Proof Workshop Week 2: Proof Strategies

September 22, 2023

Contents

1 Day 2: Proof Strategies and When To Use Them

1.1 Proofs By Counterexample

Often times, mathematical statements will have the form $\forall x,\ P(x)$. If we want to disprove this statement, this means that we want to negate it:

$$\neg(\forall x, P(x)) \iff \exists x, \neg P(x)$$

and so it is sufficient to give a simple example of an x such that $P(x)$ does not hold. In formal proofwriting, however, it is not enough to merely supply an x for which $P(x)$ is non-truth; we must also justify why such an x is a valid counterexample.

Example 1.1. *Assess the truth of the equality* $\dfrac{1}{x+y} = \dfrac{1}{x} + \dfrac{1}{y}$ *for all* $x, y \in \mathbb{R}$.

Choose $x = 2$, $y = 3$. Then $\dfrac{1}{2+3} = \dfrac{1}{5} \neq \dfrac{5}{6} = \dfrac{1}{2} + \dfrac{1}{3}$. □

Example 1.2. *Is it true that for all series* $\{a_n\}$, *if* $\lim\limits_{n\to\infty} a_n = 0$, *then* $\displaystyle\sum_{n=1}^{\infty} a_n$ *converges?*

Much to the dismay of many an introductory calculus student, no. This is because the harmonic series

$$\sum_{n=1}^{\infty} \frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots$$

diverges, even though $\lim\limits_{n\to\infty} \dfrac{1}{n} = 0$. □

Example 1.3. (Euler.) *Show whether or not it is true that for integers* $n, k > 1$, *if the sum of* n *many* k*th powers of positive integers is itself a* k*th power, then* n *is at least* k*; that is:*

$$a_1^k + a_2^k + \dots + a_n^k = b^k \implies n \geq k, \qquad a_i, n, k \in \mathbb{Z}$$

(Lander and Parkin, 1966.) It is false. Choose $(a_1, a_2, a_3, a_4, b) = (27, 84, 110, 113, 144)$, and check that

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5.$$

But $4 < 5$. □

1.1.1 Exercise

1. Is the following statement true? If not, give a counterexample.

   If n is an integer and n^2 is divisible by 4, then n is divisible by 4.

2. (★) Give a counterexample to the following statement:

   Consider real-valued functions on $[0, 1]$. If the product of two functions is the zero function, then one of the functions is the zero function.

3. For $a, b \in \mathbb{R}$, prove or disprove $(a + b)^2 = a^2 + b^2$.

4. For $x \in \mathbb{R}$, prove or disprove $\frac{1}{x+2} = \frac{1}{x} + \frac{1}{2}$.

5. For $a, b \in \mathbb{R}$, prove or disprove: if $a^2 - b^2 > 0$, then $a - b > 0$.

1.2 Proofs By Contradiction

Suppose that we want to show that some given mathematical statement P is true. Furthermore, suppose that P is false and that, from this assumption, we can deduce a statement that contradicts some assumption we already made in the proof or some other known fact (perhaps a triviality, definition, axiom, or theorem). If we call the original assumption Q, then we have deduced $\neg Q$ and have produced the contradiction $C : Q \wedge (\neg Q)$. We have therefore established the truth of the implication $(\neg P) \implies C$. However, because $(\neg P) \implies C$ is true and C is false, it follows that $\neg P$ is false, and so P is true, as desired. This technique is called **proof by contradiction**.

In the case that, given a nice domain $\mathcal{D}$, P is the quantified statement $\forall x \in \mathcal{D},\ P_1(x) \implies P_2(x)$, then the method of proving by contradiction consists of verifying the implication

$$\neg(\forall x \in \mathcal{D},\ P_1(x) \implies P_2(x)) \implies C,$$

for some contradiction C. Since

$$\begin{aligned} \neg(\forall x \in \mathcal{D},\ P_1(x) \implies P_2(x)) &\equiv \exists x \in \mathcal{D},\ \neg(P_1(x) \implies P_2(x)) \\ &\equiv \exists x \in \mathcal{D},\ (P_1(x) \wedge (\neg P_2(x))), \end{aligned}$$

the proof of such a P typically starts by assuming the existence of a counterexample of this P.

Let us summarize the above. When we prove by contradiction, we affirm a positive statement by refuting its denial. We often inform the reader that we are employing this strategy by stating something like *Suppose that P is false* or *Assume, to the contrary, that P is false*. Let's look at a few classic examples.

Example 1.4. Suppose we wish to show that there is no largest natural number. Assume the contrary, that there *is* a largest number $x \in \mathbb{N}$. By definition, there is no $n \in \mathbb{N}$ such that $n > x$. However, $x + 1 > x$, and $x + 1 \in \mathbb{N}$. This is a contradiction, so there is no largest natural number $\mathbb{N}$. □

Theorem 1 (Fundamental Theorem of Arithmetic (FTA).)
Every positive integer $n > 1$ can be expressed as the product of primes; this representation is unique, apart from the order in which the factors occur.

Example 1.5. (Euclid.) *There is an infinite number of primes.*

Let $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7, \ldots$ be the primes in ascending order, and suppose there is a last prime, called p_n. Now consider the positive integer

$$P = p_1 p_2 \cdots p_n + 1.$$

Because $P > 1$ and by FTA, P must be divisible by some prime p. But $p_1, p_2, \ldots, p_n$ are the only prime numbers out there, so p must equal one of $p_1, p_2, \ldots, p_n$. Combining the divisibility relation $p \mid p_1 p_2 \ldots p_n$ with $p \mid P$, we arrive at $p \mid P - p_1 p_2 \ldots p_n$; equivalently, $p \mid 1$. The only positive divisor of the integer 1 is 1 itself and, because $p > 1$, a contradiction arises. Hence the number of primes is infinite. □

Example 1.6. (Pythagoras.) *Show that $\sqrt{2}$ is irrational.*

Suppose, to the contrary, that $\sqrt{2}$ is a rational number, say $\sqrt{2} = a/b$, where a and b are coprime, i.e. $\gcd(a, b) = 1$. Squaring, we get $a^2 = 2b^2$, so that $b \mid a^2$. If $b > 1$, the FTA guarantees the existence of a prime p such that $p \mid b$. It then follows that $p \mid a^2$ and that $p \mid a$;[1] hence $\gcd(a, b) \geq p$. We therefore arrive at a contradiction, unless $b = 1$. But if this happens, then $a^2 = 2$, which is merely circular. Our supposition that $\sqrt{2}$ is a rational number is untenable, and so $\sqrt{2}$ must be irrational. □

Example 1.7. (Ramsey's.) *Prove that out of a party of six people, there exists a group of three mutual friends or a group of three mutual non-friends.*

Suppose, for the sake of contradiction, that given any group of three people among the six, there are no more than two friendships or two non-friendships. Let the six people be Alice, Bob, Claire, Dash, Ella, and Frank. The possible relationships are shown with dashed lines (Figure 1.7). Start with Alice. Suppose that Alice is friends with at least three people, Bob, Claire, and Dash.

Let a friendship be denoted with a double line, and let a non-friendship be denoted with a single line. If any pair of Bob, Claire, or Dash are friends, then they form a group of 3 mutual friends with Alice, as shown in Figure 1.7.

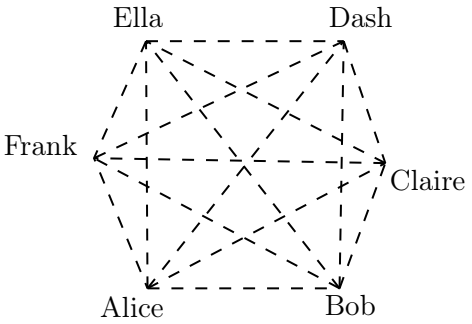
If Bob, Claire, and Dash are all non-friends, then they form a group of 3 mutual non-friends. In fact, without loss of generality, this same contradiction arises with any combination of 4 people including Alice. Therefore, given any party of 6 people, there exists a group of 3 mutual friends or a group of 3 mutual non-friends. □

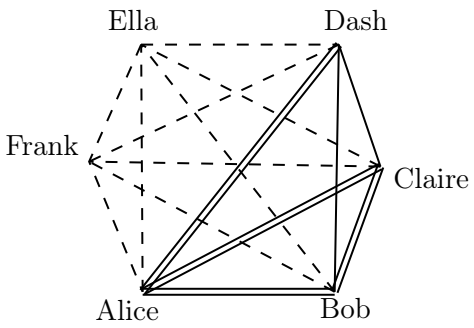
Remark 2. Often, people may give a proof of contradiction of $P \implies Q$ by assuming $\neg Q$ and proceeding to give a proof of Q, which would contradict $\neg Q$ and so $P \implies Q$. But they will never have meaningfully used the assumption $\neg Q$ in any way. *This is just a direct proof*, and will be shorter and easier to read if it is phrased as such.

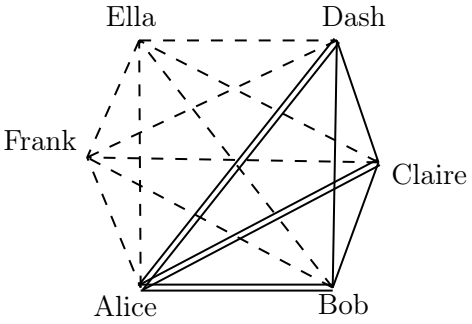
1.2.1 Exercises

1. (★) Show that there is no smallest positive real number.

[1] To see this, observe that for a prime p, if $p \mid ab$, then $p \mid a$ or $p \mid b$.







2. Show that if $a, b \in \mathbb{Z}$, then $a^2 - 4b \neq 2$.

3. Show that the sum of a rational real number and an irrational real number is always an irrational number.

4. a) Let r be a rational number. Show that $\frac{r}{\sqrt{2}}$ is irrational. (Remember $\sqrt{2}$ is irrational).

   b) Use this to show that any rational number r can be written as the product of two irrational numbers. (This doesn't need contradiction).

5. Prove that there is no integer pair of solutions (x, y) such that $x^2 = 4y + 2$.

6. Let p be a prime number. Show that if $p|n$, then $p \not| n + 1$.

7. Show that there are no positive integers x and y such that $x^2 - y^2 = 1$.

1.3 Proofs By Contrapositive

Another common proof strategy is the **proof by contrapositive**. Suppose we want to prove $\mathbb{P} \implies Q$. Then, as was noted last week, this is equivalent to the statement $\neg Q \implies \neg P$.

One way to be convinced of this is as follows. Suppose $P \implies Q$ is true. Now if $\neg Q \implies \neg P$ were not true, then it could be the case that we have $\neg Q$, but also have that P holds. But $P \implies Q$, so that both Q and $\neg Q$ hold, a contradiction. So it must be the case that $\neg Q \implies \neg P$. When giving a proof of the contrapositive, we often say "we will prove the contrapositive" or say "assume $\neg P$" to indicate we are doing so.

We often want to use the contrapositive when it is easier to work with the statement $\neg Q$ than the statement P. We give a few examples below.

Example 1.8. If $x^2 - 6x + 5$ is even, then x is odd.

Suppose x is not odd, so that it is even and $x = 2a$ for some integer a. So

$$x^2-6x+5 = (2a)^2-6(2a)+5 = 4a^2-12a+5 = 4a^2-12a+4+1 = 2(2a^2-6a+2)+1.$$

Therefore, $x^2 - 6x + 5 = 2b + 1$, where $b = 2a^2 - 6a + 2$. Thus $x^2 - 6x + 5$ is not odd, and so it must be even.

If we were to prove the above directly, we would begin by assuming $x^2 - 6x + 5$ is even, so $x^2 - 6x + 5 = 2a$. But then it is not clear where to proceed, since we would need to isolate x from the quadratic equation. But with the contrapositive, the proof reduces to a calculation.

Remember that when negating a statement you may need to use DeMorgan's law.

Example 1.9. Suppose $x, y \in \mathbb{Z}$. If $5 \nmid xy$, then $\nmid x$ and $5 \nmid y$.

Suppose it is not true that $5 \nmid x$ **and** $5 \nmid y$. Then $5|x$ **or** $5|y$. Suppose $5|x$. Then $x = 5a$ for some integer a and then $xy = (5a)y$ and so 5 divides xy. Similarly if 5 divides y then $y = 5a$ for an integer a and then $xy = x(5a)$ and we see that 5 divides xy.

Example 1.10. For $n > 2$, if n is prime then n is odd.

This seems obvious, but without the contrapositive it is not at all clear how to prove it directly. The contrapositive is, "for $n > 2$, if n is not odd then it is not prime" which is easy to prove. Indeed, if n is not odd then it is even and so 2 divides n, which shows it is not prime.

It is often useful to use the contrapositive to turn non-equalities into equalities.

Example 1.11. If $x^2 \neq x$ then $x \neq 1$.

We prove the contrapositive: if $x = 1$ then $x^2 = x$. Since $1^2 = 1$ we are done.

Remark 3. The last two examples exhibit a general strategy. In both of the statements (n is prime and $x^2 \neq x$) we are given some amount of information, but both are hard to work with. "n is prime" tells us that, of the $n-2$ integers between 1 and n, none divide n. We only care about the statement "n is not divisible by 2," but one cannot choose from the other $n - 2$ integers unless we are explicitly given n. So the contrapositive is good at avoiding situations where you have a lot of information, but little of it is useful.

Meanwhile, the statement $x^2 \neq x$ does not really give us anything to begin proving things with. It is generally good to convert non-equalities like this into proofs by contradiction or contrapositive, where they may result in a simple calculation.

Remark 4. Later in your mathematics education you will encounter statements similar to Example 1.12 in the following sense. We often define mathematical properties as things they are not. For example, an *infinite set* is one that is not finite. An *irrational* real number is one that is not rational (expressed as $\frac{n}{m}$ for integers n, m). For those in linear algebra, a set of vectors is *linearly independent* if it is not linearly dependent.

In these cases, one will often want to use the contrapositive or contradiction to turn these "not" statements into "is" statements. This is exactly what we did while proving $\sqrt{2}$ to be irrational.

1.3.1 Exercises

1. Let $x \in \mathbb{Z}$. Show that if $7x + 9$ is even, then x is odd.
2. (★) Prove the following: for any integers x and y, $x + y \geq 15$ implies $x \geq 8$ or $y \geq 8$.
3. (★) Show that if $n = xy$ for x, y positive integers, then $x \leq \sqrt{n}$ or $y \leq \sqrt{n}$.
4. Suppose $x, y \in \mathbb{R}$. Show that if $y^3 + yx^2 \leq x^3 + xy^2$, then $y \leq x$. (Hint: $(y - x)(x^2 + y^2) = yx^2 + y^3 - x^3 - xy^2$).
5. Show that if x and y are real numbers such that xy is irrational, then either x or y must be an irrational number.
6. Show that if x, y, z are integers and $x^2 + y^2 = z^2$, then at least one of x, y or z must be even.
7. Let x be an integer. Show that $3x + 2$ is odd if and only if $9x + 5$ is even.