2-23-2020

Proof by Contradiction

To prove a statement P **by contradiction**, you assume the *negation* $\neg P$ of what you want to prove and try to derive a *contradiction* (usually a statement of the form $A \wedge \neg A$). Since a contradiction is always false, your assumption $\neg P$ must be false, so the original statement P must be true.

Example. Premises: $\begin{cases} (\neg B \vee C) \to A \\ B \to D \\ C \vee \neg D \end{cases}$

Prove: A.

Since I want to prove A by contradiction, I begin by assuming the negation $\neg A$. I'm trying to construct a contradiction of the form FOO $\wedge$ $\neg$FOO.

1.	$(\neg B \vee C) \to A$	Premise
2.	$B \to D$	Premise
3.	$C \vee \neg D$	Premise
4.	$\neg A$	Premise - proof by contradiction
5.	$\neg(\neg B \vee C)$	Modus tollens (1, 4)
6.	$B \wedge \neg C$	DeMorgan (5)
7.	B	Decomposing a conjunction (6)
8.	$\neg C$	Decomposing a conjunction (6)
9.	D	Modus ponens (2, 7)
10.	C	Disjunctive syllogism (3, 9)
11.	$C \wedge \neg C$	Constructing a conjunction (8, 10)
12.	A	Proof by contradiction (4, 11)

I arrived at the contradiction $C \wedge \neg C$ at line 11. Therefore, I conclude that my premise $\neg A$ was false, so A must be true (line 12). □

In the next example, I'll look at Euclid's proof that there are infinitely many prime numbers; it occurs in Book IX of Euclid's *Elements*, which was composed around 300 B.C. and is arguably the most famous math textbook of all time.

Example. Prove that there are infinitely many prime numbers. (An integer $n > 1$ is **prime** if its only positive divisors are 1 and n.)

Suppose that there are *not* infinitely many prime numbers. That means there are finitely many prime numbers — suppose they are

$$p_1, \quad p_2, \quad \ldots, \quad p_n.$$

Look at the number

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

(It's the product of all of the p's, plus one. Notice that the product of the p's wouldn't make sense if there were infinitely many p's.)

x leaves a remainder of 1 when it's divided by p_1, since p_1 divides evenly into the $p_1 p_2 \cdots p_n$ term. Likewise, x leaves a remainder of 1 when it's divided by p_2, …, p_n. Therefore, x is not divisible by any of the p's — that is, x is not divisible by any prime number.

However, every integer greater than 1 is divisible by some prime number. A precise proof of this fact requires **induction**, which I'll discuss later. But you can see that it's reasonable. If a number z is prime, it's divisible by a prime, namely z. Otherwise, you can factor z into a product of two smaller numbers. If either factor is prime, then the prime factor is a prime which divides z. If neither factor of z is prime, you can factor them, and so on. Eventually, the process must stop, because the factors always get smaller.

Returning to my proof, I've found that x isn't divisible by any prime number, which I've just noted is impossible. This contradiction shows that there must be infinitely many prime numbers. □

Example. Prove that the following system of equations has no real solutions:

$$x^2 - 10 + e^y = 0 \quad \text{and} \quad \sin y - 10x + 37 = 0.$$

Suppose there is a real solution (x, y), so that

$$x^2 - 10 + e^y = 0 \quad \text{and} \quad \sin y - 10x + 37 = 0.$$

Add the equations, and complete the square in x:

$$\begin{aligned} x^2 - 10 + e^y + \sin y - 10x + 37 &= 0 \\ (x-5)^2 + e^y + \sin y + 2 &= 0 \end{aligned}$$

Now squares are nonnegative, so

$$(x-5)^2 \geq 0.$$

Also, $e^y > 0$.
In addition,

$$\begin{aligned} \sin y &\geq -1 \\ \sin y + 2 &\geq 1 \end{aligned}$$

Therefore,

$$(x-5)^2 + e^y + \sin y + 2 > 0 + 0 + 1 = 1.$$

So $(x-5)^2 + e^y + \sin y + 2 \neq 0$. This contradiction shows that the original system has no solutions. □

The next example is another "classical" result. The discovery that there are quantities which can't be expressed in terms of whole numbers or their ratios was known to the ancient Greeks; Boyer and Mertzbach [1] place the discovery prior to 410 B.C.

Example. Prove that $\sqrt{2}$ is irrational. (A **rational number** is a real number which can be written in the form $\frac{m}{n}$, where m and n are integers. A real number which is not rational is **irrational**.)

Suppose on the contrary that $\sqrt{2}$ is rational. Then I can write $\sqrt{2} = \frac{m}{n}$, where $m, n \in \mathbb{Z}$. (Remember that $\mathbb{Z}$ stands for the set of integers.) By dividing out any common factors, I can assume that $\frac{m}{n}$ is in lowest terms (that is, m and n have no common factors besides 1 and -1).

Clear the denominator, then square both sides:

$$\sqrt{2}n = m, \quad 2n^2 = m^2.$$

Since 2 divides the left side, it must divide the right side. But if 2 divides m^2, it must in fact divide m. So suppose $m = 2k$, where $k \in \mathbb{Z}$. Substitute in the previous equation and cancel a factor of 2:

$$2n^2 = (2k)^2 = 4k^2, \quad n^2 = 2k^2.$$

Now 2 divides the right side, so it must divide the left side. But if 2 divides n^2, it must divide n.

However, I already showed that 2 divides m, so 2 divides both m and n. This contradicts my assumption that the fraction $\frac{m}{n}$ was in lowest terms.

Therefore, $\sqrt{2}$ must be irrational. □

The preceding examples give situations in which proof by contradiction *might* be useful:

A proof by contradiction might be useful if the statement of a theorem is a **negation** — for example, the theorem says that a certain thing *doesn't* exist, that an object *doesn't* have a certain property, or that something *can't* happen. In these cases, when you assume the contrary, you negate the original negative statement and get a positive statement, which gives you something to work with.

Having said this, I should note that *it is considered bad style to write a proof by contradiction when you can give a direct proof.* In those situations, the proof by contradiction often looks awkward. Moreover, the direct proof will often tell you more. For example, a direct proof that something exists will often work by *constructing* the object. This is better than simply *knowing* that the object exists on logical grounds.

In some cases, proof by contradiction is used as part of a larger proof — for instance, to eliminate certain possibilities.

Example. Prove that the function $f(x) = x^5 + 6x^3 + 17x + 1$ cannot have more than one root.

In this proof, I'll use **Rolle's Theorem**, which says: If f is continuous on the interval $[a, b]$, differentiable on the interval (a, b), and $f(a) = f(b)$, then $f'(c) = 0$ for some $c \in (a, b)$.

Suppose on the contrary that $f(x) = x^5 + 6x^3 + 17x + 1$ has more than one root. Then f has at least two roots. Suppose that a and b are (different) roots of f with $a < b$.

Since f is a polynomial, it is continuous and differentiable for all x. Since a and b are roots, I have

$$f(a) = 0 \quad \text{and} \quad f(b) = 0, \quad \text{so} \quad f(a) = f(b).$$

By Rolle's Theorem, $f'(c) = 0$ for some c such that $a < c < b$.

However,

$$f'(x) = 5x^4 + 18x^2 + 17.$$

Since $f'(x)$ is a sum of even powers and a positive number (17), it follows that $f'(x) > 0$ for all x. This contradicts $f'(c) = 0$.

Therefore, f does not have more than one root.

Note: You could use the Intermediate Value Theorem to show that $f(x)$ has at least one root. Combined with the result I just proved, this shows that $f(x)$ has **exactly** one root. □

Example. On a certain island, each inhabitant always lies or always tells the truth. Calvin and Phoebe live on the island.

Calvin says: "Exactly one of us is lying."

Phoebe says: "Calvin is telling the truth."

Determine who is telling the truth and who is lying.

Suppose Calvin is a truth teller. Then "Exactly one of us is lying" is true, and since Calvin is a truth teller, Phoebe is a liar. Therefore, "Calvin is telling the truth" is a lie, so Calvin must be lying. This is a contradiction, because I assumed he was telling the truth.

Hence, I've proved by contradiction that Calvin must be a liar. Hence, "Exactly one of us is lying" is false. This gives two possibilities: Either both are telling the truth, or both are lying.

Suppose both are telling the truth. This contradicts the fact that Calvin is lying.

The only other possibility is that both are lying. Then Calvin's statement "Exactly one of us is lying" should be false (and it is), and Phoebe's statement "Calvin is telling the truth" should be false (and it is). Thus, this is the only possibility, *and* it's consistent with the given statements.

Therefore, Calvin and Phoebe are both liars. □

---

[1] Carl Boyer, *A History of Mathematics* (2^{nd} edition) (revised by Uta Merzbach), New York: John Wiley & Sons, Inc., 1991.