6 Proofs

6.1 Direct Proof

In an ideal world, a direct proof is a “sequence of statements each of which is a hypothesis, a fact, or inferred from previous statements using valid rules of inference.”

Consider for example, a standard introductory exercise: “Prove that the square of an even integer is even.” First, note that math-speak often omits an implied “every”. What this exercise is really saying is: “Prove that the square of every even integer is even.” Second, note that the task can be recast as a conditional statement: “Prove that if you have an even integer then its square is even”. To prove a conditional, one assumes the hypothesis and attempts to infer the conclusion.

We also need the principle of “universal generalization”: If one can prove statement about $x$ by assuming only that $x$ is a member of some universe, then one can conclude the statement is true for every member of that universe.

We can now try a proof. But we still need to know the definition of an even integer. For this chapter, we will define an integer $m$ as even if it is equal to $2i$ for some integer $i$, and define $m$ as odd if it is equal to $2i+1$ for some integer $i$.

Example 6.1. Prove that the square of an even integer is even.

Let $x$ be an even integer. Then there is an integer $i$ such that $x = 2i$. Thus $x^2 = (2i)^2 = 4i^2 = 2 \times (2i^2)$. Note that $2i^2$ is an integer. It follows that $x^2$ is two times an integer and is therefore even.

(Of course, it is admittedly artificial that one knows the properties of integers but has to prove the properties of even-ness...) Here is a similar example.

Example 6.2. Prove that the sum of two odd integers is even.

Let $m$ and $n$ be odd integers. Then there are integers $i$ and $j$ such that $m = 2i + 1$ and $n = 2j + 1$. This means that $m + n = (2i + 1) + (2j + 1) = 2(i + j + 1)$. Thus $m + n$ is two times an integer and is therefore even. Thus by universal generalization, the sum of any two even integers is even.

▶ For you to do! ◀

1. Prove that if $x^2 - 1$ is a multiple of 3, then $x$ is not a multiple of 3.
6.2 Disproofs and Counterexamples

To prove a statement such as “all roses are red”, one needs a proof that works for all roses. To prove a statement is false, one needs only one case where it fails: one rose that is not red. This is called a counterexample. For example, suppose the claim is that “All primes are odd”. But 2 is prime and even.

Example 6.3. Prove or disprove: For all real numbers $x$ and $y$ it holds that $|x + y| = |x| + |y|$.

Well, this statement is false. For a counterexample, let $x = 1$ and $y = -1$.

6.3 Proof by Contradiction

In a proof by contradiction, we suppose the negation of what we are trying to prove and try to reach a contradiction. If every step of the proof is valid, then the only possible reason for the contradiction is that the supposition is false.

For example, here is a famous proof by contradiction that $\sqrt{5}$ is not rational. (A number is rational if it can be expressed as the ratio of two integers.)

Example 6.4. Prove that $\sqrt{5}$ is irrational.

Suppose $\sqrt{5}$ is rational. Then

$$\sqrt{5} = \frac{m}{n}$$

for some integers $m$ and $n$. We can simplify the fraction so that $m$ and $n$ do not have a common factor. Now, $5 = \frac{m^2}{n^2}$ and thus $m^2 = 5n^2$. It follows that $m^2$ is a multiple of 5 and so $m$ is a multiple of 5. That is, $m = 5r$ for some integer $r$.

Then $m^2 = 25r^2$ and so $n^2 = 5r^2$. By the same reasoning, $n$ is a multiple of 5. Thus, $m$ and $n$ have a common factor (namely 5); this is a contradiction. Thus by the principle of proof by contradiction, $\sqrt{5}$ is not rational.

6.4 Valid Rules of Inference and Fallacies

In the proofs above we used deduction or inference. For example we used already the rule of inference called modus ponens:

**Modus ponens.** The rule of inference: “From $p$ and $p \Rightarrow q$, we may deduce $q$”
For example, assume we know that “all roses are red” and that “Pete is a rose”. It follows by modus ponens that “Pete is red”.

But how do we know that this rule is valid? Well, we can prove it.

A rule of inference consisting of statements $s_1, s_2, \ldots, s_n$ and assertion $q$ is valid if $s_1 \land s_2 \land \ldots \land s_n \Rightarrow q$ is a tautology.

Example 6.5. Modus ponens.

We need to show that the rule “From $p$ and $p \Rightarrow q$, we may deduce $q$” is valid. So we consider the compound statement:

$$p \land (p \Rightarrow q) \Rightarrow q$$

It is easy to check with a truth table that this is a tautology. Since this is a tautology, the argument is valid.

Example 6.6. Proof by contradiction.

Proof by contradiction is valid since the following is a tautology:

$$(\neg q \Rightarrow r \land \neg r) \Rightarrow q$$

A fallacy is an invalid argument which looks like it is a valid rule of inference.

Example 6.7. The following is a fallacy:

If Wayne likes computers, then Wayne is a nerd. Wayne is a nerd. Therefore, Wayne likes computers.

This has the form

$$(c \Rightarrow n) \land n \Rightarrow c$$

This statement is not a tautology: for example, it is false when $c$ is false and $n$ is true.
6.5 Predicates

We have seen statements that are either true or false. Often one has to deal with a more general situation where there are variables. For instance, in Example 6.7 we translated “Wayne like computers” as \( e \). Now, if we are faced with the statement about Rincewind instead of Wayne, we have to redo things. It would be better to have a generic form that handles both situations simultaneously. In programming language terminology, rather than dealing with boolean variables, we now want to deal with boolean functions.

A _predicate_ is what we need. For example, we might write \( \text{like}(\text{Wayne}, \text{computers}) \). Or we might write \( \text{likeComp}(\text{Wayne}) \), or even \( \text{emotion}(\text{Wayne}, \text{like}, \text{computers}) \). The exact choice of predicate depends on the situation and what seems appropriate at the time.

**Example 6.8.** Translate into predicates the argument: “If someone is a vegan then they have blue hair. Corin is a vegan. Therefore Corin has blue hair.”

If we have a predicate \( \text{has}(x, y) \) for “\( x \) has \( y \)” and \( \text{isa}(x, z) \) for “\( x \) is a \( z \)” , we can write this as

\[
\text{If } \text{isa}(x, \text{vegan}) \Rightarrow \text{has}(x, \text{blueHair}) \text{ and } \text{isa}(\text{Corin}, \text{vegan}), \text{ then } \text{has}(\text{Corin}, \text{blueHair}).
\]

Note that I chose these exact predicates; you might easily choose other predicates.

But the above argument is potentially ambiguous, because we have not captured the idea that this applies only to people, and not say to zebras. It is better to specify the universes involve, which we consider next.

6.6 Quantifiers

We can write multiple statements as one statement using **quantifiers**. For example, in English we might write “the square of any number is nonnegative” or “all diseases will be cured by someone eventually”. The quantifiers here are “any”, “all”, “someone” and “eventually” (if you think of this as “at some time”).

Mathematics uses the following notation:

- \( \forall \) for “for all”, called the **universal quantifier**;
- \( \exists \) for “there exists”, the **existential quantifier**.

We will put parentheses around the expression that is subject to quantification. So we might write:

\[
\forall m \ (m^2 \geq 0).
\]
However, it is unclear whether the statement is true. It is true if we are thinking of \( m \) being an integer, but false if we allow \( m \) to be a complex number (since \( i^2 = -1 \)). So we should really specify the universe (even though we often omit the universe if it is clear from context). Thus we write:

\[
\forall m \in \mathbb{Z} \,(m^2 \geq 0).
\]

The second example above, “all diseases will be cured by someone eventually”, might be written as

\[
\forall d \in \text{diseases} \,(\exists h \in \text{humans} \,(\exists t \in \text{time} \,(h \text{ cures } d \text{ at } t)))
\]

I agree that this gets cumbersome quickly; but the point is that this does allow us to write down things in mathematical notation (and also to feed things into a computer for automated reasoning).

**Example 6.9. “There is no odd number whose square is even”**

This can be written as

\[
\neg \exists x \in \mathbb{Z} \,(o(x) \land e(x^2))
\]

if we have predicates \( o(y) \) meaning \( y \) is odd and \( e(y) \) meaning \( y \) is even. Of course, we get different answers if we assume different predicates. (For example, we might define \( s(y) \) for the square of \( y \) is even, or even use \( \neg e(y) \) for being odd.)

**Example 6.10. Integer quotient and remainder**

We can express the existence of the quotient and remainder in integer division as “Given positive integer \( n \) and nonnegative integer \( m \), there exist nonnegative integers \( q \) and \( r \) (quotient and remainder) such that \( m = nq + r \) and \( r < n \). This can be written in math-speak as

\[
\forall n \in \mathbb{Z}^+ \,(\forall m \in \mathbb{N} \,(\exists q \in \mathbb{N} \,(\exists r \in \mathbb{N} \,(m = nq + r) \land (r < n))))
\]

(I wrote this slowly, so that you can read it slowly...)

There is an intimate connection between \( \forall \) and \( \exists \) (which generalizes de Morgan’s laws):

**Lemma 6.1** (a) The statement \( \neg \forall x(p(x)) \) is equivalent to \( \exists x(\neg p(x)) \).

(b) The statement \( \neg \exists x(p(x)) \) is equivalent to \( \forall x(\neg p(x)) \).

If we let \( p(x) \) stand for an arbitrary statement involving variable \( x \), then to show that \( \forall x(p(x)) \) is false, it is sufficient to find one \( x \) where \( p(x) \) is false (that is, a counterexample). Similarly, to show that \( \exists x(p(x)) \) is true, it is sufficient to find one \( x \) where \( p(x) \) is true.
We can also use predicates and quantifiers in definitions. In these, there is a “free variable”, meaning a variable that is not quantified. For example, to define an integer \( x \) as even we might say:

\[
x \text{ is even if } \exists y \in \mathbb{Z} (x = 2y).
\]

**Exercises**

6.1. Prove that the square of an even integer is a multiple of 4.

6.2. Show that the product of four consecutive integers is a multiple of 12.

6.3. Give a proof by contradiction that if \( x, y, z \) are integers such that \( xyz \leq 1000 \), then at least one of \( x, y, z \) is at most 10.

6.4. Give a **proof by contradiction** that for all real numbers \( x \), if \( x^2 - 2x \neq -1 \), then \( x \neq 1 \).

6.5. Use proof by contradiction to show that if \( x^2 + x - 2 = 0 \) then \( x \neq 0 \).

6.6. Celia has a square piece of paper with each side two feet. Prove that if she draws 11 crosses on this paper, then at least one pair of crosses must be less than one foot apart.

6.7. Let \( p \) be a prime number other than 2. Prove that \( 2^p \) cannot be written as the difference of squares (of integers).

6.8. (a) Prove that the sum of two rational numbers is rational.

   (b) Prove by contradiction that the sum of a rational and an irrational number is irrational.

   (c) What happens when you sum two irrational numbers?

6.9. (a) Suppose that there are 6 people in a room. Show that one can always find a group of 3 people such that either nobody in the group knows anybody in the group or everybody in the group knows everyone in the group.

   (b) Show that this conclusion does not hold if there are only 5 people in the room.

6.10. Use proof by contradiction to prove that there are infinitely many prime numbers.

   (Hint: consider the number \( M \) that is 1 more than the product of all primes.)

6.11. Determine which of the following are valid rules of inference. Justify your answer.
(a) If \( a \lor b \) and \( a \Rightarrow c \) and \( b \Rightarrow c \), then \( c \).
(b) If \( p \Rightarrow q \) and \( \neg q \), then \( \neg p \).
(c) If \( a \Rightarrow b \) and \( b \Rightarrow a \), then \( a \).
(d) If \( d \Rightarrow e \) and \( e \Rightarrow f \), then \( d \Rightarrow f \).

6.12. Convert to a quantified statement with predicates:

(a) Fridays are great!
(b) There is no largest integer.

6.13. Let \( \mathbb{N} \) denote the set of nonnegative integers. Translate the following statements about \( \mathbb{N} \) into English and then state whether they are true or false. Justify your answer.

(a) \( \exists x \left( \forall y \left( x \geq y \right) \right) \)
(b) \( \forall x \left( \exists y \left( x > y \right) \right) \)
(c) \( \forall x \left( \forall y \left( (x \geq y) \lor (x \leq y) \right) \right) \)

6.14. Use quantifiers to define a prime. That is, give a compound statement over the universe the integers with free variable \( x \) that is true exactly when \( x \) is a prime.

6.15. Negate and simplify the following:
\( \forall x \left( \forall y \left( (x < y) \Rightarrow \exists z (x < z < y) \right) \right) \).
(There should be no \( \neg \) in your final answer.)

6.16. Are the following pairs of statements equivalent?

(a) \( \forall x \left( p(x) \right) \) and \( \neg \exists y \left( \neg p(y) \right) \)
(b) \( \forall x \left( \forall y \left( q(x, y) \right) \right) \) and \( \forall y \left( \forall x \left( q(x, y) \right) \right) \)
(c) \( \forall x \left( \exists y \left( r(x, y) \right) \right) \) and \( \exists y \left( \forall x \left( r(x, y) \right) \right) \)
(d) \( \exists x \left( s(x) \land t(x) \right) \) and \( (\exists x \left( s(x) \right)) \land (\exists x (t(x))) \)

6.17. Using \( s(x, y, z) \) to stand for the expression \( x = yz \) and \( t(x, y) \) to stand for the expression \( x \leq y \), write down in logic what is means for \( d \) to be the greatest common divisor of \( m \) and \( n \). (Assume the universe is the positive integers throughout.)

---

**Solutions to Practice Exercises**

1. Note that \( x^2 - 1 = (x - 1)(x + 1) \). Since \( x^2 - 1 \) is a multiple of 3, it follows that either \( x - 1 \) or \( x + 1 \) is a multiple of 3. That is, it follows that \( x \) is either 1 less or 1 more than a multiple of 3, and in both cases, \( x \) is not a multiple of 3.