, we have shown that the square of any odd number is odd.

1.1 Special techniques

In addition to the "pick an arbitrary element" trick, here are several other techniques commonly seen in proofs.

1.1.1 Proof by contrapositive

Consider the statement "If it is raining today, then I do not go to class."

This is logically equivalent to the statement "If I go to class, then it is not raining today."

So if we want to prove the first statement, it suffices to prove the second statement (which is called the **contrapositive**).

Note that it is **not** equivalent to the statement "If I do not go to class, then it is raining today" (this is called the fallacy of the converse).

Example: Let x be an integer. Prove that x^2 is an odd number if and only if x is an odd number.

Proof: The "if and only if" in this statement requires us to prove both directions of the implication. First, we must prove that if x is an odd number, then x^2 is an odd number. Then we should prove that if x^2 is an odd number, then x is an odd number.

We have already proven the first statement, so now we just need to prove the second statement. The second statement is logically equivalent to its contrapositive, so it suffices to prove that "if x is an even number, then x^2 is even."

Suppose x is an even number. This means we can write $x = 2k$ for some integer k. This means $x^2 = 4k^2 = 2(2k^2)$. Since k is an integer, $2k^2$ is also an integer, so we can write $x^2 = 2\ell$ for the integer $\ell = 2k^2$. By definition, this means x^2 is an even number.

1.1.2 Proof by contradiction

In proof by contradiction, you assume your statement is not true, and then derive a contradiction. This is really a special case of proof by contrapositive (where your "if" is all of mathematics, and your "then" is the statement you are trying to prove).

Example: Prove that $\sqrt{2}$ is irrational.

Proof: Suppose that $\sqrt{2}$ was rational. By definition, this means that $\sqrt{2}$ can be written as m/n for some integers m and n. Since $\sqrt{2} = m/n$, it follows that $2 = m^2/n^2$, so $m^2 = 2n^2$. Now any square number x^2 must have an even number of prime factors, since any prime factor found in the first x must also appear in the second x. Therefore, m^2 must have an even number of prime factors. However, since n^2 must also have an even number of prime factors, and 2 is a prime number, $2n^2$ must have an odd number of prime factors. This is a contradiction, since we claimed that $m^2 = 2n^2$, and no number can have both an even number of prime factors and an odd number of prime factors. Therefore, our initial assumption was wrong, and $\sqrt{2}$ must be irrational.

1.1.3 Proof by cases

Sometimes it's hard to prove the whole theorem at once, so you split the proof into several cases, and prove the theorem separately for each case.

Example: Let n be an integer. Show that if n is not divisible by 3, then $n^2 = 3k + 1$ for some integer k.

Proof: If n is not divisible by 3, then either $n = 3m + 1$ (for some integer m) or $n = 3m + 2$ (for some integer m.

Case 1: Suppose $n = 3m + 1$. Then $n^2 = (3m + 1)^2 = 9m^2 + 6m + 1 = 3(3m^2 + 2m) + 1$. Since $3m^2 + 2m$ is an integer, it follows that we can write $n^2 = 3k + 1$ for $k = 3m^2 + 2m$.

Case 2: Suppose $n = 3m+2$. Then $n^2 = (3m+2)^2 = 9m^2+12m+4 = 9m^2+12m+3+1 = 3(3m^2 + 4m + 1) + 1$. So we can write $n^2 = 3k + 1$ for $k = 3m^2 + 4m + 1$.

Since we have proven the statement for both cases, and since Case 1 and Case 2 reflect all possible possibilities, the theorem is true.

1.2 Proof by induction

We can use induction when we want to show a statement is true for all positive integers n. (Note that this is not the only situation in which we can use induction, and that induction is not (usually) the only way to prove a statement for all positive integers.)

To use induction, we prove two things:

- **Base case:** The statement is true in the case where $n = 1$.
- **Inductive step:** If the statement is true for $n = k$, then the statement is also true for $n = k + 1$.

This actually produces an infinite chain of implications:

- The statement is true for $n = 1$

- If the statement is true for $n = 1$, then it is also true for $n = 2$
- If the statement is true for $n = 2$, then it is also true for $n = 3$
- If the statement is true for $n = 3$, then it is also true for $n = 4$
- ...

Together, these implications prove the statement for all positive integer values of n. (It does not prove the statement for non-integer values of n, or values of n less than 1.)

Example: Prove that $1 + 2 + \cdots + n = n(n + 1)/2$ for all integers $n \geq 1$.

Proof: We proceed by induction.

Base case: If $n = 1$, then the statement becomes $1 = 1(1 + 1)/2$, which is true.

Inductive step: Suppose the statement is true for $n = k$. This means $1 + 2 + \cdots + k = k(k+1)/2$. We want to show the statement is true for $n = k+1$, i.e. $1+2+\cdots+k+(k+1) = (k + 1)(k + 2)/2$.

By the induction hypothesis (i.e. because the statement is true for $n = k$), we have $1 + 2 + \cdots + k + (k + 1) = k(k + 1)/2 + (k + 1)$. This equals $(k + 1)(k/2 + 1)$, which is equal to $(k + 1)(k + 2)/2$. This proves the inductive step.

Therefore, the statement is true for all integers $n \geq 1$.

1.2.1 Strong induction

Strong induction is a useful variant of induction. Here, the inductive step is changed to

- **Base case:** The statement is true when $n = 1$.
- **Inductive step:** If the statement is true for all values of $1 \leq n < k$, then the statement is also true for $n = k$.

This also produces an infinite chain of implications:

- The statement is true for $n = 1$
- If the statement is true for $n = 1$, then it is true for $n = 2$
- If the statement is true for both $n = 1$ and $n = 2$, then it is true for $n = 3$
- If the statement is true for $n = 1$, $n = 2$, and $n = 3$, then it is true for $n = 4$
- ...

Strong induction works on the same principle as weak induction, but is generally easier to prove theorems with.

Example: Prove that every integer n greater than or equal to 2 can be factored into prime numbers.

Proof: We proceed by (strong) induction.

Base case: If $n = 2$, then n is a prime number, and its factorization is itself.

Inductive step: Suppose k is some integer larger than 2, and assume the statement is true for all numbers $n < k$. Then there are two cases:

Case 1: k is prime. Then its prime factorization is just k.

Case 2: k is composite. This means it can be decomposed into a product xy, where x and y are both greater than 1 and less than k. Since x and y are both less than k, both x and y can be factored into prime numbers (by the inductive hypothesis). That is, $x = p_1 \dots p_s$ and $y = q_1 \dots q_t$ where $p_1, \dots, p_s$ and $q_1, \dots, q_t$ are prime numbers.

Thus, k can be written as $(p_1 \dots p_s) \cdot (q_1 \dots q_t)$, which is a factorization into prime numbers.

This proves the statement.

2 References

Greg Baker, "Introduction to Proofs"

`https://www.cs.sfu.ca/~ggbaker/zju/math/proof.html`

CS 103 Winter 2016, "Guide to Proofs"

`http://stanford.io/2dexnf9`

Peng Hui How, "Proof? A Supplementary Note For CS161"

`http://web.stanford.edu/class/archive/cs/cs161/cs161.1168/HowToWriteCorrectnessProof.pdf`