How to Prove Things

Brent Yorgey

February 15, 2023

Just follow these two easy steps!

1. Translate the statement into propositional logic (using $\wedge$, $\vee$, $\neg$, $\rightarrow$, $\forall$, and $\exists$).
2. Use a proof method/template appropriate to the outermost logical connective. Repeat as necessary, nesting proof templates within each other.

Conjunction (AND): $p \wedge q$

To prove a conjunction $p \wedge q$, prove p and prove q.

> We must show $p \wedge q$, which we will do by proving them each separately.
>
> - [proof of p]
> - [proof of q]
>
> Therefore, since we have proved p and q separately, we have proved their conjunction.

Disjunction (OR): $p \vee q$

To prove a disjunction $p \vee q$, you can do *any* of the following:

1. Prove p.

   > We must show $p \vee q$, which we will do by showing that in fact p holds.
   >
   > - [proof of p]
   >
   > Therefore, $p \vee q$ is true, since we have proved the left side.

2. Prove q. (Similar to the above example.)
3. Use a proof by contradiction.

   > We must show $p \vee q$. For the purpose of obtaining a contradiction, let us suppose the opposite, that is, $\neg p \wedge \neg q$.
   >
   > - [derive a contradiction]

Therefore, since the assumption that $p \vee q$ is false led to a contradiction, we conclude that it must be true.

Implication: $p \to q$

To prove an implication, $p \to q$, you can do one of the following:

1. *Suppose* p is true, then prove q. (You will sometimes hear this called a *direct proof*, but the name does not matter.)

   Suppose p. Then we must show q.

   - [proof of q, making use of the fact that p is true.]

   Therefore, since we proved q under the supposition p, therefore $p \to q$ is true.

2. Prove the *contrapositive*, that is, prove $\neg q \to \neg p$, which is logically equivalent.

   To prove $p \to q$, we will prove the contrapositive, that is, $\neg q \to \neg p$.

   - [proof of $\neg q \to \neg p$]

   Since we have shown that $\neg q \to \neg p$, therefore $p \to q$ also.

3. Use a proof by contradiction.

   We must show $p \to q$. For the purpose of obtaining a contradiction, let us suppose the opposite, that is, $p \wedge \neg q$.

   - [derive a contradiction]

   Therefore, since the assumption that $p \to q$ is false led to a contradiction, we conclude that it must be true.

Biconditional: $p \leftrightarrow q$

To prove an if and only if, $p \leftrightarrow q$, prove $(p \to q) \wedge (q \to p)$.

To prove $p \leftrightarrow q$, we will prove both directions.

- $(\to)$ [proof of $p \to q$]
- $(\leftarrow)$ [proof of $q \to p$]

Since we have shown $p \to q$ and $q \to p$, therefore $p \leftrightarrow q$.

Negation: $\neg p$

To prove a negation $\neg p$:

1. Use De Morgan laws to "push the negation inwards", then use one of the other proof rules. For example, if you wanted to prove something of the form $\neg(p \wedge q)$, first use a De Morgan law to transform this into $\neg p \vee \neg q$; then use one of the methods listed above for proving a disjunction.

2. Use a proof by contradiction, that is, prove $p \to \mathsf{F}$.

   > We must show $\neg p$. For the purpose of obtaining a contradiction, let us suppose the opposite, that is, p.
   >
   > - [derive a contradiction]
   >
   > Therefore, since the assumption that p is true led to a contradiction, we conclude that it must be false.

Universal quantifier: $\forall x\!:\!D.\ P(x)$

To prove a "universally quantified" statement $\forall x\!:\!D.\ P(x)$, you can do one of the following:

1. Let d stand for an *arbitrary* element of the domain D, and prove $P(d)$. *Arbitrary* means we don't assume *anything* about d except the fact that it is in the domain D. This means that the same proof will work for every single element in D.

   > Let d be an arbitrary D; we must show $P(d)$.
   >
   > - [proof of $P(d)$]
   >
   > Therefore, since d was arbitrary, in fact $\forall x\!:\!D.\ P(x)$.

2. Use induction.

Warning: note it is common practice to reuse the same variable name x instead of creating a new name d.

Existential quantifier: $\exists x\!:\!D.\ P(x)$

To prove an "existentially quantified" statement $\exists x : D.\ P(x)$:

1. Pick a specific d (a "witness") in the domain D and prove $P(d)$.

   > To show $\exists x\!:\!D.\ P(x)$, we will in fact show that this is true specifically for d.
   >
   > - [proof of $P(d)$]

Since we have shown $P(d)$, and d is an element of D, therefore $\exists x : D.\ P(x)$.

2. Use a proof by contradiction.

We must show $\exists x : D.\ P(x)$. For the purpose of obtaining a contradiction, let us suppose the opposite, that is, $\forall x : D.\ \neg P(x)$.

- [derive a contradiction]

Therefore, since the assumption that $\exists x : D.\ P(x)$ is false led to a contradiction, we conclude that it must be true.

Examples

Example. if n is an odd integer, then n^2 is also odd. Translation:

$$\forall n : \mathbb{Z}.\ \mathrm{Odd}(n) \to \mathrm{Odd}(n^2).$$

Proof. To show $\forall n : \mathbb{Z}.\ \mathrm{Odd}(n) \to \mathrm{Odd}(n^2)$, let k be an arbitrary integer; then we must show that $\mathrm{Odd}(k) \to \mathrm{Odd}(k^2)$.

- To show $\mathrm{Odd}(k) \to \mathrm{Odd}(k^2)$, suppose $\mathrm{Odd}(k)$ is true, that is, there exists an integer j such that $k = 2j + 1$. Then we must show that $\mathrm{Odd}(k^2)$ is true, that is, there exists an integer p such that $k^2 = 2p + 1$.
  - $k^2 = (2j+1)^2 = 4j^2 + 4j + 1 = 2(2j^2 + 2j) + 1$, so we can pick $p = 2j^2 + 2j$, which is an integer since k is an integer.

  Therefore, $\mathrm{Odd}(k) \to \mathrm{Odd}(k^2)$.

Therefore, since k was arbitrary, $\mathrm{Odd}(n) \to \mathrm{Odd}(n^2)$ for all integers n. □

Example. If n is an integer and $3n + 2$ is odd, then n is odd. Translation:

$$\forall n : \mathbb{Z}.\ \mathrm{Odd}(3n+2) \to \mathrm{Odd}(n)$$

Proof. Let m be an arbitrary integer; we must show $\mathrm{Odd}(3m+2) \to \mathrm{Odd}(m)$.

- We will do this by showing the contrapositive, $\neg\mathrm{Odd}(m) \to \neg\mathrm{Odd}(3m+2)$, that is, $\mathrm{Even}(m) \to \mathrm{Even}(3m+2)$.
  - So suppose $\mathrm{Even}(m)$, that is, there exists an integer k such that $m = 2k$. We must show $\mathrm{Even}(3m+2)$, that is, $3m + 2 = 2j$ for some integer j.

Note that it is actually not obvious from the definitions that $\neg\mathrm{Odd}(m) \equiv \mathrm{Even}(m)$! But we will assume it for now. See the discussion following the next example.

  * We calculate as follows: $3m + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$. Thus, $j = 3k + 1$ is the desired integer such that $3m + 2 = 2j$, so $\text{Even}(3m + 2)$.

  Thus, since we were able to show $\text{Even}(3m + 2)$ under the supposition that $\text{Even}(m)$, therefore $\text{Even}(m) \to \text{Even}(3m + 2)$.

Therefore, the contrapositive $\text{Odd}(3m + 2) \to \text{Odd}(m)$ is also true.

Since m was an arbitrary integer, this shows that $\forall n : \mathbb{Z}.\ \text{Odd}(3m + 2) \to \text{Odd}(m)$. □

Example. Every odd integer is not even. Translation:

$$\forall n : \mathbb{Z}.\ \text{Odd}(n) \to \neg\,\text{Even}(n).$$

Note that this may seem obvious, but since we have defined $\text{Even}(n) = \exists k : \mathbb{Z}.\ n = 2k$ and $\text{Odd}(n) = \exists k : \mathbb{Z}.\ n = 2k + 1$, the fact that they are negations of each other does not follow automatically from the definitions.

Proof. Let n be an arbitrary integer; we must show $\text{Odd}(n) \to \neg\,\text{Even}(n)$.

- Suppose $\text{Odd}(n)$, that is, there exists some integer k such that $n = 2k + 1$. We must show $\neg\,\text{Even}(n)$.

  – For the purpose of obtaining a contradiction, suppose otherwise, that is, suppose $\text{Even}(n)$, which means $n = 2j$ for some integer j.

    * We now have $n = 2k + 1$ and $n = 2j$. Hence $2k + 1 = 2j$. Solving for j, we get $j = k + 1/2$, but this is impossible: we assumed that j and k are both integers, and adding $1/2$ to an integer can never yield another integer.

    Since the assumption of $\text{Even}(n)$ led to a contradiction, in fact we must have $\neg\,\text{Even}(n)$.

  Since we have shown $\neg\,\text{Even}(n)$ under the assumption of $\text{Odd}(n)$, therefore $\text{Odd}(n) \to \neg\,\text{Even}(n)$.

Therefore, since n was arbitrary, we conclude that every odd integer is not even. □

Note that proving the converse, $\forall n : \mathbb{Z}.\ \neg\,\text{Odd}(n) \to \text{Even}(n)$, is more difficult. It follows from the fact that $\forall n : \mathbb{Z}.\ \text{Even}(n) \vee \text{Odd}(n)$, but proving this fact requires the Division Algorithm.