Velleman

Malcolm

Started 6th September 2025

Contents

Chapter 1

Logic

1.0.1 Logic Factsheet

De Morgan's laws

$$\neg\,(P \wedge Q) \text{ is equivalent to } \neg\,P \vee \neg\,Q$$
$$\neg\,(P \vee Q) \text{ is equivalent to } \neg\,P \wedge \neg\,Q$$

Commutative laws

$$P \wedge Q \text{ is equivalent to } Q \wedge P$$
$$P \vee Q \text{ is equivalent to } Q \vee P$$

Associative laws

$$P \wedge (Q \wedge R) \text{ is equivalent to } (P \wedge Q) \wedge R$$
$$P \vee (Q \vee R) \text{ is equivalent to } (P \vee Q) \vee R$$

Indempotent laws

$$P \wedge P \text{ is equivalent to } P$$
$$P \vee P \text{ is equivalent to } P$$

Distributive laws

$$P \wedge (Q \vee R) \text{ is equivalent to } (P \wedge Q) \vee (P \wedge R)$$
$$P \vee (Q \wedge R) \text{ is equivalent to } (P \vee Q) \wedge (P \vee R)$$

Absorption laws

$$P \vee (P \wedge Q) \text{ is equivalent to } P$$
$$P \wedge (P \vee Q) \text{ is equivalent to } P$$

Double Negation law

$$\neg\neg\,P \text{ is equivalent to } P$$

1.0.2 Set operation definitions

The *intersection* of two sets A and B is the set $A \cap B$ defined as follows:

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}$$

The *union* of A and B is the set $A \cup B$ defined as follows:

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}$$

The *difference* of A and B is the set $A \setminus B$ defined as follows:

$$A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}$$

See that

$$x \in A \cap B = x \in \{y \mid y \in A \text{ and } y \in B\}$$

where y is a dummy variable. So we can also write that

$$x \in A \cap B = x \in A \wedge x \in B$$

The same can be shown for the union and difference.

1.0.3 Distributivity of set operations

We show

$$x \in A \cap (B \cup C) \text{ is equivalent to } x \in (A \cap B) \cup (A \cap C)$$

By analysing their logical forms:

$$\begin{aligned} & x \in A \cap (B \cup C) \\ & = x \in A \wedge x \in (B \cup C) \\ & = x \in A \wedge (x \in B \vee x \in C) \end{aligned}$$

and

$$\begin{aligned} & x \in (A \cap B) \cup (A \cap C) \\ & = x \in (A \cap B) \vee x \in (A \cap C) \\ & = (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \\ & = [(x \in A \wedge x \in B) \vee x \in A)] \wedge [(x \in A \wedge x \in B) \vee x \in C)] \\ & = x \in A \wedge [(x \in A \vee x \in C) \wedge (x \in B \vee x \in C)] \\ & = [x \in A \wedge (x \in A \vee x \in C)] \wedge (x \in B \vee x \in C) \\ & = x \in A \wedge (x \in B \vee x \in C) \end{aligned}$$

We can also show, in a similar manner, that

$$x \in A \cup (B \cap C) \text{ is equivalent to } x \in (A \cup B) \cap (A \cup C)$$

1.0.4 $x \in A \setminus (B \cap C) = x \in (A \setminus B) \cup (A \setminus C)$

We can also show

$$x \in A \setminus (B \cap C) = x \in (A \setminus B) \cup (A \setminus C)$$

See that

$$\begin{aligned}
& x \in A \setminus (B \cap C) \\
&= x \in A \wedge \neg (x \in B \cap C) && \text{(Definition of } \setminus\text{)} \\
&= x \in A \wedge \neg (x \in B \wedge x \in C) && \text{(Definition of } \cap\text{)} \\
&= x \in A \wedge (x \notin B \vee x \notin C) && \text{(De Morgan's)} \\
&= (x \in A \wedge x \notin B) \vee (x \in A \wedge x \notin C) && \text{(Distributivity)} \\
&= (x \in A \setminus B) \vee (x \in A \setminus C) && \text{(Definition of } \setminus\text{)} \\
&= x \in (A \setminus B) \cup (A \setminus C) && \text{(Definition of } \cup\text{)}
\end{aligned}$$

1.0.5 $x \in (A \cup B) \setminus (A \cap B) = x \in (A \setminus B) \cup (B \setminus A)$

$$\begin{aligned}
& x \in (A \cup B) \setminus (A \cap B) \\
&= (x \in A \vee x \in B) \wedge \neg (x \in A \wedge x \in B) && \text{(By definition)} \\
&= (x \in A \vee x \in B) \wedge (x \notin A \vee x \notin B) && \text{(De Morgan's)} \\
&= [(x \in A \vee x \in B) \wedge (x \notin A)] \\
&\qquad \vee [(x \in A \vee x \in B) \wedge (x \notin B)] && \text{(Distributivity)} \\
&= [(x \notin A \wedge x \in A) \vee (x \notin A \wedge x \in B)] \\
&\qquad \vee [(x \notin B \wedge x \in A) \vee (x \notin B \wedge x \in B)] && \text{(Distributivity)} \\
&= (x \notin A \wedge x \in B) \vee (x \notin B \wedge x \in A) \\
&= (x \in A \wedge x \notin B) \wedge (x \in B \wedge x \notin A) && \text{(Commutativity)} \\
&= x \in (A \setminus B) \cup (B \setminus A) && \text{(By definition)}
\end{aligned}$$

1.0.6 $(A \cap B) \cap (A \setminus B) = \emptyset$

See that

$$\begin{aligned}
& x \in (A \cap B) \cap (A \setminus B) \\
&= (x \in A \wedge x \in B) \wedge (x \in A \wedge x \notin B) && \text{(Definition)} \\
&= x \in A \wedge \underbrace{(x \in B \wedge x \notin B)}_{\text{Contradiction}} && \text{(Associativity + Commutativity)}
\end{aligned}$$

The last statement is a contradiction, so the statement $x \in (A \cap B) \cap (A \setminus B)$ will always be false, no matter what x is. In other words, nothing can be an element of $(A \cap B) \cap (A \setminus B)$, so it must be the case that $(A \cap B) \cap (A \setminus B) = \emptyset$; $A \cap B$ and $A \setminus B$ are disjoint.

1.0.7 Conditional and Contrapositive laws

Conditional Law

$$P \to Q \text{ is equivalent to } \neg\,(P \wedge \neg\, Q)$$

by De Morgan's law we can also say that

$$P \to Q \text{ is equivalent to } \neg\, P \vee Q$$

Contrapositive law

$$P \to Q \text{ is equivalent to } \neg\, Q \to \neg\, P$$

This can be justified using

$$P \to Q = \neg\,(P \wedge \neg\, Q) = \neg\,(\neg\, Q \wedge P) = \neg\, Q \to \neg\, P$$

Intuition
Intuitive ways to think of $P \to Q$ (and equivalently $\neg\, Q \to \neg\, P$) include:

- P implies Q.
- Q, if P.
- P only if Q.
- P is a sufficient condition for Q.
- Q is a necessary condition for P.

1.0.8 Biconditional statements

We write

$$P \leftrightarrow Q = (P \rightarrow Q) \wedge (Q \rightarrow P)$$

Note that by the contrapositive law, this is also equivalent to

$$(P \rightarrow Q) \wedge (\neg P \rightarrow \neg Q)$$

Intuition
$Q \rightarrow P$ can be written as 'P if Q' and $P \rightarrow Q$ can be written as 'P only if Q' (since this means $\neg Q \rightarrow \neg P$ which is $P \rightarrow Q$).

Combining the two as $(P \rightarrow Q) \wedge (Q \rightarrow P) = P \leftrightarrow Q$ therefore corresponds to the statement 'P if and only if Q'.

$P \leftrightarrow Q$ means 'P iff Q', or 'P is a necessary and sufficient condition for Q'.

1.1 Quantificational logic

1.1.1 Quantifier negation laws

We have

$$\neg\exists x P(x) \text{ is equivalent to } \forall x \neg P(x)$$
$$\neg\forall x P(x) \text{ is equivalent to } \exists x \neg P(x)$$

Intuition
No matter what $P(x)$ stands for, the formula $\neg\exists x P(x)$ means that there is no value of x for which $P(x)$ is true; this is ths same as saying that for every value of x in the universe of discourse, $P(x)$ is false—meaning $\forall x \neg P(x)$.

Similarly, to say that $\neg\forall x P(x)$ means that it is not the case that for all values of x, $P(x)$ is true. This is equivalent to saying that that there is at least one value of x for which $P(x)$ is false—so $\exists x \neg P(x)$.

1.1.2 Notation

'Exactly one' notation
We write

$$\exists! x P(x) = \exists x (P(x) \wedge \neg\exists y (P(y) \wedge y \neq x))$$

As a shorthand way to write 'there is exactly one value of x such that $P(x)$ is true', or 'there is a unique x such that $P(x)$'.

Specifying quantifiers
We write

$$\forall x \in A\, P(x)$$

to mean that *for every value of x in the set A, $P(x)$ is true.* Similarly,

$$\exists x \in A\, P(x)$$

means *there is at least one value of x in the set A such that $P(x)$ is true.*

Formulas containing bounded quantifiers can also be thought of as abbreviations for more complicated formulas containing only normal, unbounded quantifiers. See that

$$\forall x \in A\, P(x) = \forall x (x \in A \to P(x))$$

and

$$\exists x \in A\, P(x) = \exists x (x \in A \wedge P(x))$$

1.1.3 Negation law for bounded quantifiers

We can show

$$\neg\forall x \in A\, P(x) = \exists x \in A\, \neg P(x)$$

See that

$$\begin{aligned}
&\neg\forall x \in A\, P(x) && \\
&= \neg\forall x(x \in A \to P(x)) && \text{(as defined)} \\
&= \exists x\neg(x \in A \to P(x)) && \text{(negation law)} \\
&= \exists x\neg\neg(x \in A \wedge \neg P(x)) && \text{(conditional law)} \\
&= \exists x(x \in A \wedge \neg P(x)) && \\
&= \exists x \in A\, \neg P(x) && \text{(as defined)}
\end{aligned}$$

Similarly we can show

$$\neg\exists x \in A\, P(x) = \forall x \in A\, \neg P(x)$$

See that

$$\begin{aligned}
&\neg\exists x \in A\, P(x) && \\
&= \neg\exists x(x \in A \wedge P(x)) && \text{(as defined)} \\
&= \forall x\neg(x \in A \wedge P(x)) && \text{(negation law)} \\
&= \forall x(x \in A \to \neg P(x)) && \text{(conditional law)} \\
&= \forall x \in A\, \neg P(x) && \text{(as defined)}
\end{aligned}$$

1.1.4 Vacuously true

It is clear that if $A = \emptyset$ then $\exists x \in A\, P(x)$ will be false regardless of $P(x)$, since there is nothing in A that makes $P(x)$ come true (since there is nothing in A to being with).

Now consider $\forall x \in A\, P(x)$. We can reason that

$$\forall x \in A\, P(x) = \neg \exists x \in A\, \neg P(x) \quad \text{(quantifier negation)}$$

See that if $A = \emptyset$ then this formula will be true, no matter what $P(x)$ is. In this case we say that the statement is *vacuously true*.

Another way to see this is to rewrite

$$\forall x \in A\, P(x) = \forall x (x \in A \to P(x))$$

The only way this can be false is if there is some value of x such that $x \in A$ is true but $P(x)$ false; but there is no such value of x. Intuitively, because the condition cannot be met, it is impossible to provide a counterexample to prove something wrong.

An analogy would be me claiming 'i've never lost a race to Usain Bolt'. This is true, but vacuously so.

1.1.5 Alternate definition for indexed families

Say we are looking for the set $\{p_1, p_2, \ldots, p_{100}\}$; another way of describing this set would be to say that it consists of all numbers p_i, for i an element of the set $I = \{1, 2, 3, \ldots, 100\} = \{i \in \mathbb{N} | 1 \leq i \leq 100\}$. We can write

$$P = \{p_i | i \in I\}$$

Each element p_i in this set is identified by $i \in I$, called the *index* of each element. A set defined this way is called an *indexed family*, and I the *index set*. Although the indices for an indexed family are often numbers, they need not be.

In general, see that any indexed family

$$A = \{x_i | i \in I\}$$

Can also be defined as

$$A = \{x | \exists i \in I \, (x = x_i)\}$$

It follows that the statement

$$x \in \{x_i | i \in I\}$$

means the same thing as

$$\exists i \in I \, (x = x_i)$$

1.1.6 Power set

Suppose A is as set. The *power set* of A, denoted $\mathscr{P}(A)$, is the set whose elements are all subsets of A. In other words,

$$\mathscr{P}(A) = \{x | x \subseteq A\}$$

For instance, the set $A = \{7, 12\}$ has four subsets $\emptyset, \{7\}, \{12\}$, and $\{7, 12\}$; thus, $\mathscr{P}(A) = \{\emptyset, \{7\}, \{12\}, \{7, 12\}\}$.

1.1.7 Intersection and union of a family of sets

Suppose $\mathcal{F}$ is a family of sets. The *intersection* and *union* of $\mathcal{F}$ are the sets $\bigcap \mathcal{F}$ and $\bigcup \mathcal{F}$ are defined as follows:

$$\bigcap \mathcal{F} = \{x | \forall A \in \mathcal{F}(x \in A)\} = \{x | \forall A(A \in \mathcal{F} \to x \in A)\}$$
$$\bigcup \mathcal{F} = \{x | \exists A \in \mathcal{F}(x \in A)\} = \{x | \exists A(A \in \mathcal{F} \wedge x \in A)\}$$

Notice that if A and B are any two sets and $\mathcal{F} = \{A, B\}$, then $\bigcap \mathcal{F} = A \cap B$ and $\bigcup \mathcal{F} = A \cup B$; the definitions of intersection and union of a family of sets are generalisations of our old definitions of the intersection and union of two sets.

Alternative notation
An alternative notation is sometimes used for the union or intersection of an indexed family of sets. Suppose $\mathcal{F} = \{A_i | i \in I\}$, where each A_i is a set, then $\bigcap \mathcal{F}$ and $\bigcup \mathcal{F}$ could also be written as $\bigcap_{i \in I} A_i$ and $\bigcup_{i \in I} A_i$; as such

$$\bigcap \mathcal{F} = \bigcap_{i \in I} A_i = \{x | \forall i \in I(x \in A_i)\}$$
$$\bigcup \mathcal{F} = \bigcup_{i \in I} A_i = \{x | \exists i \in I(x \in A_i)\}$$

1.1.8 More on set notation

One generally defines a set using the elementhood test notation

$$\{x|P(x)\}$$

Where the set consists of all x that satisfy the specified condition $P(x)$. Sometimes this notation can be modified to allow the x before the vertical line to be replaced with a more complex expression. For example, suppose we wanted to define S to be the set of all perfect squres, we could write

$$S = \{n^2|n \in \mathbb{N}\}$$

This is the same as

$$S = \{x|\exists n \in \mathbb{N}(x = n^2)\}$$

See therefore that

$$x \in \{n^2|n \in \mathbb{N}\} = \exists n \in \mathbb{N}(x = n^2)$$

Chapter 2

Proof Strategies

2.0.1 Terminology

We want to state the answer to a mathematical question in the form of a *theorem* that says that if certain assumptions called the *hypotheses* of the theorem are true, then some conclusion must also be true.

An assignment of particular values to these variables is called an *instance* of the theorem, and in order for the theorem to be correct it must be the case that for every instance of the theorem that makes the hypotheses come out true, the conclusion is also true.

If there is even one instance in which the hypotheses are true but the conclusion is false, then the theorem is incorrect; such an instance is called a *counterexample* to the theorem.

As in the next section, we will refer to statements that are known or assumed to be true at some point in the course of figuring out the proof as *givens*, and the statements that remains to be proven at that point as the *goal*.

2.1 To prove a conclusion of the form $P \to Q$

To prove a conclusion of the form $P \to Q$, we can *assume P is true and then prove Q*.

Assuming that P is true amounts to adding P to the lists of hypotheses. If the conclusion of the theorem we are trying to prove has the form $P \to Q$, then we can *transform the problem* by adding P to the list of hypotheses and changing the conclusion form $P \to Q$ to Q.

How we solve this new problem will now then be guided by the logical form of the new conclusion Q, and perhaps also that of the new hypothesis P.

This strategy is one that proves the *goal* of $P \to Q$. Even if the conclusion of a theorem is not a conditional statement, if we transform the problem in such a way that the conditional statement becomes the goal, then we can apply this strategy as the next step in figuring out the proof.

Example:

Theorem. *Suppose a and b are real numbers. If $0 < a < b$ then $a^2 < b^2$.*

Proof. Suppose $0 < a < b$. Multiplying the inequality $a < b$ by the positive number a we can conclude that $a^2 < ab$; similarly multiplying by b we get $ab < b^2$. Therefore $a^2 < ab < b^2$, so $a^2 < b^2$. Thus, if $0 < a < b$ then $a^2 < b^2$. □

We were given as a hypothesis that a and b are real numbers with a conclusion of the form $P \to Q$, where P is the statement $0 < a < b$ and Q the statement $a^2 < b^2$. Thus we start with these statements as given and goal:

Givens	*Goal*
a and b are real numbers	$(0 < a < b) \to (a^2 < b^2)$

As per our strategy, we assume that $0 < a < b$ and try to use this assumption to prove $a^2 < b^2$. In other words we add $0 < a < b$ to the list of givenas and make $a^2 < b^2$ our goal:

Givens	*Goal*
a and b are real numbers	$a^2 < b^2$
$0 < a < b$	

(next page)

Generalising
Here's a restatement of the proof strategy we discussed, in the form we will be using to present proof strategies from now on.

To prove a goal of the form $P \to Q$:
Assume P is true and then prove Q.

Scratch work
Before using strategy:

Givens	*Goal*
—	$P \to Q$
—	

After using strategy:

Givens	*Goal*
—	Q
—	
P	

Form of final proof:
Suppose P.
[Proof of Q goes here.]
Therefore $P \to Q$.

(next page)

2.1.1 Alternative approach

Another approach could utilise the contrapositive law, where

$$P \to Q = \neg Q \to \neg P$$

In other words:

> To prove a goal of the form $P \to Q$:
> Assume Q is false and prove that P is false.

Scratch work
Before using strategy:

Givens	*Goal*
—	$P \to Q$
—	

After using strategy:

Givens	*Goal*
—	$\neg P$
—	
$\neg Q$	

Form of final proof:

> Suppose Q is false.
> > [Proof of $\neg P$ goes here.]
>
> Therefore $P \to Q$.

(next page)

Example
Suppose a, b and c are real numbers and $a > b$. Prove that if $ac \leq bc$ then $c \leq 0$.

Scratch work
Before using strategy:

Givens	*Goal*
a, b and c are real numbers $a > b$	$(ac \leq bc) \to (c \leq 0)$

The contrapositive of the goal is $\neg(c \leq 0) \to \neg(ac \leq bc)$, or $(c > 0) \to (ac > bc)$. As per the previous strategy, we can prove this by adding $c > 0$ to the list of givens and making $ac > bc$ our new goal:

Givens	*Goal*
a, b and c are real numbers $a > b$ $c > 0$	$ac > bc$

Form of final proof:
Suppose $c > 0$.
[Proof of $ac > bc$ goes here.]
Therefore, if $ac \leq bc$ then $c \leq 0$.

Solution

Theorem. *Suppose a, b and c are real numbers and $a > b$. If $ac \leq bc$ then $c \leq 0$.*

Proof. We will prove the contrapositive. Suppose $c > 0$. Then we can multiply both sides of the given inequality $a > b$ by c and conclude that $ac > bc$. Therefore if $ac \leq bc$ then $c \leq 0$. □

2.2 Proofs involving negations and conditionals

2.2.1 Reexpress

We now consider proofs in which the goal has the form $\neg P$. Usually it's easier to prove a positive statement than a negative statement, so it is often helpful to reexpress the goal before proving it. Thus our first strategy for proving negated statements is:

> To prove a goal of the form $\neg P$:
> If possible, reexpress the goal in some other form.

Example
Suppose $A \cap C \subseteq B$ and $a \in C$. Prove that $a \notin A \setminus B$.

Scratch Work

Givens	*Goal*
$A \cap C \subseteq B$	$a \notin A \setminus B$
$a \in C$	

We have a negative goal, which we can try to reexpress as a positive statement:

$$\begin{aligned} a \notin A \setminus B &= \neg(a \in A \wedge a \notin B) && \text{(Definition)} \\ &= a \in A \to a \in B && \text{(Conditional law)} \end{aligned}$$

This gives us

Givens	*Goal*
$A \cap C \subseteq B$	$a \in A \to a \in B$
$a \in C$	

We can apply the strategy for conditional goals:

Givens	*Goal*
$A \cap C \subseteq B$	$a \in B$
$a \in C$	
$a \in A$	

See how the proof is now much more straightforward; from the givens $a \in A$ and $a \in C$ we can conclude $a \in A \cap C$. Since $A \cap C \subseteq B$, it follows that $a \in B$.

Solution

Theorem. *Suppose $A \cap C \subseteq B$ and $a \in C$. Then $a \notin A \setminus B$.*

Proof. Suppose $a \in A$. Then since $a \in C$, $a \in A \cap C$. Since $A \cap C \subseteq B$ it follows that $a \in B$. Thus it cannot be the case that a is an element of A but not B, so $a \notin A \setminus B$. □

(next page)

2.2.2 Proof by contradiction

Say a goal of the form $\neg P$ cannot be reexpressed as a positive statement, in this case one could attempt *proof by contradiction*—start by assuming P is true, and try to use this assumption to prove that something one already knows is false.

Often this is done by proving a statement that contradicts one of the givens; because one knows that the statement proven is false, the assumption that P was true must have been incorrect—the only remaining possibility then is that P is false.

To prove a goal of the form $\neg P$:
Assume P is true and try to reach a contradiction. In which case P must be false.

Scratch Work

Givens	*Goal*
—	$\neg P$
—	

After using strategy:

Givens	*Goal*
—	Contradiction
—	
P	

Form of final proof:
Suppose P is true.
[Proof of contradiction goes here.]
Thus, P is false.

(next page)

Example
Prove that if $x^2 + y = 13$ and $y \neq 4$ then $x \neq 3$.

Scratch work
The goal is a conditional statement. We treat the antecedent as a given and make the consequent our new goal:

Givens	*Goal*
$x^2 + y = 13$	$x \neq 3$
$y \neq 4$	

Our current idea of the proof structure looks like

Suppose $x^2 + y^2 = 13$ and $y \neq 4$.
    [Proof of $x \neq 3$ goes here.]
Thus, if $x^2 + y^2 = 13$ and $y \neq 4$ then $x \neq 3$.

In this sense, each manipulation of our problem dictates the structure of our final proof. At this point the first and last sentences of the final proof have been produced. What remains is to prove $x \neq 3$ given our manipulated problem.

The goal $x \neq 3$ means $\neg(x = 3)$; we try proof by contradiction and transform the problem as follows:

Givens	*Goal*
$x^2 + y = 13$	Contradiction
$y \neq 4$	
$x = 3$	

Once again, the proof strategy that suggested this transformation also tells us how to fill in a few more sentences of the final proof:

Suppose $x^2 + y^2 = 13$ and $y \neq 4$.
    Suppose $x = 3$
        [Proof of contradiction goes here.]
    Therefore $x \neq 3$
Thus, if $x^2 + y^2 = 13$ and $y \neq 4$ then $x \neq 3$.

The first and last lines go together and indicate that we are proving a conditional statement by assuming the antecedent and proving the consequent. Between these lines is a proof of the consequent $x \neq 3$. This inner proof has the form of a proof by contradiction, as indicated by the second first and second last lines; between these lines we still need to fill in a proof of a contradiction.

At this point we don't have a particular statement as a goal; any impossible conclusion will do. We must look closely at the givens to find a contradiction.
(next page)

Example cont.
Solution

Theorem. *If* $x^2 + y = 13$ *and* $y \neq 4$ *then* $x \neq 3$.

Proof. Suppose $x^2 + y = 13$ and $y \neq 4$. Suppose $x = 3$. Substituting this into the equation $x^2 + y = 13$, we get $9 + y = 13$, so $y = 4$. But this contradicts the fact that $y \neq 4$. Therefore $x \neq 3$. Thus, if $x^2 + y = 13$ and $y \neq 4$ then $x \neq 3$. □

2.2.3 To use a given of the form $\neg P$ in proof by contradiction

If attempting a proof by contradiction with a given $\neg P$. Here is a useful strategy;

To use a given of the form $\neg P$:
Try making P the goal. If one can prove P, then the proof is complete, since P contradicts the given $\neg P$.

Scratch Work
Before using strategy:

Givens	*Goal*
$\neg P$	Contradiction
—	
—	

After using strategy:

Givens	*Goal*
$\neg P$	P
—	
—	

Form of final proof:
[Proof of P goes here.]
Since we already know $\neg P$, this is a contradiction.

Note that proof by contradiction is not restricted to goals of the form $\neg P$, and can be used for any goal.
(next page)

Example
Suppose A, B and C are sets, $A \setminus B \subseteq C$, and x is anything at all. Prove that if $x \in A \setminus C$ then $x \in B$.

Scratch work
We're given $A \setminus B \subseteq C$ and our goal is $x \in A \setminus C \to x \in B$. We use the previously discussed strategy for conditionals (assume antecedent and prove consequent):

Givens	*Goal*
$A \setminus B \subseteq C$	$x \in B$
$x \in A \setminus C$	

Our proof currently looks like
Suppose $x \in A \setminus C$.
[Proof of $x \in B$ goes here.]
Thus, if $x \in A \setminus C$ then $x \in B$.

We attempt proof by contradiction:

Givens	*Goal*
$A \setminus B \subseteq C$	Contradiction
$x \in A \setminus C$	
$x \notin B$	

Now our proof looks like
Suppose $x \in A \setminus C$.
Suppose $x \notin B$
[Proof of contradiction goes here.]
Therefore $x \in B$
Thus, if $x \in A \setminus C$ then $x \in B$.

Because we're doing a proof by contradiction and our last given is now a negated statement, we could try our strategy for using givens of the form $\neg P$. Unfortunately, this strategy suggests making $x \in B$ our goal which just gets us back to where we started. We must look at the other givens to try to find the contradiction.
(next page)

Example cont.
We have

Givens	*Goal*
$A \setminus B \subseteq C$	Contradiction
$x \in A \setminus C$	
$x \notin B$	

In this case writing out the definition of the second given is key to the proof. By definition $x \in A \setminus C$ means $x \in A$ and $x \notin C$. Replacing this given by its definition gives us

Givens	*Goal*
$A \setminus B \subseteq C$	Contradiction
$x \in A$	
$x \notin C$	
$x \notin B$	

Now the third given has the form $\neg P$. We can apply the strategy for using givens of the form $\neg P$ and make $x \in C$ our goal, where showing it would complete the proof by contradicting the given $x \notin C$:

Givens	*Goal*
$A \setminus B \subseteq C$	$x \in C$
$x \in A$	
$x \notin C$	
$x \notin B$	

Once again, we can add a little more to the proof we are gradually forming with each step. We add in the fact that we plan to derive our contradiction by proving $x \in C$; we also add the definition of $x \in A \setminus C$ to the proof.

Suppose $x \in A \setminus C$. This means $x \in A$ and $x \notin C$.
  Suppose $x \notin B$
    [Proof of $x \in C$ goes here.]
    This contradicts the fact that $x \notin C$.
  Therefore $x \in B$
Thus, if $x \in A \setminus C$ then $x \in B$.

We have finally reached a point where the goal follows apparently from the givens—from $x \in A$ and $x \notin B$ we conclude that $x \in A \setminus B$. Since $A \setminus B \subseteq C$ it follows that $x \in C$.
(next page)

Example cont.
Solution

Theorem. *Suppose A, B and C are sets, $A \setminus B \subseteq C$, and x is anything at all. If $x \in A \setminus C$ then $x \in B$.*

Proof. Suppose $x \in A \setminus C$. This means that $x \in A$ and $x \notin C$. Suppose $x \notin B$. Then $x \in A \setminus B$, so since $A \setminus B \subseteq C$, $x \in C$. But this contradicts the fact that $x \notin C$. Therefore $x \in B$. Thus, if $x \in A \setminus C$ then $x \in B$. □

2.2.4 Given conditionals

We consider strategies for using givens of the form $P \to Q$:

To use a given of the form $P \to Q$:
If also given P, or if one can prove P, then one can use this to conclude Q. Another approach would be to use its equivalence to $\neg Q \to \neg P$; if one can prove that Q is false, then one can conclude that P is false.

The first rule says that if you know both P and $P \to Q$ are true, then Q must also be true; this rule is called *modus ponens*. The second rule, called *modus tollens*, says that if you know $P \to Q$ is true and Q is false, then you can conclude that P must also be false.

Example
Suppose $P \to (Q \to R)$. Prove that $\neg R \to (P \to \neg Q)$.

Scratch work
We start with the following situation:

Givens	*Goal*
$P \to (Q \to R)$	$\neg R \to (P \to \neg Q)$

If either P or $\neg(Q \to R)$ gets added to the givens list, then we should consider using modus ponens or modus tollens. For now we concentrate on the goal; being a conditional statement, we assume the antecedent and set the consequent as the new goal:

Givens	*Goal*
$P \to (Q \to R)$	$P \to \neg Q$
$\neg R$	

Our proof currently looks like:

Suppose $\neg R$.
[Proof of $P \to \neg Q$ goes here.]
Therefore $\neg R \to (P \to \neg Q)$.
(next page)

Example cont.
We had

Givens	*Goal*
$P \to (Q \to R)$	$P \to \neg Q$
$\neg R$	

The goal is still a conditional. We use the same strategy again:

Givens	*Goal*
$P \to (Q \to R)$	$\neg Q$
$\neg R$	
P	

Now the proof looks like

Suppose $\neg R$.
    Suppose P.
        [Proof for $\neg Q$ goes here.]
    Therefore $P \to \neg Q$.
Therefore $\neg R \to (P \to \neg Q)$.

Since we know $P \to (Q \to R)$ and P, by modus ponens we can infer $Q \to R$:

Givens	*Goal*
$P \to (Q \to R)$	$\neg Q$
$\neg R$	
P	
$Q \to R$	

We add one more line to our proof:

Suppose $\neg R$.
    Suppose P.
        Since P and $P \to (Q \to R)$, it follows that $Q \to R$.
        [Proof of $\neg Q$ goes here.]
    Therefore $P \to \neg Q$.
Therefore $\neg R \to (P \to \neg Q)$.

Finally, our last step is to use modus tollens. We now know $Q \to R$ and $\neg R$, so by modus tollens we can conclude $\neg Q$.
(next page)

Example cont.
Solution

Theorem. *Suppose* $P \to (Q \to R)$. *Then* $\neg R \to (P \to \neg Q)$.

Proof. Suppose $\neg R$. Suppose P. Since P and $P \to (Q \to R)$, it follows that $Q \to R$. But then since $\neg R$, we can conclude $\neg Q$. Thus $P \to \neg Q$. Therefore $\neg R \to (P \to \neg Q)$. □

2.3 Proofs involving quantifiers

2.3.1 Goals of form $\forall x P(x)$

If you can give a proof of the goal $P(x)$ that would work for all x, then you can conclude that $\forall x P(x)$ must be true. Thus it is important to start the proof with no assumptions about x, that is, x must be *arbitrary*; one must not assume that x is already equal to any other object already under discussion in the proof.

If x is already being used in the proof to stand for some particular object, then one cannot use it to stand for an arbitrary object, and must choose a different variable that is not already being used in the proof, say y, and replace $\forall x P(x)$ with the equivalent statement $\forall y P(y)$.

To prove a goal of the form