MATH 582, INTRODUCTION TO SET THEORY, WINTER 1999

What is a proof?

Mathematics is a dual activity. We *think* in terms of intuitions and visualizations, but we *prove* things from axioms and definitions via logical reasoning. But what exactly are proofs? How do we know our reasoning is logical? Proofs can be defined very precisely and in a formal way; this is done in a logic course. In this set theory course, we have been precise about what *formulas* are, but we will be somewhat more informal about proofs. Still, there are certain patterns that occur over and over in mathematical proofs; for instance, to prove a statement of the form $\forall x.P(x)$, we take an arbitrary x and then prove $P(x)$. To prove $P \Rightarrow Q$, we assume P and then prove Q. The following table summarizes some expressions that are commonly used in proofs. The parts in [*brackets*] must be filled in.

To prove:		you might do the following:
$P \Rightarrow Q$		Assume P. [*Prove* Q]. Since we assumed P, this proves $P \Rightarrow Q$.
	Or:	Assume $\neg Q$. [*Prove* $\neg P$]. We have proved $\neg Q \Rightarrow \neg P$, which, by taking the contrapositive, implies $P \Rightarrow Q$.
$P \wedge Q$		[*Prove* P]. [*Prove* Q]. Therefore $P \wedge Q$.
$\forall x.P(x)$		Consider an arbitrary x. [*Prove* $P(x)$]. Since x was arbitrary, this proves $\forall x.P(x)$.
$\neg P$		Assume P. [*Derive a contradiction*]. The assumption P led to a contradiction, therefore we have shown $\neg P$.
$\exists x.P(x)$		[*Construct an object* a]. [*Prove* $P(a)$]. We have shown $P(a)$, hence $\exists x.P(x)$.
$P \vee Q$		[*Prove* P]. Therefore we have $P \vee Q$.
	Or:	[*Prove* Q]. Therefore we have $P \vee Q$.
	Or:	Case distinction: If P, we are done proving $P \vee Q$. Assume that, on the contrary, $\neg P$. [*Prove* Q]. In either case, we have shown $P \vee Q$.
P (by contradiction)		Assume $\neg P$. [*Derive a contradiction*]. The assumption $\neg P$ led to a contradiction, thus we have proved P.
P (by case distinction)		(Here, Q is some formula). We distinguish two cases. Case 1: Q holds. [*Prove* P]. Case 2: $\neg Q$ holds. [*Prove* P]. In either case, we have proved P.
(to divide a long proof)		We will first show P. [*Show* P]. We have shown P. (etc.)

Another question is how you can *use* assumptions, hypotheses, and axioms, as well as statements that you have previously proved:

The statement:	can be used as follows:
$P \Rightarrow Q$	If you know P, you may conclude Q.
$P \wedge Q$	You may conclude P. You may also conclude Q.
$\forall x.P(x)$	You may conclude $P(a)$, for any a of your choosing.
$\neg P$	If you also know P, you may derive a contradiction.
$\exists x.P(x)$	You may introduce a new name b for some set that satisfies $P(b)$.
$P \vee Q$	You may prove any formula C by a case distinction as follows: Assume P. [*Prove* C]. Now assume Q. [*Prove* C]. In either case, we have proved C.
$a = b$	If you know $P(a)$, you may conclude $P(b)$.

The only primitive concepts in set theory are that of set and element. All other concepts are *defined*, i.e. they have been introduced as abbreviations. If you are proving something about such a defined concept, then you have to use the definition. For instance:

To prove:	you have to show:
$a \subseteq b$	$\forall x(x \in a \Rightarrow x \in b)$.
$a = b$ (for sets)	$\forall x(x \in a \Rightarrow x \in b)$ and $\forall x(x \in b \Rightarrow x \in a)$ (by extensionality).
$x \in a \cap b$	$x \in a$ and $x \in b$.
$x \in \bigcup A$	$\exists z(x \in z \wedge z \in A)$.
$x \in \mathcal{P}A$	$x \subseteq A$.

and so on. Of course, you may also use any lemmas that you have previously proved, that have been proved in class, etc.

Notice the difference between (1) a *hypothetical* assumption, and (2) using something that you already know. For example, if you want to prove $x \in A \Rightarrow x \in B$, then you *assume* $x \in A$ and proceed to show $x \in B$. At this point, you do not need to be concerned about whether such an $x \in A$ actually exists; you are simply proving something about a *hypothetical* $x \in A$. On the other hand, suppose you already know (or you have previously assumed) that a certain set A is non-empty. In this case, you are allowed to *pick* some $b \in A$ and use that element b in your further proof. Here, the assumption that $b \in A$ is *not* hypothetical; you are simply giving the name "b" to something that you already know exists. But to be allowed to do this, you need to know ahead of time that A is non-empty.

As an example, let us consider a proof of the simple statement

$$\forall A \forall x (x \in A \Rightarrow x \subseteq \bigcup A).$$

If you want to be extremely verbose, you could write the following proof.

	We want to show $\forall A \forall x (x \in A \Rightarrow x \subseteq \bigcup A)$.
	Consider an arbitrary A.
(*)	We will prove $\forall x (x \in A \Rightarrow x \subseteq \bigcup A)$.
	Consider an arbitrary x.
(*)	We will prove $x \in A \Rightarrow x \subseteq \bigcup A$.
	Assume $x \in A$.
(*)	We will prove $x \subseteq \bigcup A$.
(*)	By definition of $\subseteq$, we have to show $\forall z (z \in x \Rightarrow z \in \bigcup A)$.
	Consider an arbitrary z.
(*)	We will prove $z \in x \Rightarrow z \in \bigcup A$.
	Assume $z \in x$.
(*)	We will prove $z \in \bigcup A$.
(*)	By definition of $\bigcup A$, we have to show $\exists b (z \in b \wedge b \in A)$.
	We know that $z \in x$ and $x \in A$.
(*)	Thus, taking $b = x$, we have proved $\exists b (z \in b \wedge b \in A)$.
	Thus, we have proved $z \in \bigcup A$.
(*)	Since we assumed $z \in x$, we have proved $z \in x \Rightarrow z \in \bigcup A$.
	Since z was arbitrary, (*) we have proved $\forall z (z \in x \Rightarrow z \in \bigcup A)$.
	This shows $x \subseteq \bigcup A$.
(*)	Since we have assumed $x \in A$, we have proved $x \in A \Rightarrow x \subseteq \bigcup A$.
(*)	Since x was arbitrary, this proves $\forall x (x \in A \Rightarrow x \subseteq \bigcup A)$.
(*)	Since A was arbitrary, this proves $\forall A \forall x (x \in A \Rightarrow x \subseteq \bigcup A)$.
	So we are done.

Obviously, this proof is very redundant and tedious. Since your proofs will probably be read by people, and not by computers, you can leave some things implicit. For instance, if we omit all the parts marked (*), we get a much more readable proof.

> We want to show $\forall A \forall x (x \in A \Rightarrow x \subseteq \bigcup A)$.
> Consider arbitrary A and x such that $x \in A$.
> Consider an arbitrary $z \in x$.
> We know that $z \in x$ and $x \in A$.
> Thus, by definition of $\bigcup A$, we have proved $z \in \bigcup A$.
> Since z was arbitrary, this shows $x \subseteq \bigcup A$, by definition of $\subseteq$.
> We are done.

Usually, one will be even more concise and write, for instance:

> We want to show $\forall A \forall x (x \in A \Rightarrow x \subseteq \bigcup A)$. So let $x \in A$. Then for any $z \in x$, by definition of union, we have $z \in \bigcup A$. Thus, by definition of subset, $x \subseteq \bigcup A$, and we are done.

For another discussion of logic and proofs, see the Appendix in Enderton (p.263ff).