Chapter 5

⋆ Proof Strategies

You want proof? I'll give you proof!

- Sidney Harris.

So far, we have concentrated on developing formal languages for rigorously and unambiguously expressing properties of systems, namely the languages of propositional logic, predicate logic, sets and Boolean algebras. In the case of propositional logic we have used truth tables to determine the validity of logical arguments. We have also learned what it means for statements of predicate logic to be true or false, but we have not yet seen a procedure for determining truth or falsity. This is perhaps not too surprising, as predicates can range over infinite universes of discourse, hence infinitely many candidates potentially need to be inspected to test statements such as *"This program will terminate (with the correct result) at some point in time."*

A ***proof*** of a (true) statement is a demonstration of its validity which contains sufficient detail to convince someone that the statement is true. Statements which are provable are called ***theorems***. We encountered formal proofs already in Chapter 3, where we derived the truth of various theorems of Boolean algebra; each such derivation ended with the symbol □ indicating that the truth of the theorem had been established.

Proofs allow us to reason formally about properties of systems, so that (ultimately) we can provide convincing and irrefutable evidence of their correctness. We have already explored some basic proof techniques, for instance reasoning with logical equivalences in propositional logic and reasoning equationally with Boolean algebras. However, thus far we have asked no more of our reader than to use common sense to follow our reasoning.

Proofs of theorems often require creativity and inspiration. Furthermore, there will always be many different ways to prove a given theorem, and any valid proof of a given theorem will be just as correct a proof as any other. However, some proofs will be more elegant and more easily grasped than others. The mathematician Paul Erdős often referred to "The Book" in which God keeps the most elegant proof of each mathematical theorem, and noted that "You don't have to believe in God, but you should believe in

F. Moller, G. Struth, *Modelling Computing Systems*,
Undergraduate Topics in Computer Science,
DOI 10.1007/978-1-84800-322-4_6, © Springer-Verlag London 2013

The Book."

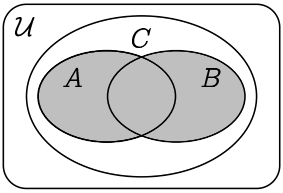
Elegance aside, all formal proofs follow certain patterns that can be learned like the rules of chess. Different ***proof strategies*** can be applied, depending only on the form of the property being considered. Once these strategies are learned, proofs can be easily – even mechanically – constructed and checked. In this chapter, we develop such proof strategies that will allow us to verify (or indeed falsify) system properties from a systematic point of view, relieving us of the need for too much *Eureka!*-invoking inspiration.

5.1 A First Example

It is obvious – by drawing a Venn diagram – that the union $A \cup B$ of two sets A and B contains both A and B as subsets:

$$A \subseteq A \cup B \text{ and } B \subseteq A \cup B.$$

But $A \cup B$ is a very special superset of A and B: it consists of *precisely* the elements of A and the elements of B – no more and no less – and is therefore the *least* superset of both A and B. In other words, any set C which is a superset of both A and of B is also a superset of $A \cup B$:



Although this fact should be intuitively clear, its validity deserves a formal proof such as the following.

Theorem 5.1

Let A, B and C be sets. Then

$$A \subseteq C \wedge B \subseteq C \Rightarrow A \cup B \subseteq C.$$

Proof: Assume that $A \subseteq C$ and $B \subseteq C$; we must show that $A \cup B \subseteq C$. To do this, we expand the definition of the set inclusion $A \cup B \subseteq C$:

> every element of $A \cup B$ must also be in C.

So we pick an arbitrary element $x \in A \cup B$ and we show that $x \in C$. Noting that $x \in A \cup B$ is the same as $x \in A \vee x \in B$, we proceed by case analysis on whether $x \in A$ or $x \in B$.

1. If $x \in A$, then $x \in C$, since we assumed that $A \subseteq C$.
2. If $x \in B$, then again $x \in C$, since we assumed that $B \subseteq C$.

In each case, $x \in C$ follows from the assumptions. □

At first sight you might find this proof perhaps more difficult to understand and less revealing than, for instance, a Venn diagram. However, in a few steps, it can be completely reduced to some basic proof strategies for predicate logic and some basic principles about sets. Everyone who has learned these strategies and principles can then easily check this proof, and, in fact, even machines can do that for you.

So let us take a quick initial look at some of the proof strategies that occur in this argument. They are based on logical principles of reasoning with propositional connectives and quantifiers. They deal with these connectives and quantifiers in two essentially different ways.

First, in order to prove the implication

$$A \subseteq C \ \wedge \ B \subseteq C \ \ \Rightarrow \ \ A \cup B \subseteq C,$$

we have *assumed* that $A \subseteq C \wedge B \subseteq C$ and proved that $A \cup B \subseteq C$ from this assumption. The underlying proof strategy allows us to prove an arbitrary implication $P \Rightarrow Q$ by assuming P and proving Q from this assumption. In a similar fashion, instead of proving

$$\forall x \, (x \in A \cup B \ \Rightarrow \ x \in C),$$

we have proved $x \in A \cup B \Rightarrow x \in C$ for an *arbitrary* x taken from the universe of discourse.

One way of understanding these proof strategies is that they decompose a proof goal, replacing it with a simpler one from which the original goal follows more or less automatically. These strategies narrow the distance between the assumptions and the goal from the goal side, hence in a bottom up way. Another way of understanding these strategies is to observe that they introduce a logical connective or quantifier into a proof. They can therefore be characterised as ***introduction strategies*** for connectives or quantifiers. The strategies mentioned above, for instance, introduce implication and universal quantification, respectively.

A second kind of strategy allows us to use complex assumptions or intermediate proof results (which can also be seen as assumptions) in proofs. In the above proof, for instance, we have used a strategy that allowed us to decompose the assumption $A \subseteq C \ \wedge \ B \subseteq C$ into two separate assumptions $A \subseteq C$ and $B \subseteq C$. Also, to prove $x \in C$ from the assumption $x \in A \ \vee \ x \in B$, we have used a case analysis strategy and proved $x \in C$ first from $x \in A$ and then from $x \in B$. The underlying proof strategy allows us to prove a goal R from a disjunction $P \vee Q$ by case analysis, that is, by proving R from the assumption P and from the assumption Q separately.

This second type of strategy can be understood as narrowing the distance between the assumptions and the goal from the assumptions side, hence in a top down way. They eliminate logical connectives or quantifiers and can therefore be characterised as *elimination strategies*.

When faced with the prospect of proving a theorem, a sensible approach would be to:

1. write out any assumptions, and previously-established facts that you suspect may be relevant, at the top of a page;
2. write out the statement which you wish to prove at the bottom of the page;
3. repeatedly apply elimination strategies to the statements at the top, and introduction strategies to the statements at the bottom, and look for how to make the logical argument meet in the middle.

With this in mind, we will present basic introduction and elimination strategies for each of the propositional connectives and quantifiers, and depict these as proof outlines with "holes" in the middle that need to be filled in. The justification behind each such proof outline will be made evident.

Exercise 5.2 (Solution on page 427)

Let A, B and C be sets. Prove the converse of Theorem 5.1, that

$$A \cup B \subseteq C \;\Rightarrow\; A \subseteq C \,\wedge\, B \subseteq C.$$

5.2 Proof Strategies for Implication

A proof of a theorem consists of a sequence of statements, each either being assumed or known to be true, or logically inferred from (i.e., implied by) earlier statements appearing in the proof. It is sensible, therefore, to start by considering proof strategies for implication.

In our introductory example we proved the theorem

$$A \subseteq C \,\wedge\, B \subseteq C \;\Rightarrow\; A \cup B \subseteq C.$$

by assuming that $A \subseteq C \,\wedge\, B \subseteq C$ and showing from this that $A \cup B \subseteq C$. This idea can be generalised to the following proof strategy for implication.

Assume P.

Then

⋮

proof of Q

⋮

Therefore, $P \Rightarrow Q$. □

This is an introduction strategy for implication, as it gives a method for introducing a statement of the form $P \Rightarrow Q$ into a proof.

Example 5.2

Consider the fact that the average of two different numbers lies somewhere strictly between the two. For example, the average of the two numbers 13 and 25 is 19, which lies strictly between the two given numbers 13 and 25. This general fact is intuitively obvious. However, once it is rendered in precise mathematical terms, it becomes something that is nonetheless deserving of a proof.

As a mathematical statement, the above fact becomes:

$$\textit{If } a < b \textit{ then } a < \frac{a+b}{2} \textit{ and } \frac{a+b}{2} < b.$$

More precisely, this statement is of the form

$$P \Rightarrow Q$$

where

$$P = a < b, \quad \text{and}$$

$$Q = a < \frac{a+b}{2} \wedge \frac{a+b}{2} < b.$$

Here we prove one half of this result:

If $a < b$ then $\frac{a+b}{2} < b$.

Proof: Assume that $a < b$.

Then, by adding b to both sides, we get that $a+b < b+b$.

Thus, by dividing both sides by 2, we get that $\frac{a+b}{2} < \frac{b+b}{2}$.

Since $\frac{b+b}{2} = b$, we get that $\frac{a+b}{2} < b$.

Therefore, if $a < b$ then $\frac{a+b}{2} < b$. □

The introduction strategy for implication is so fundamental that one usually just assumes P and proves Q without even mentioning that this yields a proof of $P \Rightarrow Q$.

Example 5.3

Prove that the product of two even integers is an even integer.

Proof: Assume that a and b are even integers.

An even integer is twice an integer.

Thus $a = 2p$ and $b = 2q$ for some integers p and q.

$$\begin{aligned}\text{Hence } ab &= (2p)(2q) = 4pq \\ &= 2k \text{ for the integer } k = 2pq.\end{aligned}$$

Therefore, ab is an even integer. □

Exercise 5.3

(Solution on page 427)

Prove that the product of two odd integers is an odd integer.

There is another introduction strategy for implication which may be more natural to apply on occasion. We can assume that Q is false and prove that, under this assumption, P must also be false. The form of such a proof would thus be as follows.

Assume $\neg Q$.

Then

$\vdots$

proof of $\neg P$

$\vdots$

Therefore, $P \Rightarrow Q$. □

A proof which employs this strategy is referred to as a *proof by contraposition.*

Example 5.4

Prove, by contraposition, the result from Example 5.2 that, for any two real numbers a and b, if $a < b$ then $\frac{a+b}{2} < b$.

Proof: Suppose that $\frac{a+b}{2} \geq b$.

Then, by multiplying both sides by 2, we get that $a + b \geq 2b$.

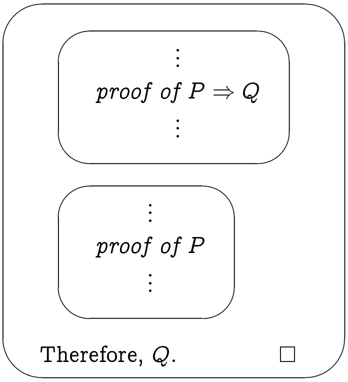
Thus, by subtracting b from both sides, we get that $a \geq b$.

Therefore, if $a < b$ then $\frac{a+b}{2} < b$. □

Corresponding to the above two introduction strategies, there are two elimination strategies for implication which allow us to draw inferences from statements in a proof that involve implication. These strategies are as follows.

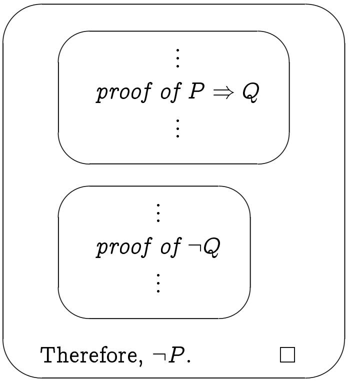
1. If $P \Rightarrow Q$ is true and P is true, then Q is true.

   A use of this proof strategy is referred to as ***modus ponens***, and takes the following form.



2. If $P \Rightarrow Q$ is true and $\neg Q$ is true, then $\neg P$ must be true.

   A use of this proof strategy is referred to as ***modus tollens***, and takes the following form.



Indeed, we have already seen these proof principles in action, particularly extensively in the solution to the Amos Judd puzzle of Exercise 1.14 (page 33).

Example 5.5

Prove that if $a \in A$ and $A \subseteq B$ then $a \in B$.

Proof: Assume that $a \in A$, and that $A \subseteq B$.

By definition, $A \subseteq B$ means that $x \in A \Rightarrow x \in B$ for any x.

In particular, $a \in A \Rightarrow a \in B$.

Thus, by *modus ponens*, $a \in B$. □

Exercise 5.5 (Solution on page 427)

Prove that the number 9 839 853 is divisible by 3. (You may use the fact that a number is divisible by 3 if the sum of its digits is divisible by 3.)

5.3 Proof Strategies for Negation

The main approaches to proving a property of the form $\neg P$ is to assume that P is true and to infer from this a contradiction. By this, we mean that both some property Q and its negation $\neg Q$ can be inferred from our assumption P; as such a contradiction is impossible, the assumption from which it was inferred must be invalid. The form of such a proof would thus be as follows.

Assume P.

Then

⋮

proof of contradiction

⋮

Therefore, $\neg P$. □

This is the standard negation introduction strategy. The associated negation elimination strategy is nearly identical, allowing positive results to be proven by contradiction. It takes the following form.

Assume $\neg P$.

Then

$\vdots$

proof of contradiction

$\vdots$

Therefore, P. □

A proof which employs either of these strategies is referred to as a ***proof by contradiction*** or, more fancily, as ***reductio ad absurdum***.

Our first example of a proof by contradiction is over 2000 years old and is attributed to the school of Pythagoras.

Example 5.6

Prove that $\sqrt{2}$ is irrational; that is, $\sqrt{2} \notin \mathbb{Q}$.

Proof. Suppose to the contrary that $\sqrt{2} \in \mathbb{Q}$; specifically, suppose that $\sqrt{2} = \frac{a}{b}$ where a and b are positive integers and $\frac{a}{b}$ is a fraction in lowest form; in particular, a and b are not both even.

Then squaring both sides gives us that $2 = \frac{a^2}{b^2}$, and then multiplying both sides by b^2 gives us that $2b^2 = a^2$.

Hence a must be even (since, by Exercise 5.3, if a were odd then a^2 would also be odd); that is, $a = 2c$ for some integer c.

As a and b are not both even, b must be odd.

But then $2b^2 = a^2 = (2c)^2 = 4c^2$, so $b^2 = 2c^2$, which means that b must be even, contradicting our earlier observation that b must be odd.

This must mean that our assumption that $\sqrt{2}$ is rational must be invalid; that is, $\sqrt{2}$ must in fact be irrational. □

Another famous example of a proof by contradiction that is also over 2000 years old, this time due to Euclid, is the following argument that there are infinitely many prime numbers. The proof relies on the *Fundamental Theorem of Arithmetic* – also proved by Euclid and which we prove in Exercise 9.9, page 235 – which states that every positive integer can be expressed as a product of prime numbers; in particular, every such number is divisible by some prime number.

Example 5.7

Prove that there are infinitely many prime numbers.

Proof. Suppose to the contrary that there are finitely many prime numbers, which we may list as $\{ p_1, p_2, p_3, \ldots, p_k \}$.

Let $n = (p_1 \times p_2 \times p_3 \times \cdots \times p_k) + 1$.

This number cannot be prime, as it is clearly larger than every one of the k prime numbers p_1 through p_k.

Thus, by the *Fundamental Theorem of Arithmetic*, some prime number p_i must divide evenly into n.

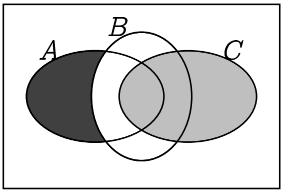
However this is impossible, as dividing n by p_i clearly leaves a remainder of 1, and hence p_i does not divide evenly into p.

Therefore, our assumption that there are finitely many prime numbers must be invalid; that is, there must in fact be infinitely many prime numbers. □

Example 5.8

Suppose that $A \cap C \subseteq B$ and that $a \in C$. Prove that $a \notin A \setminus B$.

As always, before blindly starting a proof, you should try to get a good impression in your mind as to what it is you are trying to prove. If possible, this is best done by drawing a picture, which in this case means a Venn diagram:



Here we have depicted three sets A, B and C which satisfy the premise of the proposition that we wish to prove: that $A \cap C \subseteq B$. From this we need to infer that any element $a \in C$ (i.e., which lies in the light gray area) will not be in $A \setminus B$ (i.e., cannot lie in the dark gray area). This seems obvious in the picture, but a rigorous argument is still demanded. Fortunately, now that we have a clear picture in our mind, a rigorous proof seems trivial.

Proof. Assume that the premises of the proposition are true, that $A \cap C \subseteq B$ and that $a \in C$. We shall show that assuming that $a \in A \setminus B$ leads to a contradiction.

Suppose that $a \in A \setminus B$; that is, that $a \in A$ but that $a \notin B$.

Since $a \in A$ and $a \in C$ (from the premise of the proposition), we have that $a \in A \cap C$.

But since $A \cap C \subseteq B$ (again from the premise of the proposition), from $a \in A \cap C$ we get that $a \in B$, contradicting $a \notin B$.

Therefore, we cannot have $a \in A \setminus B$; that is, we have $a \notin A \setminus B$. □

As usual, there are various ways that this proposition can be proven, all of which being equally valid. The following is provided as an example.

A Different Proof. Assume that the premises of the proposition are true, that $A \cap C \subseteq B$ and that $a \in C$.

As $a \in A \setminus B$ if, and only if, $a \in A$ and $a \notin B$, we shall show that $a \notin A \setminus B$ by showing that we cannot have both $a \in A$ and $a \notin B$; that is, if we assume that $a \in A$ then we can deduce that $a \in B$.

Suppose then that $a \in A$.

Since $a \in C$ (from the premise of the proposition), we have that $a \in A \cap C$.

But then since $A \cap C \subseteq B$ (again from the premise of the proposition), we have that $a \in B$.

Therefore, we cannot have both $a \in A$ and $a \notin B$; that is to say, we must have $a \notin A \setminus B$. □

Example 5.9

Assume that a and b are positive real numbers.

Prove that either $a \leq \sqrt{ab}$ or $b \leq \sqrt{ab}$.

Proof. Suppose to the contrary that $a > \sqrt{ab}$ and $b > \sqrt{ab}$.

Then $ab > \left(\sqrt{ab}\right)^2 = ab$, which is impossible.

Therefore, either $a \leq \sqrt{ab}$ or $b \leq \sqrt{ab}$. □

Exercise 5.9

(Solution on page 427)

Prove that there is no such thing as the smallest positive rational number.

Exercise 5.10 (Solution on page 428)

Prove that every integer greater than 1 can be written as a product of prime numbers.

(Note that a prime number is the trivial product of one prime number.)

5.4 Proof Strategies for Conjunction and Equivalence

There is very little interesting or needed to say about dealing with conjunctions in proofs. To prove a property of the form $P \wedge Q$, we simply prove P and Q separately. The form of such a proof will look as follows.

$\vdots$

proof of P

$\vdots$

$\vdots$

proof of Q

$\vdots$

Therefore, $P \wedge Q$. □

This is the basic introduction strategy for conjunction. The basic elimination strategy is equally straightforward: we may infer the truth of one of the conjuncts of an established conjunction. The form of such a proof will look like one of the following following.

$\vdots$

proof of $P \wedge Q$

$\vdots$

Therefore, P. □

$\vdots$

proof of $P \wedge Q$

$\vdots$

Therefore, Q. □

These will rarely be used in isolation, and their use inevitably comes naturally. As such, the following examples – while instructive – are somewhat contrived and superfluous.

Example 5.10

Prove that if $x \in A$ and $x \in B$ then $x \in A \cap B$.

Proof: Assume that $x \in A$ and that $x \in B$.

By the conjunction introduction strategy, we can infer from this that $x \in A \ \wedge \ x \in B$, which by definition means that $x \in A \cap B$. □

Example 5.11

Prove that if $x \in A \cap B$ then $x \in A$ and $x \in B$.

Proof: Assume that $x \in A \cap B$

By definition this means that $x \in A \ \wedge \ x \in B$.

By the conjunction elimination strategy, we can infer from this both that $x \in A$ and that $x \in B$. □

An equivalence $P \Leftrightarrow Q$ between properties P and Q simply represents the fact that each property implies the other; it is true if, and only if, $P \Rightarrow Q$ and $Q \Rightarrow P$. As such, proof strategies for equivalence are naturally based on those for conjunction. To prove $P \Leftrightarrow Q$, we simply prove $P \Rightarrow Q$ and $Q \Rightarrow P$ separately. The form of such a proof will look as follows.

⋮

proof of $P \Rightarrow Q$

⋮

⋮

proof of $Q \Rightarrow P$

⋮

Therefore, $P \Leftrightarrow Q$. □

This is the basic introduction rule for equivalence. The basic elimination strategy is to infer the implication in one direction or the other from an established equivalence. The form of such a proof will look as follows.

⋮

proof of $P \Leftrightarrow Q$

⋮

Therefore, $P \Rightarrow Q$. □

⋮

proof of $P \Leftrightarrow Q$

⋮

Therefore, $Q \Rightarrow P$. □

5.5 Proof Strategies for Disjunction

To prove that a disjunctive property $P \vee Q$, it suffices to prove one or the other of the disjuncts. The basic introduction strategy for disjunction is thus of the following forms.

$\vdots$

proof of P

$\vdots$

Therefore, $P \vee Q$. □

$\vdots$

proof of Q

$\vdots$

Therefore, $P \vee Q$. □

The above is rather weak, though. It might not be the case that one of P or Q always holds; rather, which holds might depend on some other factors. That is, it might be that P holds whenever some property R holds, and that Q holds when the property R does not hold. In this case the proof of $P \vee Q$ needs to be broken into cases. The relevant introduction strategy would then be of the following proof form.

Assume R.

Then

$\vdots$

proof of P

$\vdots$

Next, assume $\neg R$.

Then

$\vdots$

proof of Q

$\vdots$

Therefore, $P \vee Q$. □

Example 5.12

Prove that for any integer n, the remainder of n^2 when divided by 4 is either 0 or 1.

Proof: Either n is even or it is odd.

- If n is even, then $n = 2k$ for some integer k, and

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

  which clearly has a remainder of 0 when divided by 4.

- If n is odd, then $n = 2k + 1$ for some integer k, and

  $$n^2 \;=\; (2k+1)^2 \;=\; 4k^2 + 4k + 1 \;=\; 4(k^2 + k) + 1$$

  which clearly has a remainder of 1 when divided by 4.

Thus the remainder of n^2 when divided by 4 is either 0 or 1. □

A special case of the above strategy is to take the property R to be P itself. In this case, there would be no effort needed to infer P from the assumption P, so the form of the proof would be as follows.

Assume $\neg P$.

Then

⋮

proof of Q

⋮

Therefore, $P \vee Q$. □

Example 5.13

Prove that if x is a real number with $x^2 > x$ then either $x < 0$ or $x > 1$.

Proof: Assume as given that $x^2 > x$. Clearly this means that $x \neq 0$.

If it is *not* the case that $x < 0$, then $x > 0$, and we can divide each side of the given inequality $x^2 > x$ by x to deduce that $x > 1$.

Hence, either $x < 0$ or $x > 1$. □

Exercise 5.13

(Solution on page 428)

Prove that if the product of two integers is even, then one of these two integers is itself even.

Exercise 5.14 (Solution on page 429)

Prove that if $A \subseteq B$ then either $x \notin A$ or $x \in B$.

The elimination strategy for disjunction is more interesting. If we have as given a property $P \vee Q$, we can prove that a further property R holds by breaking the proof into cases; that is, we show that $P \Rightarrow R$ and $Q \Rightarrow R$. This being the case, regardless of which of P or Q is true, R must be true. The form of this elimination strategy is thus as follows.

$\vdots$

proof of $P \vee Q$

$\vdots$

Thus, either P is true, or Q is true.

Assume first that P is true.

Then

$\vdots$

proof of R

$\vdots$

Thus R must be true.

Next, assume that Q is true.

Then

$\vdots$

proof of R

$\vdots$

Thus, once again, R must be true.

Therefore, R is true (regardless of whichever of P or Q is true). □

Example 5.14

Prove that $A \cap (B \cup C) \subseteq (A \cap B) \cup C$.

Proof. Let $x \in A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Then either $x \in A \cap B$, in which case $x \in (A \cap B) \cup C$;

or $x \in (A \cap C)$, in which case $x \in C$ so again $x \in (A \cap B) \cup C$. □

Example 5.15

Prove that if $|x-3| > 3$ then $x^2 > 6x$.

Proof. If $|x-3| > 3$ then either $x > 6$, in which case $x^2 > 6x$;

or $x < 0$, in which case $x^2 > 0 > 6x$. □

Exercise 5.15 (Solution on page 429)

Prove the triangle inequality: For real numbers a and b, $|a+b| \leq |a| + |b|$.

Exercise 5.16 (Solution on page 429)

Prove that if n is an integer, then the final (units) digit of n^2 must be either 0, 1, 4, 5, 6 or 9; that is, n^2 cannot end with a 2, 3, 7 or 8.

Exercise 5.17 (Solution on page 430)

What is wrong with the following proof?

Fact: If $x+y = 12$ then $x \neq 7$ and $y \neq 8$.

Proof: Assume that the conclusion is false, that is, that it is *not* the case that $x \neq 7$ and $y \neq 8$.

Then $x = 7$ and $y = 8$,

Hence if $x+y = 12$ then $x \neq 7$ and $y \neq 8$. □

5.6 Proof Strategies for Quantifiers

5.6.1 Universal Quantification

A universal quantification $\forall x\, P(x)$ represents a potentially-infinite conjunction, asserting that $P(a)$ is true for *every* value a of the universe of discourse for the predicate P. As such, we look at how to generalise the proof strategies for conjunction.

To prove a property of the form $\forall x\, P(x)$, let a stand for an *arbitrary* object, and prove $P(a)$. The form of such a proof would thus be as follows.

> Let a be arbitrary.
>
> $\vdots$
>
> *proof of* $P(a)$
>
> $\vdots$
>
> Therefore, $\forall x\, P(x)$. □

As long as we make no assumptions about a in the proof of $P(a)$, then this proof will be valid for whatever choice of a we make. That is, we will have shown that $P(x)$ must be true for every x (that is, for any and every choice of value a for x). It should be apparent how this introduction strategy generalises that for conjunction.

Note that we have already been tacitly using this strategy. For instance, in Example 5.9 we proved a result held for all positive real numbers a and b, by assuming as given arbitrary values for a and b. Usually this is fine – we generally don't have to think twice about taking arbitrary values as given. However, we do sometimes have to be more careful with introducing values.

We can next look to the elimination strategy for conjunction to derive a straightforward generalisation which tells us how to use a universal quantification within a proof. If we have ascertained that $\forall x\, P(x)$ is true and a is an element in the universe of discourse for the predicate P, then we can immediately infer that $P(a)$ is true. The form of such a proof will look as follows.

> $\vdots$
>
> *proof of* $\forall x\, P(x)$
>
> $\vdots$
>
> Therefore, $P(a)$. □

Example 5.17

Prove that if $A \cap B = A$ then $A \subseteq B$.

Proof. Assume that $A \cap B = B$. We need to demonstrate that $A \subseteq B$, that is, that for any x, if $x \in A$ then $x \in B$:

$$\forall x\, (x \in A \;\Rightarrow\; x \in B).$$

To this end, let a be an arbitrary value.

To show that $a \in A \Rightarrow a \in B$, we assume that $a \in A$ and prove from this assumption that $a \in B$.

Assume then that $a \in A$.

Since $A \cap B = A$ (from the premise of the proposition), this means that $a \in A \cap B$.

But this means that $a \in A$ and $a \in B$; in particular, that $a \in B$.

Therefore, $\forall x\, (x \in A \Rightarrow x \in B)$; that is, $A \subseteq B$. □

Example 5.18

Prove that $\forall x \left(P(x) \wedge Q(x)\right) \Leftrightarrow \forall x\, P(x) \wedge \forall x\, Q(x)$.

Proof. ($\Rightarrow$) Suppose $\forall x \left(P(x) \wedge Q(x)\right)$, and let a be an arbitrary value.

Then $P(a) \wedge Q(a)$, so $P(a)$ and $Q(a)$.

Since a is arbitrary, we can infer that $\forall x\, P(x)$ and $\forall x\, Q(x)$; that is, $\forall x\, P(x) \wedge \forall x\, Q(x)$.

($\Leftarrow$) Suppose $\forall x\, P(x) \wedge \forall x\, Q(x)$, and let a be an arbitrary value.

Then $P(a)$ and $Q(a)$, so $P(a) \wedge Q(a)$.

Since a is arbitrary, we can infer that $\forall x \left(P(x) \wedge Q(x)\right)$. □

Exercise 5.18 (Solution on page 430)

Prove that if A and $B \setminus C$ are disjoint then $A \cap B \subseteq C$.

5.6.2 Existential Quantification

An existential quantification $\exists x\, P(x)$ represents a potentially-infinite disjunction, asserting that $P(a)$ is true for *some* value a of the universe of discourse for the predicate P. As such, we look at how to generalise the proof strategies for disjunction.

To prove a property of the form $\exists x\, P(x)$, we need only find a value a for which $P(a)$ holds, and prove $P(a)$. The form of such a proof would thus be as follows.

Let a be some value (which you believe satisfies P).

⋮

proof of $P(a)$

⋮

Therefore, $\exists x\, P(x)$. □

Note the difference between this introduction strategy and the introduction strategy for $\forall x\, P(x)$. To prove $\forall x\, P(x)$ you need to prove that $P(a)$ holds for an *arbitrary* value a without making any assumptions about a. To prove $\exists x\, P(x)$ you need to prove that $P(a)$ holds for a single chosen value of a.

We next look to the elimination strategy for disjunction to derive a generalisation which tells us how to use an existential quantification within a proof. If we have ascertained that $\exists x\, P(x)$ is true, and if some property R holds under the assumption that $P(a)$ holds regardless of the specific value a of the universe of discourse, then we can infer that R is true. The form of such a proof will look as follows.

⋮

proof of $\exists x\, P(x)$

⋮

Let a be arbitrary, and assume $P(a)$.

Then

⋮

proof of R

⋮

Therefore, R is true. □

Example 5.19

Prove that, if $x \neq 1$, then $\frac{y-2}{y+1} = x$ for some y.

Proof. Let $y = \frac{x+2}{1-x}$ (noting that, since $x \neq 1$, $1-x \neq 0$, and so we are not inadvertently dividing by 0 in defining y).

$$\text{Then } y-2 = \frac{x+2 \; - \; 2(1-x)}{1-x} = \frac{3x}{1-x},$$

$$\text{and } y+1 = \frac{x+2 \; + \; 1-x}{1-x} = \frac{3}{1-x},$$

so $\frac{y-2}{y+1} = \left(\frac{3x}{1-x}\right) / \left(\frac{3}{1-x}\right) = \left(\frac{3x}{1-x}\right) \times \left(\frac{1-x}{3}\right) = x.$ □

The difficulty with proving the existence of an object a for which a property P holds is: how do we find the particular value a? In the above example, why did we choose to take $y = \frac{x+2}{1-x}$? The answer in this case – as it typically will be – lies in working backwards. Since we wanted to find a value y such that $\frac{y-2}{y+1} = x$, we worked from this equation:

- by multiplying both sides by $(y+1)$ we get $y-2 = x(y+1) = xy + x$;
- by rearranging terms to get all (and only) terms involving y on one side (i.e.. by adding $2-xy$ to both sides) we get $x+2 = y-xy = y(1-x)$.
- Dividing each side by $(1-x)$ – noting that this will not be an illegal division by zero, since the premise stipulates that $x \neq 1$ – we arrive at the value we seek: $y = \frac{x+2}{1-x}$.

Exercise 5.19 (Solution on page 430)

Prove that for every real $x>0$ there is a real y such that $y(y+1) = x$.

Although typically the case, it isn't strictly necessary (nor sometimes even possible) to explicitly find the specific value x which witnesses the fact that $\exists x P(x)$; the mere fact that such a value exists is all that needs to be demonstrated.

Example 5.20 A Strange Proof of Existence

Fact: There are irrational numbers a and b such that a^b is rational.

Proof. We know from Example 5.6 that $\sqrt{2}$ is irrational.

Furthermore, either $\left(\sqrt{2}\right)^{\sqrt{2}}$ is rational or it is irrational.

- Suppose $\left(\sqrt{2}\right)^{\sqrt{2}}$ is rational. Let $a = b = \sqrt{2}$.

  Then a and b are irrational, and $a^b = \left(\sqrt{2}\right)^{\sqrt{2}}$ is rational.
- Suppose $\left(\sqrt{2}\right)^{\sqrt{2}}$ is irrational. Let $a = \left(\sqrt{2}\right)^{\sqrt{2}}$ and $b = \sqrt{2}$.

  Then a and b are irrational, and

  $$a^b = \left(\left(\sqrt{2}\right)^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^{\left(\sqrt{2}\sqrt{2}\right)} = \left(\sqrt{2}\right)^2 = 2$$

  is rational. □

What is strange about this example is that we demonstrated the *existence* of two particular irrational numbers a and b which satisfy our conditions *without* discovering for certain what these particular numbers are!

Exercise 5.20 (Solution on page 431)

Prove that $\exists x \left(P(x) \vee Q(x)\right) \;\Leftrightarrow\; \exists x\, P(x) \;\vee\; \exists x\, Q(x)$.

(Hint: refer to the proof in Example 5.18.)

5.6.3 Uniqueness

There are two approaches to proving a property of the form $\exists! x\, P(x)$, the first by proving existence and uniqueness separately, and the second by combining these two concerns.

1. First prove *existence*: $\exists x\, P(x)$

   and then *uniqueness*: $\forall y \forall z \left[\left(P(y) \wedge P(z)\right) \Rightarrow y{=}z\right]$.
2. Prove $\exists x \left[P(x) \wedge \forall y \left(P(y) \Rightarrow y = x\right)\right]$.

Either way, the proof strategies are derived from existing strategies.

Example 5.21

Prove that for every x there is a unique y such that $x^2 y = x{-}y$.

Proof. Let $y = \dfrac{x}{x^2+1}$.

$$\text{Then } x^2 y \;=\; \frac{x^3}{x^2+1} \;=\; \frac{x(x^2+1) - x}{x^2+1} \;=\; x{-}y.$$

Furthermore, if $x^2 z = x{-}z$, then $z(x^2+1) = x$,

so $z = \dfrac{x}{x^2+1} = y$. □

Example 5.22

Suppose $\mathcal{F}$ is a family of sets. Prove that there is a unique set A that has the following two properties:

1. $\mathcal{F} \subseteq \mathcal{P}(A)$.
2. $\forall B \left(\mathcal{F} \subseteq \mathcal{P}(B) \Rightarrow A \subseteq B\right)$.

Proof. Let $A = \bigcup \mathcal{F}$.

1. Suppose $X \in \mathcal{F}$.

   Then $X \subseteq \bigcup \mathcal{F}$; that is, $X \subseteq A$.

   Hence $X \in \mathcal{P}(A)$.

2. Suppose B is *any* set satisfying $\mathcal{F} \subseteq \mathcal{P}(B)$.

   Let $a \in A$; that is, $a \in \bigcup \mathcal{F}$.

   Then $\exists X \in \mathcal{F}$ with $a \in X$.

   Thus $X \in \mathcal{P}(B)$, so $X \subseteq B$.

   Hence $a \in B$. □

Exercise 5.22 (Solution on page 431)

Prove that there is a unique set A such that, for every set B, $A \cup B = B$.

5.7 Additional Exercises

1. Prove that, for any two real numbers $a, b \in \mathbb{R}$: if $a < b$ then $a < \frac{a+b}{2}$.
2. Assume that m and n are integers. Prove that if $m+n$ is even, then m and n are either both even or both odd.
3. Assume that n is an integer. Prove that if $3n + 2$ is an odd integer, then n must be an odd integer.
4. Prove that there is no even prime number greater than 2.
5. Prove that $\sqrt{3}$ is irrational.
6. Prove or disprove each of the following.
   (a) The sum of two rational numbers is rational.
   (b) The sum of two irrational numbers is irrational.
7. Assume that n is an integer. Prove that $n^2 \geq n$.
8. Prove that if n is an integer, then the final digit of n^4 must be either 0 or 1 or 5 or 6.
9. Prove that there are no integer solutions to the equation $x^2 + 2y^2 = 24$.
10. Prove the Distributivity Laws for sets:
    (a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
    (b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

11. Prove the following.

    (a) $P \;\Rightarrow\; (Q \Rightarrow P)$.

    (b) $(P \Rightarrow Q) \;\Rightarrow\; (P \vee R \;\Rightarrow\; Q \vee R)$.

    (c) $(P \Rightarrow Q) \;\Rightarrow\; (P \wedge R \;\Rightarrow\; Q \wedge R)$.

12. Prove the following.

    (a) $\forall x(\, P(x) \wedge Q(x)\,) \;\Leftrightarrow\; \forall x\, P(x) \;\wedge\; \forall x\, Q(x)$.

    (b) $\exists x(\, P(x) \vee Q(x)\,) \;\Leftrightarrow\; \exists x\, P(x) \;\vee\; \exists x\, Q(x)$.

    (c) $\forall x(\, P(x) \vee Q(x)\,) \;\Leftarrow\; \forall x\, P(x) \;\vee\; \forall x\, Q(x)$.

    (d) $\exists x(\, P(x) \wedge Q(x)\,) \;\Rightarrow\; \exists x\, P(x) \;\wedge\; \exists x\, Q(x)$.

13. Prove that the two approaches to proving $\exists! x\, P(x)$ from Section 5.6.3 are equivalent.