For theorems like:	You might try:	In which case, write:	And then prove:	Special notes
$\forall x \in D, P(x)$.	WLOG	"WLOG, let x be an element of D."	$P(x)$.	Don't assume anything about x that isn't true of all elements of D.
	Exhaustion	"We proceed by exhaustion over D."	$P(d)$ for each element d in D.	Only works for finite domains. (Really just proof by cases.)
	Cases	"Note that $Q(x)$ or $R(x)$ must be true."	$\forall x \in D, Q(x) \to P(x)$ and $\forall x \in D, R(x) \to P(x)$.	$Q(x)$, $R(x)$, or both must be true of each d in D. You can break D into more than two pieces, like breaking $\mathbf{Z}^+$ into primes, composites, and 1.
$\exists x \in D, P(x)$.	Witness	"Let $x = d$, a particular element of D."	$P(d)$	Pick d to be convenient for your proof! In particular, leave a blank for d and fill it in later once you know what a "convenient" value is.
$p \to q$.	Antecedent assumption	"Assume p."	q	**Very** common approach to conditionals.
p (so, any theorem!)	Contradiction	"Assume $\sim p$ (for contradiction)."	F, a contradiction	Best when you can make few useful assumptions with more direct techniques.
$p \wedge q$	Conjunction		Prove p. Then, prove q.	These are two separate proofs.
$p \vee q$	Generalization		Prove p and generalize.	Or prove q and generalize, instead.
$\sim p$	Disproof		Disprove p.	Usable on any statement (with double negation).
$a = b$	Equality proof	Consider: $a = ??$ $\dots$ $= b$.		In scratch work, you can: work from both sides to the middle; divide/multiply the equation by something; solve for a variable; ... **but** work from one side to the other in your formal proof!
$a < b$ (or $a > b$)	Strict inequality proof	Consider: $a < ??$ $= ??$ $\dots$ $\leq b$.	Note: mix $<$, $=$, and $\leq$ steps however you like except that there must be **at least one** $<$ step. **Never** take a $>$ or $\geq$ step.	As with equalities, try anything you like in scratch work, but work from one side to the other in your formal proof. Beware of multiplying/dividing by negative values—which flip the inequality—or dividing by zero.
$a \leq b$ (or $a \geq b$)	Inequality proof	Consider: $a < ??$ $= ??$ $\dots$ $\leq b$.	Note: Just as with strict inequality, except that you aren't **required** to take a $<$ step.	Proving "a less than or equal to b" is proving "a less than b" **OR** "a equals b". So, if you prove either one, you can generalize to "a is less than or equal to b".
$P(d)$ with a definition for P			Prove the result of plugging d into P's definition.	

Put these strategies together! To prove $\forall x \in D, \exists y \in E, P(x) \to Q(y)$, you might: use WLOG on x, leaving $\exists y \in E, P(x) \to Q(y)$; use witness on y (choosing y based on x), leaving $P(x) \to Q(y)$; and finally, assume $P(x)$, leaving $Q(y)$. (You need P and Q's definitions to go further.)

Got assumptions/premises with quantifiers? (Like in proof by contradiction?)

When you assume $\forall x \in D, P(x)$, you know $P(d)$ is true for any d in D that you want (and however many d you want). Whatever's convenient.

When you assume $\exists x \in D, P(x)$, you only know there's **some** d in D for which P holds. You don't know which one. So, you can give it a name like d and say "Based on $\exists x \in D, P(x)$, I know $P(d)$ holds for some d in D.", but you **cannot** assume anything about d that isn't true of **every** element in D.

(Note: this is roughly the reverse of how the quantifier's proofs proceed.)

Use logical equivalences to rearrange a theorem or premise! Particularly handy: move negations inward, change $\to$ to $\vee$, and try the contrapositive of $\to$. To prove a biconditional, turn it into two conditionals—$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$—and then prove each individually.

Don't know whether to prove or disprove a theorem? Try proving for a while, then switch to disproving (proving the negation) for a while, and repeat until you figure it out. Keep scratch work from both! While proving, **believe with all your heart** that it's true. While disproving, **believe with all your heart** that it's false. Humans work better that way!

For a theorem like $\forall x \in D, \text{IsAFoo}(x) \to Q(x)$: (1) The Epp textbook says to assume x is a Foo, and prove $Q(x)$. This tip sheet agrees: WLOG and then antecedent assumption: "Without loss of generality, let x be a member of D. Assume $\text{IsAFoo}(x)$. ..." (2) Proof by cases is often handy!

CPSC 121 Proof Strategy Tips
Steve Wolfman, July 16, 2012

Not Getting Stuck: Stop yourself after a few minutes, check what you're trying to prove and how it compares to what you're doing right now. Be sure you're making progress. If not, change strategies... but keep your old notes!

Frequently Asked Questions: Can I move a quantifier outward (or inward)? With caution:

- Move quantifiers across negations using generalized De Morgan's (flip universals to existentials and vice versa).
- **Beware:** the antecedent (left-hand side) of a conditional has a "hidden negation" on it. (Why? Convert it to an $\vee$ to see.)
- Don't move quantifiers into or out of $\leftrightarrow$ or $\oplus$! (They both have and *don't* have "hidden negations".)
- If two quantifiers quantify the same variable name, rename one of the variables and all of its occurrences so they're different.
- You can swap directly neighbouring quantifiers of the same type (e.g., both universals), but *not* a universal and an existential.

What are those "predicate logic idioms"?

- "At least one..." $\Rightarrow \exists \ldots$
- "At least two..." $\Rightarrow \exists a \ldots, \exists b \ldots, a \neq b \wedge \ldots$
- "At most one..." $\Rightarrow$ negation of "at least two"
- "Exactly one..." $\Rightarrow$ "at least one" and "at most one"
- Restricting the domain of a universal (e.g., "all even integers") $\Rightarrow \forall \ldots, \textit{restriction} \to \ldots$ (e.g., "$\forall x \in \mathbf{Z}, (\exists k \in \mathbf{Z}, 2k = x) \to \ldots$)
- Restricting the domain of an existential (e.g., "some even integer") $\Rightarrow \exists \ldots, \textit{restriction} \wedge \ldots$ (e.g., "$\exists x \in \mathbf{Z}, (\exists k \in \mathbf{Z}, 2k = x) \wedge \ldots$")