

Proof writing strategies.

A formal proof of a sentence β is a sequence of sentences $\alpha_1, \alpha_2, \dots, \alpha_n$ where (i) $\beta = \alpha_n$ and (ii) each α_i is deducible from earlier sentences via an accepted rule of deduction. A disproof of β is a proof of $\neg\beta$.

An informal proof of β is an explanation of why β is true that contains all of the essential details of a formal proof, but which is more understandable to humans. This note contains terminology and hints about writing informal proofs.

Theorems. A statement β that has a proof is called a **Theorem**. Theorems sometimes go by other names, such as **Proposition**, **Lemma**, **Corollary**. From a mathematical perspective, these all mean “theorem”, but from a human perspective they communicate a little bit more. It has been said that “a theorem is a proposition you are proud of!” A lemma is (usually) a theorem proved as a step toward proving a more substantial theorem. A corollary is a theorem that is an immediate consequence of a substantial theorem.

The Deduction Theorem. Most theorems have the structure “Theorem. $H \rightarrow C$ ” (hypotheses imply conclusions).¹ Since $\models (H \rightarrow C)$ is equivalent to $H \models C$, proof systems are constructed so that $\vdash (H \rightarrow C)$ is equivalent to $H \vdash C$. The statement that, for a given proof system, $\vdash (H \rightarrow C)$ is equivalent to $H \vdash C$ is called The Deduction Theorem for that proof system. It reduces a proof $\alpha_1, \dots, (H \rightarrow C)$ of the theorem $H \rightarrow C$ to a deduction H, \dots, C of C from H .

Direct versus indirect proof.

$(H \rightarrow C)$, $((\neg C) \rightarrow (\neg H))$, and $((H \wedge (\neg C)) \rightarrow \text{False})$ are all equivalent as propositions. Coupled with The Deduction Theorem this suggests some basic strategies for proving $H \rightarrow C$.

- (1) Direct proof: H, \dots, C .
- (2) Proof of the contrapositive: $(\neg C), \dots, (\neg H)$.
- (3) Proof by contradiction: $H, (\neg C), \dots, \text{False}$.

Theorems with multiple hypotheses or conclusions can be approached with more complex strategies. For example, a statement $((H_1 \wedge H_2) \rightarrow C)$ with two hypotheses could be proved by the mixed strategy $H_1, (\neg C), \dots, (\neg H_2)$.

If and only if. A theorem statement of the form “ P iff Q ” means “(If P , then Q) and (if Q , then P)”. Two proofs are required, one for $P \rightarrow Q$ and one for $Q \rightarrow P$. These are sometimes written as follows:

¹Sometimes the hypotheses are not explicitly stated, so the theorem reads “Theorem. C ” (some conclusion is true). Here the unwritten hypotheses are: anything about the subject that has already been established! For example, the unwritten hypotheses of “Theorem. There are infinitely many primes” are: any statements about arithmetic that have already been established. These types of theorems are best proved indirectly.

Theorem. P iff Q .

Proof.

$[P \rightarrow Q] P, \dots, Q.$

$[Q \rightarrow P] Q, \dots, P. \square$

A slightly different way to write the proof is:

Proof.

$[\Rightarrow] P, \dots, Q.$

$[\Leftarrow] Q, \dots, P. \square$

A more elaborate version of “iff” is a statement of the form “ P iff Q iff R ”. This might be written:

Theorem. The following are equivalent. (Or just “TFAE”.)

(1) P

(2) Q

(3) R

Proof.

$[(1) \Rightarrow (2)] P, \dots, Q.$

$[(2) \Rightarrow (3)] Q, \dots, R.$

$[(3) \Rightarrow (1)] R, \dots, P. \square$

(Note: such cycles can be longer.)

Case division. Suppose we want to prove $H \rightarrow C$ via a deduction that starts with H and ends with C . Suppose your proof has reached a stage that looks like $H, \dots, P \vee Q$. (I.e., H proves that either P or Q holds.) If you also have proofs P, \dots, C and Q, \dots, C , then it is possible to combine these proof fragments (i) $H, \dots, P \vee Q$, (ii) P, \dots, C and (iii) Q, \dots, C into a proof that H implies C .

Formally, the reason this is possible is that the proposition $(P \rightarrow C) \wedge (Q \rightarrow C)$ is logically equivalent to $((P \vee Q) \rightarrow C)$, so by introducing the proper tautologies and using The Deduction Theorem we can arrange fragments (ii) and (iii) into a proof $P \vee Q, \dots, C$. This can be appended to the proof fragment (i) to obtain a proof $H, \dots, P \vee Q, \dots, C$.

Informally, the strategy we use is to **argue by cases**. If you can prove from H that P or Q must be true, then you write the deduction $H, \dots, (P \vee Q)$ and follow it with

Case 1. P holds.

In this case, P, \dots, C .

Case 2. Q holds.

In this case, Q, \dots, C .

Since we reach the conclusion in either case, we are done. \square

(Note: there can be more than two cases.)

Quantifiers. Suppose you are writing a proof $H, \dots, \exists xP(x), \dots, Q, \dots, R$ where at sentence Q you need to make use of the fact, established earlier, that there is some element that satisfies $P(x)$. Suppose that further on, at sentence R , you also need to make use of the fact that some element satisfies $P(x)$. Moreover, suppose that you need the element referred to at sentence R to be the **same** element referred to at sentence Q . What do you do?

Formally, there is a nontrivial, but mechanical trick to handle this situation. Informally, we handle this in an obvious way: At sentence $\exists xP(x)$ we introduce a name (like a) for an element that satisfies $P(x)$. Then at later stages we refer to the name a when we need to refer to the element.

To prove that $\forall xP(x)$ holds we may introduce a new symbol, say y , and prove that $P(y)$ holds when y is arbitrary. For example, the statement that sets $A \cap (B \cup C)$ and $(A \cap B) \cup (A \cap C)$ are equal is a universally quantified statement:

$$\forall x((x \in (A \cap (B \cup C))) \leftrightarrow (x \in ((A \cap B) \cup (A \cap C))))$$

To prove it we may select an arbitrary y and show that

$$y \in (A \cap (B \cup C)) \leftrightarrow y \in ((A \cap B) \cup (A \cap C)).$$

(Establishing that this holds requires two proofs: $y \in (A \cap (B \cup C)) \rightarrow y \in ((A \cap B) \cup (A \cap C))$ and $y \in ((A \cap B) \cup (A \cap C)) \rightarrow y \in (A \cap (B \cup C)).$)

Examples and counterexamples. To prove an existential sentence $\exists xC(x)$ it is enough to give an example. That is, exhibiting an element $x = a$ for which $C(a)$ holds suffices to prove that $\exists xC(x)$ is true. On the other hand, to prove a universal sentence $\forall xC(x)$ it is not enough to give an example.

To disprove a universal sentence $\forall xC(x)$ you must show that its negation is true. Since the negation is equivalent to the existential sentence $\exists x(\neg C(x))$, it is enough to give an example to establish the falsity of $\forall xC(x)$. That is, to disprove $\forall xC(x)$ it is enough to exhibit some a such that $\neg C(a)$ holds or, equivalently, such that $C(a)$ fails. Examples used to disprove universal sentences are called **counterexamples**. (If $C(x) =$ “if x is odd, then x is prime”, then $\forall xC(x)$ is false. You can disprove it by exhibiting the counterexample $x = 9$.)

What to do when you don't know what to do. There is no algorithm to discover the proof of a statement, but there is always something you can do when you are stuck. Here are three suggestions:

- (1) Draw a picture.
- (2) Write out the definitions.
- (3) Work from both ends.

Exercises.

1. Consider the following statement about the real numbers: If $0 < x < 1$, then $x^2 < x$. Give a direct proof, proof of the contrapositive, and a proof by contradiction.

Solution to Exercise 1.

Direct proof. Choose x arbitrarily so that the hypothesis holds, i.e., so that $0 < x < 1$. Then x is positive and $x < 1$. We can multiply an inequality, like $x < 1$, by the positive value x and maintain the inequality. Hence $x \cdot x < x \cdot 1$, or $x^2 < x$, as desired.

Proof of the contrapositive. Choose x arbitrarily so that the conclusion fails, i.e., so that $x^2 \not< x$. Then $x \leq x^2$, so $0 \leq x^2 - x$. Upon factoring we find that $0 \leq x(x - 1)$. This implies that x and $x - 1$ have the same sign (although one could be zero). Since $x - 1 < x$, this implies that either $0 \leq x - 1$ or $x \leq 0$.

Case 1. $0 \leq x - 1$.

In this case, $1 \leq x$, so the hypothesis $0 < x < 1$ fails.

Case 2. $x \leq 0$.

Again the hypothesis $0 < x < 1$ fails.

Cases 1 and 2 exhaust all cases, so we are done.

Proof by contradiction. Choose x arbitrarily so that $0 < x < 1$ and $x^2 \not< x$. As in the proof by contradiction, the second assumption leads to $0 \leq x(x - 1)$. The first assumption yields that x is positive and $(x - 1)$ is negative, so $0 \leq x(x - 1) = (\text{positive})(\text{negative}) = \text{negative} < 0$. This yields $0 < 0$, a contradiction.

Write proofs of the following statements, and then identify any of the proof writing strategies from this document that you used.

2. $A \subseteq B$ is equivalent to both $A \cap B = A$ and $A \cup B = B$.
3. If f and g are real functions such that f is bounded above and g is bounded below, then $f - g$ is bounded above.
4. If f is a positive increasing function, then f^2 is also a positive increasing function.