Math 300 **Introduction to Mathematical Reasoning** **Autumn 2018**

Handout 5: Proof Templates (UPDATED 10/17/18)[1]

In its most basic form, a mathematical proof is just a sequence of mathematical statements, connected to each other by strict rules that describe what types of statements may be added and in what order. If, by following these rules, you produce a sequence of statements, the last of which is the statement of the theorem you're trying to prove, then you have produced a proof that will convince any mathematically educated reader or listener beyond reasonable doubt that your theorem is correct.

In this note, we focus on the underlying structure of a proof as a sequence of statements, each justified according to the conventions of mathematical reasoning. To make that structure as plain as possible, we present our proofs in a "two-column" format, similar to the way proofs are introduced in some high-school geometry courses. In the left column is the sequence of statements that constitute the proof; in the right column are the reasons that justify the steps. The proof will be correct provided that each step is justified by one or more of the following six types of reasons:

- by hypothesis;
- by a definition;
- by an axiom;
- by a previously proved theorem;
- by a previous step in the same proof;
- by the laws of logic.

There are several different types of proofs, each of which is appropriate in certain circumstances. This note describes the most important types, with a template for each.

Direct Proofs

The most straightforward type of proof is called a *direct proof*: This is one in which we assume the hypotheses, and then, using the rules of deduction that we discussed above, derive the conclusion. It is easiest to set up when applied to a simple implication.

Template 1 (Direct Proof of an Implication)**.**

Theorem. $P \Rightarrow Q$.

Proof.

	Statement	**Reason**	
	Assume P.	(hypothesis)	
	...	(...)	
Goal:	Q.	(...)	□

There are a number of variations on direct proofs. One of the most common is *proof by contrapositive*. Because the contrapositive of an implication is equivalent to the original implication, we can always prove an implication by proving its contrapositive instead, if that is more convenient. Here is the template.

[1] Adapted from *Axiomatic Geometry* by John M. Lee,

Template 2 (Proof by Contrapositive)**.**

Theorem. $P \Rightarrow Q$.

Proof.

	Statement	**Reason**	
	Assume $\neg Q$.	(hypothesis)	
	...	(...)	
Goal:	$\neg P$.	(...)	□

Proofs of Universal Statements

The simple implications we have been considering so far are not very realistic; most theorem statements contain variables and (implicit or explicit) universal quantifiers. Here is the basic template for proving a universal statement.

Template 3 (Universal Statement)**.**

Theorem. $(\forall x \in D)(Q(x))$.

Proof.

	Statement	**Reason**	
	Let x be an arbitrary element of D.	(hypothesis)	
	...	(...)	
Goal:	$Q(x)$.	(...)	□

Pay close attention to the wording of the first step in this template. The word "let" is generally reserved for a special role in mathematical arguments: it should be used only to introduce a new symbolic name for something. One situation in which it occurs frequently is when assigning a specific value to a variable: "let $a = 2$." Another such situation is at the beginning of a proof of a universal statement, as in the template above, to introduce a symbol that represents a universally quantified variable in the proof. You should avoid using "let" to introduce anything other than a new symbolic name—for example, it would not be appropriate to use "let" to introduce an assumption, as in "let AB and AC be equal." It would be much better to say "assume that AB and AC are equal," or "suppose AB and AC are equal." (Occasionally, mathematicians do carelessly use the word "let" instead of "assume" or "suppose" in sentences like these, but your proofs will be clearer if you learn from the start to use "let" only to introduce new symbolic names.)

The other important word in the first step is "arbitrary." This is reserved for universally quantified objects, and indicates that the symbol x can stand for any unspecified element of the domain D. This means that we are not allowed to assume anything special about it except that it is an element of D (unless the subsequent steps in the proof call for such an assumption, an example of which we will see in the next template we consider). As long as we remember this restriction, the steps of our proof will be applicable to any element of D whatsoever, and we will have proved that each element $x \in D$ must satisfy the conclusion $Q(x)$.

Many of the templates we give here can be combined to obtain more complicated proof structures, for example by embedding one type of proof as a series of steps inside a longer proof of a different type. An important and common instance of this occurs when the theorem statement is a *universal implication*. In this case, the structure of the proof combines the patterns for proving both a universal statement and an implication. The vast majority of all theorems in mathematics are stated as universal implications (often with an implicit universal quantifier), so it is important to become very familiar with the template for such proofs.

Template 4 (Universal Implication)**.**

Theorem. $(\forall x \in D)(P(x) \Rightarrow Q(x))$.

Proof.

	Statement	**Reason**	
	Let x be an arbitrary element of D.	(hypothesis)	
	Assume $P(x)$.	(hypothesis)	
	...	(...)	
Goal:	$Q(x)$.	(...)	□

Of course, a universal implication can also be proved by proving the contrapositive; we leave it to you to figure out the details of all the possible variations on such combinations. You will see many of them in action in the proofs you encounter throughout this book.

Proofs of Conjunctions

Another type of theorem you will encounter is one in which you must prove a conjunction. Most often, the conjunction occurs as the conclusion of an implication, as in "$P \Rightarrow Q_1 \wedge Q_2$." In this case, the idea is simple: to prove the conclusion, we must prove that Q_1 and Q_2 are both true, so the proof will have two parts, one for each conclusion. Here is what the template looks like.

Template 5 (Proof of a Conjunction)**.**

Theorem. $P \Rightarrow Q_1 \wedge Q_2$.

Proof.

	Statement	**Reason**	
	Assume P.	(hypothesis)	
	Part 1: Proof of Q_1		
	...	(...)	
	...	(...)	
Goal:	Q_1.	(...)	
	Part 2: Proof of Q_2		
	...	(...)	
	...	(...)	
Goal:	Q_2.	(...)	□

The hypothesis P is stated before the beginning of Part 1 to make it clear that it can be used throughout both parts of the proof.

Proofs of Equivalence

A common type of theorem is an *equivalence theorem*, one that asserts a biconditional like $P \Leftrightarrow Q$. Since this statement is equivalent to the conjunction "$P \Rightarrow Q \wedge Q \Rightarrow P$," a proof of equivalence has to be carried out in two parts like a proof of a conjunction.

Template 6 (Proof of Equivalence)**.**

Theorem. $P \Leftrightarrow Q$.

Proof.

	Statement	**Reason**
	Part 1: Proof that $P \Rightarrow Q$	
	Assume P.	(hypothesis)
	...	(...)
Goal:	Q.	(...)
	Part 2: Proof that $Q \Rightarrow P$	
	Assume Q.	(hypothesis)
	...	(...)
Goal:	P.	(...) $\square$

A common variation on this pattern is to prove one or the other of the implications by proving its contrapositive. For example, a common way to prove $P \Leftrightarrow Q$ is first to prove $P \Rightarrow Q$ and then to prove $\neg P \Rightarrow \neg Q$.

Proof by Cases

Another important variation on direct proof is *proof by cases*. This is needed whenever you need to prove that two or more different hypotheses lead to the same conclusion. The most common example of this is a theorem whose hypothesis is a disjunction (an "or" statement). For example, suppose we want to prove a statement of the form "$P_1 \vee P_2 \Rightarrow Q$." In this case, the hypothesis tells us that either P_1 or P_2 is true, but we don't know which one; you need to show that either hypothesis leads to the conclusion that Q is true. For such a theorem, it is necessary to carry out two proofs, one for the case in which P_1 is true, and the other for the case in which P_2 is true. The template looks like this:

Template 7 (Proof by Cases)**.**

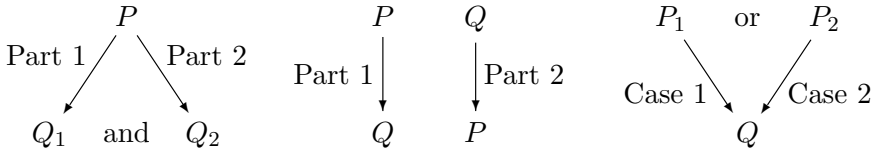
Theorem. $P_1 \vee P_2 \Rightarrow Q$.

Proof.

	Statement	**Reason**
	Assume $P_1 \vee P_2$.	(hypothesis)
	Case 1:	
	Assume P_1.	(hypothesis)
	...	(...)
Goal:	Q.	(...)
	Case 2:	
	Assume P_2.	(hypothesis)
	...	(...)
Goal:	Q.	(...) $\square$

Note the difference between *cases* and *parts* of a proof: as explained in the preceding section, your proof will have multiple *parts* when you have two or more different conclusions to prove, with the same or different hypotheses. On the other hand, it will have multiple *cases* when there is only one

conclusion to prove, but it must be proved under two or more different hypotheses. The typical patterns are summarized in the following diagrams:



Proofs by cases can be useful even when there is not a disjunction in the hypothesis. If, at any point during a proof, you have deduced a statement of the form $P_1 \vee P_2$, then it is legitimate to divide the remainder of the proof into cases depending on whether P_1 is true or P_2 is true.

In fact, sometimes cases are useful even when no disjunction is evident. If one of two (or more) possibilities must hold, and different proofs are needed to handle the different possibilities, then a proof by cases is called for. In effect, we introduce a disjunction of the form $R \vee \neg R$ (which is always true by the laws of logic), and then use those two cases to continue the proof. Consider the following snippet:

	Statement	**Reason**
	...	(...)
5.	a is a real number.	(...)
6.	Either $a = 0$ or $a \neq 0$.	(logic)
	Case 1:	
7.	Assume $a = 0$.	(hypothesis)
	...	(...)
	Case 2:	
10.	Assume $a \neq 0$.	(hypothesis)
	...	(...)

In practice, in cases like this, the explicit statement of the disjunction (Step 6 in the preceding snippet) is frequently omitted from the proof, as long as it will be obvious to the reader that at least one of the specified cases must hold.

Proof of a Disjunction

If the *conclusion* of a theorem is a disjunction, as in "$P \Rightarrow Q_1 \vee Q_2$," the most common way to prove the theorem is to use the following logical equivalence, which can be verified using a truth table:

$$\big(P \Rightarrow Q_1 \vee Q_2\big) \equiv \big((P \wedge \neg Q_1) \Rightarrow Q_2\big).$$

(Or, if it's easier, you can reverse the roles of Q_1 and Q_2.) From that point on, it's just like any other proof of an implication.

Template 8 (Proof of a Disjunction)**.**

Theorem. $P \Rightarrow Q_1 \vee Q_2$.

Proof.

	Statement	**Reason**
	Assume $P \wedge \neg Q_1$.	(hypothesis)
	...	(...)
Goal:	Q_2.	(...)

□

Proofs by Contradiction

All of the types of proofs we have discussed so far are variants of direct proofs: we assume one or more hypotheses, and reason directly until we reach the desired conclusion(s). Now we will discuss a very different type of proof, called a *proof by contradiction* or an *indirect proof*. In this type of proof, we assume that the theorem statement is false and derive a contradiction.

An indirect proof can be used for any type of theorem. Here's the general template.

Template 9 (Proof by Contradiction)**.**

Theorem. Q.

Proof.

	Statement	**Reason**
	Assume $\neg Q$.	(hypothesis for contradiction)
	...	(...)
Goal:	Contradiction.	(...)
Conclusion:	Q.	

□

The "contradiction" can be any statement that is known to be false, but usually it is a statement of the form $R \wedge \neg R$, where R is any statement whatsoever.

The most common use of indirect proof is to prove an implication, such as $P \Rightarrow Q$. In that case, the hypothesis for contradiction is the negation of $P \Rightarrow Q$, which is $P \wedge \neg Q$. Thus we get to assume both that P is true and that Q is false. Since P is what we would normally assume for a direct proof, only the $\neg Q$ assumption needs to be labeled as a hypothesis for contradiction. The template looks like this.

Template 10 (Proof of an Implication by Contradiction)**.**

Theorem. $P \Rightarrow Q$.

Proof.

	Statement	**Reason**
	Assume P.	(hypothesis)
	Assume $\neg Q$.	(hypothesis for contradiction)
	...	(...)
Goal:	Contradiction.	(...)
Conclusion:	$P \Rightarrow Q$.	(logic)

□

Existence Proofs

Many important mathematical theorems are existence statements. A generic existence statement is one of the form "$(\exists y \in D)(Q(y))$." To prove such a statement, we need only show that there is one element y in D that satisfies the condition $Q(y)$. We get to choose or construct the element in any way that is convenient. Once we have chosen it, we then need to prove that it satisfies the condition $Q(y)$. Thus a proof of existence will typically have two parts: the first part describes how to construct or choose an appropriate element $y \in D$, and the second part proves that y has the desired properties.

This kind of proof is often called a *constructive proof*, because the object y whose existence is being asserted is sometimes "constructed," for example by giving a formula for it. Even if y is not really constructed, but is just chosen from among some already-existing set of objects, this type of proof

is still called a constructive proof as long as it gives a definite formula, rule, or algorithm for how to choose y. Here is a template.

Template 11 (Constructive Existence Proof)**.**

Theorem. $(\exists y \in D)(Q(y))$.

Proof.

	Statement	**Reason**
	Part 1: Choosing $y \in D$	
	...	(...)
	...	(...)
	Let $y = \ldots$.	(...)
	Part 2: Proof of $Q(y)$	
	...	(...)
	...	(...)
Goal:	$Q(y)$.	(...)

□

The first part of a constructive existence proof might require a little more ingenuity than other kinds of proofs, because there are no general guidelines about how to construct or choose an object that satisfies the desired conditions; you have to look at each particular situation and figure out how to use the given information to find an object of the right type.

Most often, an existence statement occurs as the conclusion of a different type of statement, such as a universal statement. Templates for such proofs are simply combinations of the template for an existence proof with the appropriate template for the enclosing statement. Here is a template for one of the most common types of existence theorems.

Template 12 (Universal Existence Proof)**.**

Theorem. $(\forall x \in E)(\exists y \in D)(Q(x, y))$.

Proof.

	Statement	**Reason**
	Let x be an arbitrary element of E.	(hypothesis)
	Part 1: Choosing $y \in D$	
	...	(...)
	...	(...)
	Let $y = \ldots$.	(...)
	Part 2: Proof of $Q(y)$	
	...	(...)
	...	(...)
Goal:	$Q(y)$.	(...)

□

The important feature of this template is that, due to the order in which the quantifiers appear, the universally quantified variable x is introduced first, and then you get to choose or construct y in a way that might depend on x; typically, different choices of x will result in different choices of y. For example, to prove the statement $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(y > x)$, we would start by letting x be an arbitrary real number, and then defining y by some formula involving x, such as $y = x + 1$.

Nonexistence Proofs

Closely related to existence proofs are proofs of *nonexistence statements*. For example, to show that the square root of 2 is irrational, we have to prove that there do not exist integers p and q such that $(p/q)^2 = 2$. Of course, a negated existence statement is equivalent to a universal statement: "For all integers p and q, $(p/q)^2 \neq 2$," so we could attempt to prove this universal statement. But it is almost always easier to prove nonexistence indirectly, by assuming that an object exists with the given properties and deriving a contradiction. Here is a template for the simplest case.

Template 13 (Nonexistence Proof)**.**

Theorem. $\neg(\exists y \in D)(Q(y))$.

Proof.

	Statement	**Reason**
	Assume $(\exists y \in D)(Q(y))$.	(hypothesis for contradiction)
	...	(...)
Goal:	Contradiction.	(...)

□

Uniqueness Proofs

We need one more kind of proof template: uniqueness proofs. You have seen uniqueness statements before; one example is Theorem 2 on our axioms list: *The numbers* 0 *and* 1 *in the identity axiom are unique*. The statement that 0 is unique means that if someone manages to come up with two numbers, say 0 and $0'$, that satisfy the conclusion of the identity axiom ("$0 + a = a + 0$ for every real number a and $0' + a = a + 0'$ for every real number a"), then it must be the case that $0 = 0'$.

A uniqueness statement always says that an object is the unique one *satisfying a certain property*. A statement like "the object $x \in D$ satisfying $P(x)$ is unique" is really a short way of saying "if x_1 and x_2 are elements of D that satisfy $P(x_1)$ and $P(x_2)$, then they are equal." (Note the implicit universal quantifier in this statement.) Symbolically, this can be written

$$\forall x_1, x_2 \in D, P(x_1) \wedge P(x_2) \Rightarrow x_1 = x_2. \tag{1}$$

It is important to understand the distinction between the mathematical terms "unique" and "distinct": to say that an object is the *unique* one satisfying a certain condition is to say that any two objects satisfying the same condition must be equal to each other; while to say that two or more objects are *distinct* is to say that they are *not* equal to each other. Mathematically, these terms are not interchangeable, even though in nonmathematical contexts, they are sometimes used interchangeably. For example, in computer science, one speaks of the number of "unique visitors" to a website during a certain period of time, meaning the number of *different* people who logged on to the site. A mathematician would prefer to call these "distinct visitors."

The symbolic statement (1) points the way to proving uniqueness statements. Here's a template.

Template 14 (Uniqueness Proof)**.**

Theorem. $\forall x_1, x_2 \in D, P(x_1) \wedge P(x_2) \Rightarrow x_1 = x_2$.

Proof.

	Statement	**Reason**
	Let $x_1, x_2 \in D$.	(hypothesis)
	Assume $P(x_1)$ and $P(x_2)$ are true.	(hypothesis)
	...	(...)
Goal:	$x_1 = x_2$	(...)

□

Uniqueness statements often come paired with existence statements, as in Theorem 95 on our axioms handout: "If a is any nonnegative real number, there is a unique nonnegative real number $\sqrt{a}$, called the ***square root of a***, such that $\left(\sqrt{a}\right)^2 = a$." In other words, for every nonnegative real number a, there *exists* a nonnegative number whose square is a, and it is the *unique* nonnegative number whose square is a. To prove this, you would start by letting a represent an arbitrary nonnegative real number, and first prove existence and then prove uniqueness.

An existence and uniqueness statement is often symbolized by adding an exclamation point after the symbol for "there exists"; thus "there exists a unique x in D such that $P(x)$" can be symbolized as

$$\exists! x \in D, P(x). \tag{2}$$

As always, the domain of the quantifier must be either specified or understood from the context. "Existence and uniqueness" is not really a new kind of quantifier; rather, it is just a shorthand for the conjunction of two separate statements, one asserting existence ("there exists at least one such x") and the other asserting uniqueness ("there exists at most one such x").