

## 0.2 The Art and Science of Proof

*I don't think groove is a gift, it's a combination of learnable skills.*  
~ Benny Greb

Now that we are comfortable with the formal system by which logical statements are built, we can construct a theory of proof techniques. This is equal parts art and science, requiring as much precision and honest interrogation of your core curiosity as it does a poet's bizarre and far-reaching dreams or simple artistic dumb luck in the name of inspiration and originality. We will begin with the least tricky of the proof techniques. Our discussion in this section will remain mostly informal to avoid need for a theory of types.

**Definition 0.23** (Direct Proof). Let  $P$  be a hypothesis and  $Q$  a conclusion. A direct proof of  $P \implies Q$  is a chain of implications  $P \implies R_1, R_1 \implies R_2, \dots, R_k \implies Q$ , such that each implication in the chain follows from the definitions and prior knowledge. It is permissible for intermediate statements  $R_i$  to depend on  $P$  or any  $R_j : j < i$ .

*Example 0.24.* Let  $n$  be an integer. Then, the sum of consecutive integers  $n, n+1, n+2$  is a multiple of three. We may prove this directly.


*Proof.* We have  $n + (n + 1) + (n + 2) = 3n + 3 = 3(n + 1)$ . 

In this example,  $P$  is the statement that  $n$  is an integer.  $R_1$  is the statement that the sum works out to  $3n + 3$ , accomplished by our prior understanding of commutativity and collection of like terms.  $R_1 \implies R_2$  is the distributive property.  $R_2 \implies Q$  is accomplished via the definition of “multiple of three.”

*Example 0.25.* Let  $m, n$  be odd integers. Then,  $nm$  is odd.

*Proof.* Since  $n, m$  are odd, we may write  $n = 2k + 1, m = 2\ell + 1$  for integers  $k, \ell$ . Thus,

$$nm = (2k + 1)(2\ell + 1) = 4k\ell + 2k + 2\ell + 1 = 2(2k\ell + k + \ell) + 1.$$

This is equal to one plus a multiple of two as an integer, so we see it satisfies the definition of an odd number. 


Related to this idea is the idea of proof by contrapositive. Since a contrapositive is equivalent to an implication, this does not require anything new. Sometimes it is easier to think in terms of the contrapositive than a statement itself.

**Definition 0.26** (Proof by Contrapositive). A proof by contrapositive of  $P \implies Q$  is a proof of  $\neg Q \implies \neg P$ , either directly or by other techniques or means. Since an implication and its contrapositive are equivalent, this is equivalent to a proof of the statement.

*Example 0.27.* If  $n$  is an integer such that  $n^2$  is odd, then  $n$  is odd.

*Proof.* We will show that if  $n$  is even, then  $n^2$  is even. Write  $n = 2k$  for some  $k \in \mathbb{Z}$ , and compute

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

with  $2k^2 \in \mathbb{Z}$ . 

*Example 0.28.* If  $p^2q$  is irrational, then  $p$  is irrational or  $q$  is irrational.

*Proof.* Contrapositively, we will prove that if  $p, q$  are both rational, then so is  $p^2q$ . Write  $p = \frac{m}{n}$ ,  $q = \frac{k}{\ell}$  for integers  $m, k, n, \ell$  with  $n, \ell > 0$ . Then,  $p^2q = \frac{m^2k}{n^2\ell}$ , which is clearly a rational since the product of integers is an integer, and in particular the denominator is a product of positive integers so is a positive integer. ♣

We take this example one layer further with our next technique, the proof by contradiction, a mathematician's *reductio ad absurdum*.

**Definition 0.29** (Proof by Contradiction). A proof by contradiction of a statement  $S$  is a proof of the implication  $\neg S \implies C$ , where  $C$  is a contradiction.

Before we see this in an example, we should verify the equivalence  $S \iff (\neg S \implies C)$ .

**Theorem 0.3** (Proof by Contradiction). Let  $S$  be a statement and  $C$  a contradiction. Then,  $S \iff (\neg S \implies C)$ .

*Proof.* Consider the truth table

$S$	$\neg S$	$\neg S \implies C$
F	T	F
F	T	F
T	F	T
T	F	T

Here, we used the fact that the only true implication concluding “False” is “False  $\implies$  False”. ♣

Let us continue that prior example about  $p^2q$ .

*Example 0.30.* Let  $p^2q$  be irrational for some rational  $p$ . Then,  $q$  is irrational.

*Proof.* By way of contradiction, we assume the negation holds. Let  $p^2q$  be irrational with  $p, q$  rational. Writing  $p = \frac{m}{n}$ ,  $q = \frac{k}{\ell}$  as before, we see that  $p^2q = \frac{m^2k}{n^2\ell}$  is rational. This implies  $p^2q$  is irrational (we assumed it) and  $p^2q$  is rational (we derived it), and this is a contradiction. ♣

Back to working with integers, sometimes it is helpful to find mutually exclusive, exhaustive cases to wield more control over some feature of our hypothesis or proof. Then, each individual case is easier than the whole problem, to be addressed one after the other before concluding. Consider the following example.

*Example 0.31.* If  $n$  is an integer, then  $n(n+1)$  is an even integer.

*Proof.* There are two cases to consider, as  $n$  could be odd or even. First, we will take  $n$  to be even. Then, we may write  $n = 2k$  for some integer  $k$ , and conclude  $n(n+1) = 2k(2k+1) = 2(2k^2+k)$  is even. Then, we assume  $n$  is odd. In this case, we write  $n = 2k+1$  and find  $n(n+1) = (2k+1)(2k+1+1) = (2k+2)(2k+1) = 2(k+2)(2k+1)$  which is even since  $(k+2)(2k+1)$  is an integer. ♣

In some instances, two or more cases will have essentially the same proof, up to some relabeling. Usually, we like to preserve time, ink, and sanity by writing the case once, no matter the symbols, and say “without loss of generality” we have done so.

*Example 0.32.* If  $n$  is even or  $m$  is even, then  $n \cdot m$  is even.

*Proof.* Without loss of generality, suppose  $n$  is even. Write  $n = 2k$  for some integer  $k$ , and conclude  $n \cdot m = 2k \cdot m = 2 \cdot km$  is an even integer. ♣

What we have done is condense the  $m$  even case to be included in the  $n$  even case, since they look the same and ultimately this means the *ideas* are the same.

**Exercise 0.33.** Prove the following equivalences. (future me: 09/07 323), excluding some contained above.

We conclude this exploration of proof techniques with a powerful method known as induction.

**Definition 0.34** (Proof by Induction). Let  $P_n$  be a logical statement involving a parameter  $n$ , for each  $n \in \mathbb{N}$ . A proof by induction for  $P_n$  for all  $n \in \mathbb{N}$  involves a proof of  $P_0$  and a proof of the implication  $P_k \implies P_{k+1}$  for all  $k \in \mathbb{N}$ .

Our next theorem will verify this technique is sound. It will make use of the following property of the natural numbers.

**Proposition 0.4** (Well-Ordering Principle). *The natural numbers  $\mathbb{N}$  are well-ordered, i.e. every nonempty set of natural numbers has a least element.*

*Proof.* Note the natural numbers has a least element, 0. Let  $S$  be a nonempty subset of  $\mathbb{N}$ . That is,  $S$  is a set of natural numbers, and there is at least some natural number in  $S$ . By way of contradiction, suppose  $S$  has no least element. Then,  $0 \notin S$ , as this is a least element for  $\mathbb{N}$  so would be for  $S$  also. Let  $s$  be any element of  $S$ , which exists, as  $S$  is not empty. If, for all other elements  $x \in S$ ,  $m < x$ , then we have found our contradiction, as this would make  $m$  a least element. Otherwise, take  $j = 1$ . If  $1 \in S$ , it must be a least element since  $0 \notin S$ , giving us a contradiction. So we consider  $j = 2$ . If  $2 \in S$ , following our demonstration that  $0, 1 \notin S$ , then 2 is a least element. Proceeding in this fashion, for any natural  $j$ ;  $2 < j < m$ , we have shown  $0, 1, \dots, j-2, j-1 \notin S$ , in which case  $j$  cannot, within the bounds of our assumption  $S$  has no least element, be an element of  $S$ . This process terminates by finiteness of  $m$ , forcing  $0, 1, 2, \dots, m-2, m-1 \notin S$  such that  $m$  is a least element of  $S$ . ♣

**Theorem 0.5** (Induction). *Let  $P_n$  be a logical statement involving a parameter  $n$ , for each  $n \in \mathbb{N}$ . Assume  $P_0$  is true and we have  $P_k \implies P_{k+1}$  for all  $k \in \mathbb{N}$ . Then,  $P_n$  is true for all  $n \in \mathbb{N}$ .*

*Proof.* We will show that there is no least  $n$  for which  $P_n$  is false, concluding the set of false statements in this family is empty, which holds iff they are all true. So, take  $x \in \mathbb{N}$  to be the least value such that  $P_n$  is false.  $P_0$  is true. Thus,  $x \notin 0$ . More specifically,  $x > 0$ . Thus,  $x-1 \in \mathbb{N}$ . And,  $P_{x-1}$  must be false, because if it were true and  $P_{x-1} \implies P_x$ , then  $P_x$  is true. But this contradicts our assumption  $x = n$  is the least value for which  $P_n$  is false. ♣