MATH 135 — Fall 2021
Sample Proofs from Lecture 9

Mark Girard

September 27, 2021

Proof by Contradiction

- Given a statement A, ***exactly one*** of A and $\neg A$ is true.
- A *contradiction* is a statement of the form:

$$A \wedge \neg A. \tag{$*$}$$

  A statement of the form in $(*)$ must be false!

- If you make an assumption in a proof, and using logical reasoning you are able to use that assumption to arrive at a contradiction of the form $A \wedge \neg A$, then your original assumption must have been wrong!

To prove a statement P by contradiction:

1. Suppose instead that P is false (i.e., that $\neg P$ is true).
2. Use the assumption that $\neg P$ is true to arrive at a contradiction of the form $A \wedge \neg A$.
3. Conclude that the assumption that P is false must have been wrong.
4. This proves that P is true.

Example

Claim. $\forall a, b \in \mathbb{Z},\ a \geq 2 \implies (a \nmid b \text{ or } a \nmid (b+1))$.

In words, this says that "No integer greater than one can divide two successive integers."

Proof. Let a and b be integers and assume that $a \geq 2$. [We will prove that either $a \nmid b$ or $a \mid (b+1)$.] For the sake of deriving a contradiction, suppose instead that $a \mid b$ and $a \nmid (b+1)$. Then there exist integers m and n such that

$$b = am \quad \text{and} \quad b + 1 = an.$$

Then $am = b = an - 1$ and thus $a(n - m) = 1$, which implies that $a \mid 1$, as $n - m$ is an integer. Because the only integers that divide 1 are 1 and -1, this implies that either $a = 1$ or $a = -1$ and thus $a < 2$ in either case. We conclude that both

$$a \geq 2 \quad \text{and} \quad a < 2,$$

which is a contradiction. Thus the assumption that $a \mid b$ and $a \mid (b + 1)$ is false. Hence it must be the case that either $a \nmid b$ or $a \nmid (b + 1)$. This completes the proof. □

Note that the proof of the above claim is essentially equivalent to proving by contrapositive. Either method is fine here.

Proof of irrationality of $\sqrt{2}$

Here is an example of a proof by contradiction that *cannot* be redone as a proof by contrapositive.

Claim. $\sqrt{2}$ *is irrational*

Proof. Towards a contradiction, suppose instead that $\sqrt{2}$ were rational. Then there exist integers a and b having no common divisors (other than 1 and -1) such that $b \neq 0$ and

$$\sqrt{2} = \frac{a}{b}. \tag{1}$$

As we may suppose that a and b are reduced and have no common factors, we may conclude that they are not both even. (Otherwise, we would have that $2 \mid a$ and $2 \mid b$, which would mean that a and b share 2 as a common factor.) Squaring both sides of (1) and rearranging, we find that

$$2b^2 = a^2$$

and thus a^2 is even, which implies that a is even. Hence there is an integer k such that $a = 2k$. Now

$$2b^2 = (2k)^2 = 4k^2$$

and thus $b^2 = 2k^2$, which implies that b^2 is also even and thus b is even. We conclude that both a and b are even, which contradicts the statement that a and b are chosen such that they have no common factors. Hence, the assumption that $\sqrt{2}$ is rational is false. It follows that $\sqrt{2}$ must be irrational. □

Another example

Claim. *For all real numbers x, if $x > 0$ then $x + \frac{1}{x} \geq 2$.*

Proof. Let x be a real number ans suppose that $x > 0$. Suppose for the sake of obtaining a contradiction that

$$x + \frac{1}{x} < 2.$$

Multiplying both sides by x and rearranging yields

$$x^2 - 2x + 1 < 0$$

or equivalently $(x-1)^2 < 0$. But the square of every real number is non-negative, so it is also the case that $(x-1)^2 \geq 0$. Hence we conclude that both

$$(x-1)^2 < 0 \qquad \text{and} \qquad (x-1)^2 \geq 0$$

are true, which is a contradiction. Therefore our assumption that $x + \frac{1}{x} < 2$ is false, which proves that $x + \frac{1}{x} \geq 2$, as desired. □

Proving uniqueness

To prove a statement of the form:

"There exists a unique $x \in S$ such that $P(x)$ is true"

we must prove two things:

(i) Prove there exists at least one $x \in S$ such that $P(x)$ is true.

(ii) Prove that, if $y \in S$ is another element such that $P(y)$ is true, then it must be that $y = x$.

Symbolically, these two statements are:

(i) $\exists x \in S,\ P(x)$.

(ii) $\forall y \in S,\ P(y) \implies (y = x)$.

Example

Claim. *For every odd integer a, there exists a unique integer k such that $a = 2k+1$.*

Proof. Let a be an odd integer. By definition, there exists an integer k such that $a = 2k+1$. Suppose now that m is another integer such that $a = 2m+1$. Then

$$2k + 1 = 2m + 1$$

which implies that $k = m$. Thus, k is the unique integer satisfying this claim. □