MATH 2135, LINEAR ALGEBRA, Winter 2013

Handout 2: What is a proof?

This handout summarizes some basic techniques used in "everyday" proofs. We use the usual logical notations $P \Rightarrow Q$ for "P implies Q", $\forall x \in A.P(x)$ for "for all $x \in A$, $P(x)$", $\exists x \in A.P(x)$ for "there exists an $x \in A$ such that $P(x)$". We also use the notation $P(x)$ for any statement involving a variable x.

The goal of a proof is to show that a given **conclusion** follows from some given **assumptions**. At any time during a proof, you have access to a number of facts that you "**already know**" (this includes assumptions, previously proved statements, theorems, definitions, and axioms), as well as a conclusion that you currently "**want to prove**". During the course of the proof, both what you know and what you want to prove continues to change, in response to the logical principles that you are applying. Note that "previously proved statements" does not include statements that were proved in a separate branch of the current case distinction, or facts that were proved from some temporary assumption that is no longer valid.

Mathematical proofs are constructed from a limited number of patterns of reasoning. The most important patterns are shown in the following tables.

Patterns for proving what you want to prove.

The patterns in the first table are governed by what you want to prove. You should always use them first, if you can. The parts in [*brackets*] must be filled in.

To prove:	you should follow this pattern:
$P \Rightarrow Q$	Assume P. [*Prove* Q]. Since we assumed P, this proves $P \Rightarrow Q$.
P and Q	First we prove P. [*Prove* P]. Then we prove Q. [*Prove* Q].
$\forall x \in A.P(x)$	Take an arbitrary $x \in A$. [*Prove* $P(x)$]. Since x was arbitrary, it follows that $\forall x \in A.P(x)$.
not P	Assume P. [*Derive a contradiction*]. Since we derived a contradiciton from assumption P, this shows that P is false.
$\exists x \in A.P(x)$	[*Describe a specific element* $a \in A$]. [*Prove that* $P(a)$ *is true*].
P or Q	Assume that both P and Q are false. [*Derive a contradiction*]. Therefore, either P or Q must be true.
P or Q (alternatively)	Assume that P is false. [*Prove* Q]. This shows that either P or Q is true.

Patterns for using what you already know.

If none of the patterns in the first table can be applied, you should examine what you already know, i.e., assumptions, axioms, previously proved statements, etc.. The following table shows how such facts can be used.

If you already know:	it can be used as follows:
$P \Rightarrow Q$	If you also know P, you may conclude Q.
P and Q	You may conclude P. You may also conclude Q.
$\forall x \in A.P(x)$	You may choose some particular $a \in A$, and conclude $P(a)$.
P and not P	This is a contradiction. Use it to conclude that the most recent assumption was false.
$a \neq a$	This is also a contradiction.
$\exists x \in A.P(x)$	You may give a new name to an (unknown) element $b \in A$ such that $P(b)$ holds. (You cannot choose b).
P or Q	You can do a case distinction. Suppose you currently want to prove some statement C. Case 1: Assume P. [*Prove* C]. Case 2: Assume Q. [*Prove* C]. Then you know C is true.
$a = b$	If you also know $P(a)$, you may conclude $P(b)$.

Pattens to use when everything else fails.

Here are a few additional reasoning patterns that you can use when all else fails.

To prove:	you can also follow this pattern:
P (by contradiction)	Assume that P is false. [*Derive a contradiction*]. Since we derived a contradiction from the assumption that P is false, it follows that P is true.
P (by case distinction)	(Here, Q is some statement). We distinguish two cases. Case 1: Q is true. [*Prove* P]. Case 2: Q is false. [*Prove* P]. Since we have proved P in both cases, it follows that P is true.
(to divide a long proof)	We first show P. [*Show* P]. We have shown P. (etc.)

One common use for a case distinction is when you want to do something that may not be allowed. For example, suppose you want to divide something by a, where a is an unknown number. Since you don't know whether $a = 0$, you don't know if you can divide by a or not. A case distinction allows you to proceed: Case 1: $a \neq 0$. [*Go ahead and divide by* a]. Case 2: $a = 0$. [*Prove it some other way*].

Using definitions.

Writing mathematical proofs also requires the use of definitions. In fact, a mathematical subject (such as linear algebra) can have hundreds of definitions. Definitions usually take the form of abbreviations. For example,

$P \Leftrightarrow Q$	is an abbreviation for	$P \Rightarrow Q$ and $Q \Rightarrow P$;
$A \subseteq B$	is an abbreviation for	$\forall x.(x \in A \Rightarrow x \in B)$;
$A = B$ (for sets)	is an abbreviation for	$A \subseteq B$ and $B \subseteq A$;
$f = g$ (for functions)	is an abbreviation for	$\forall x.f(x) = g(x)$;
$a \in A \cap B$	is an abbreviation for	$a \in A$ and $a \in B$;
$a \in A \cup B$	is an abbreviation for	$a \in A$ or $a \in B$;
$a \in \{x \mid P(x)\}$	is an abbreviation for	$P(a)$;
$a \in f^{-1}(Y)$	is an abbreviation for	$f(a) \in Y$;

and so on. Therefore, to prove $P \Leftrightarrow Q$, you have to prove $P \Rightarrow Q$ and $Q \Rightarrow P$. Following the patterns from the first table, we often write: "To prove the left-to-right implication, assume P. [*Prove* Q]. Conversely, assume Q. [*Prove* P]".

Similarly, to prove $A \subseteq B$, you have to prove $\forall x.(x \in A \Rightarrow x \in B)$. Following the patterns of the first table, we often write: "To prove $A \subseteq B$, let $x \in A$ be an arbitrary element. We have to prove $x \in B \ldots$".

More complex definitions, for example "K is a field", can be abbreviations for a much longer list of axioms. To prove that something is a field, you have to prove the axioms. On the other hand, if you are given a field, you may use the axioms.

Completeness of the logical rules.

It is an interesting fact that the reasoning patterns in the preceding tables, along with the axioms of set theory, are sufficient to do *any* mathematical proof. This fact is proved in a course on formal logic, such as PHIL 3140.