Math 220
October 9, 2003

To PROVE a statement of the form....
In each case below, we assume we want to prove a statement of the given form. Some forms can be handled by more than one technique.

- $P \wedge Q$: Prove both P and Q.
- $\neg P$: Usually this comes in the form of "prove P is false." Determine the negation of P and then prove this new statement.
- $P \Rightarrow Q$: (Direct) Assume that P is true. Under this assumption prove that Q is true.
- $P \Rightarrow Q$: (Contrapositive) Assume that Q is false. Under this assumption prove that P is false.
- $P \Rightarrow Q$: (Convert to $\vee$) $P \Rightarrow Q$ is equivalent to $\neg P \vee Q$, so can use techniques for OR statements.
- $P \Leftrightarrow Q$: This is the same as $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$, so prove $P \Rightarrow Q$ and then prove $Q \Rightarrow P$.
- $P \vee Q$: (Method 1) Use a proof by cases (see below). In each case, either prove P or prove Q. Usually you would do this if your OR statement is combined with a FOR ALL statement: e.g., $\forall x, P(x) \vee Q(x)$.
- $P \vee Q$: (Method 2) Assume $\neg P$ is true. Under this assumption prove that Q is true. (Or assume that $\neg Q$ is true, and then prove that P is true.)
- $P \vee Q$: (Convert to $\Rightarrow$) Since $P \vee Q$ is equivalent to $\neg P \Rightarrow Q$, can use techniques for IF...THEN statements. This is essentially the same as Method 2, but rewritten as an implication the statement might convey more meaning.
- $\forall x \in U, P(x)$: Let x represent an arbitrary, unspecified element of U. Then prove $P(x)$ is true for this x.
- $\exists x \in U$ so that $P(x)$: Find a specific $x_0 \in U$ so that you can prove $P(x_0)$ is true. That is, your proof should have the form "Let $x = x_0$. ...Proof proof proof proof... Therefore, $P(x_0)$ is true."

Other methods of proof:

- **Proof by cases:** Usually this is useful in proving a statement of the form "$\forall x \in U, P(x)$." To prove by cases, break U up into pieces, and then prove $P(x)$ for an arbitrary x in each piece.

  For example, if you want to prove "$\forall x \in \mathbb{Z}$, $x^2 - x$ is even," you first let $x \in \mathbb{Z}$ be arbitrary. Then

  - Case 1: x is even. Then prove $x^2 - x$ is even in this case.
  - Case 2: x is odd. Then prove $x^2 - x$ is even in this case.

- **Proof by contradiction:** Suppose that P is the statement that you want to prove. Proof by contradiction then works in the following way.

  - You first assume that P is false.
  - Then under this assumption, you want to derive a contradiction. That is, find a statement Q such that both Q and $\neg Q$ are true.

  A contradiction is of course is a worrisome thing, since every statement is either true or false, and if a statement is true, it's negation is false and vice versa. Thus, once we find a contradiction, it must have been our assumption that P is false that led us astray, and so in fact it must be that P is true.

- **Proof by induction:** This is the subject of section 5.2 in Bond & Keane.

To USE a statement of the form....

That is, you are given or have already proven that a statement is true. How do you then use it to deduce the truth of other statements?

In each case below, we are assuming that we have a statement of the given form. What can we deduce?

- $P \wedge Q$: This just means that P is true and Q is true.
- $\neg P$: If $\neg P$ is true, then write out the negation of P, which is now a true statement and use it.
- $P \Rightarrow Q$: (Direct) If you also know that P is true or can prove that P is true, then having both $P \Rightarrow Q$ and P true implies that Q must be true also. So showing that P is true will allow you to conclude Q is true.
- $P \Rightarrow Q$: (Contrapositive) If you also know or can prove that Q is false, then you can conclude that P is false.
- $P \Leftrightarrow Q$: This means that both $P \Rightarrow Q$ and $Q \Rightarrow P$ are true. It also means that P and Q are either both true or both false.
- $P \vee Q$: Break into cases. Case 1: P is true. Case 2: Q is true.
- $\forall x \in U, P(x)$: This means that any time you have a element $y \in U$, you can conclude that $P(y)$ is true.
- $\exists x \in U$ so that $P(x)$: This only means existence. So you can conclude that there is a specific element $y \in U$ so that $P(y)$ is true. (Though we may not actually know the specific value of y.)