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 $a \notin A \setminus B$. □

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 $\forall P(x)$:

Let x stand for an arbitrary object and prove $P(x)$. The letter x must be a new variable in the proof. If x is already being used to stand for something, then choose an unused variable, say y, to stand for the arbitrary object, and prove $P(y)$.

Scratch work
Before using strategy:

Givens	*Goal*
—	$\forall x P(x)$
—	

After using strategy:

Givens	*Goal*
—	$P(x)$
—	

Form of final proof:

Let x be arbitrary.

[Proof of $P(x)$ goes here.]

Since x was arbitrary, we can conclude that $\forall x P(x)$.

(next page)

Example
Consider a proof covered earlier, but phrased slightly differently: Suppose A, B, and C are sets, and $A \setminus B \subseteq C$. Prove that $A \setminus C \subseteq B$.

Scratch work
Before using strategy:

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

As usual we consider the logical form of the goal to plan our strategy. In this case we can write out the definition of $\subseteq$:

Givens	*Goal*
$A \setminus B \subseteq C$	$\forall x(x \in A \setminus C \to x \in B)$

Because the goal has the form $\forall x P(x)$, where $P(x)$ is the statement $x \in A \setminus C \to x \in B$, we will introduce a new variable x into the proof to stand for an arbitrary object and then try to prove $x \in A \setminus C \to x \in B$.

Note that x is a new variable in the proof; it appeared in the logical form of the goal as a bound variable, but, being a bound variable, didn't represent anything in particular. We also haven't used it as a free variable in any statement so it doesn't stand for any particular object. To make sure x is arbitrary we must be careful not to add any assumptions about x to the givens column. Our goal becomes

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

Our proof looks like

> Let x be arbitrary.
> [Proof of $x \in A \setminus C \to x \in B$ goes here]
> Since x was arbitrary, we can conclude that $\forall x(x \in A \setminus C \to x \in B)$, so $A \setminus C \subseteq B$.

The problem is now exactly the same as it was in the previous example.

Solution

Theorem. *Suppose A, B, and C are sets, and $A \setminus B \subseteq C$. Then $A \setminus C \subseteq B$.*

Proof. Let x be arbitrary. 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 $x \in B$. Since x was arbitrary we can conclude that $\forall x(x \in A \setminus C \to x \in B)$, so $A \setminus C \subseteq B$. □

(next page)

Another example
Suppose A and B are sets. Prove that if $A \cap B = A$ then $A \subseteq B$.

Scratch work

Our goal is $A \cap B = A \to A \subseteq B$. We add the antecedent to the givens list and make the consequent the goal. We write out the logical form of this new goal:

Givens	*Goal*
$A \cap B = A$	$\forall x(x \in A \to x \in B)$

We let x be arbitrary, assume $x \in A$, and probe $x \in B$:

Givens	*Goal*
$A \cap B = A$	$x \in B$
$x \in A$	

Our final proof form looks like

Suppose $A \cap B = A$.
    Let x be arbitrary.
        Suppose $x \in A$.
            [Proof of $x \in B$ goes here.]
        Therefore $x \in A \to x \in B$.
    Since x was arbitrary, we can conclude that $\forall x(x \in A \to x \in B)$,
    so $A \subseteq B$.
Therefore, if $A \cap B = A$ then $A \subseteq B$.

Since $x \in A$ and $A \cap B = A$, it follows that $x \in A \cap B$, so $x \in B$. (recall $x \in A \cap B$ means $x \in A$ and $x \in B$)

Oftentimes the statement that x is arbitrary is left out—when a new variable x is introduced into a proof it is usually understood that it is arbitrary and no assumptions are being made about x. Many of the proofs written so far end with multiple concluding sentences; oftentimes these are condensed into a single sentence, or skipped entirely.

Solution

Theorem. *Suppose A and B are sets. If $A \cap B = A$ then $A \subseteq B$.*

Proof. Suppose $A \cap B = A$, and suppose $x \in A$. Then since $A \cap B = A$, $x \in A \cap B$, so $x \in B$. Since x was an arbitrary element of A, we can conclude that $A \subseteq B$. □

2.3.2 Goals of form $\exists x P(x)$

Proving a goal of the form $\exists x P(x)$ also involves introducing a new variable x into the proof and proving $P(x)$. But in this case x will not be arbitrary; we only need to prove that $P(x)$ is true for *at least one* x. It suffices to assign a particular value to x and prove $P(x)$ for this one value of x.

To prove a goal of the form $\exists x P(x)$:

Try to find a value of x for which $P(x)$ would be true. Start with 'Let $x =$ (decided value)' and proceed to prove $P(x)$ for this x. Once again if the variable name x is already being used in the proof for some other purpose then one should choose an unused variable, say y and rewrite the goal in the equivalent form $\exists y P(y)$ and proceed as before.

Scratch work
Before using strategy:

Givens	*Goal*
—	$\exists x P(x)$
—	

After using strategy:

Givens	*Goal*
—	$P(x)$
—	
$x =$ (the value you decided on)	

Form of final proof:

Let $x =$ (the value you decided on).
[Proof of $P(x)$ goes here.]
Thus, $\exists x P(x)$.

Note that *the reasoning used for finding a specific x will not appear in the final proof.* To justify the conclusion that $\exists x P(x)$ it is only necessary to verify that $P(x)$ comes out true when x is assigned some particular value. How one thought of that value is not part of the justification of the conclusion (be it by trial and error etc.).
(next page)

Example
Prove that for every real number x, if $x > 0$ then there is a real number y such that $y(y + 1) = x$.

Scratch work
Logically, our goal is $\forall x(x > 0 \to \exists y[y(y + 1) = x])$, where the variables x and y in this statement are understood to range over $\mathbb{R}$. We start by letting x be an arbitrary real number, and then assume that $x > 0$ and try to prove that $\exists y[y(y + 1) = x]$:

Givens	*Goal*
$x > 0$	$\exists y[y(y + 1) = x]$

Because our goal has the form $\exists y P(y)$, where $P(y)$ is the statement $y(y+1) = x$, according to our strategy we should try to find a value of y for which $P(y)$ is true. In this case we do this by solving the equation $y(y + 1) = x$ for y.

$$y(y + 1) = x \iff y^2 + y - x = 0 \iff y = \frac{-1^2 \pm \sqrt{1 + 4x}}{2}$$

Note that $\sqrt{1 + 4x}$ is defined since we have $x > 0$ as a given. Also see that we have found two solutions for y, but to prove that $\exists y[y(y + 1) = x]$ we only need one valid y, so either of the the two solutions could be used.

Givens	*Goal*
$x > 0$	$y(y + 1) = x$
$y = (-1 + \sqrt{1 + 4x})/2$	

Our final proof looks like

Let x be an arbitrary real number.
  Suppose $x > 0$.
    Let $y = (-1 + \sqrt{1 + 4x})/2$.
      [Proof of $y(y + 1) = x$ goes here.]
    Thus, $\exists y[y(y + 1) = x]$.
  Therefore $x > 0 \to \exists y[y(y + 1) = x]$.
Since x was arbitrary, we can conclude that $\forall x(x > 0 \to \exists y[y(y + 1) = x])$.

(next page)

Example cont.
Solution

Theorem. *For every real number x, if $x > 0$ then there is a real number y such that $y(y+1) = x$.*

Proof. Let x be an arbitrary real number and suppose $x > 0$. Let

$$y = \frac{-1 + \sqrt{1+4x}}{2}$$

which is defined since $x > 0$. Then

$$\begin{aligned} y(y+1) &= \left(\frac{-1+\sqrt{1+4x}}{2}\right) \cdot \left(\frac{-1+\sqrt{1+4x}}{2} + 1\right) \\ &= \left(\frac{\sqrt{1+4x}-1}{2}\right) \cdot \left(\frac{\sqrt{1+4x}+1}{2}\right) \\ &= \frac{1+4x-1}{4} = \frac{4x}{4} = x \end{aligned}$$

□

2.3.3 Givens of the form $\exists x P(x)$ and $\forall x P(x)$

Givens of the form $\exists x P(x)$
This given says that an object with a certain property exists. A good approach would be to introduce a new variable, say x_0, to stand for this object, and add $P(x_0)$ to the givens list.

To use a given of the form $\exists x P(x)$:
Introduce a new variable x_0 into the proof to stand for an object for which $P(x_0)$ is true. This means that one can now assume that $P(x_0)$ is true.

Logicians call this *existential instantiation*. Note that this is very different from our treatment of goals of the same form—we can assume that x_0 stands for some object for which $P(x_0)$ is true, but we can't assume anything else about x_0.

Givens of the form $\forall x P(x)$
This says that $P(x)$ would be true no matter what value is assigned ot x. One can therefore *choose any value* to be plugged in for x and use this to conclude $P(x)$.

To use a given of the form $\forall x P(x)$
Plug in any value, say a, for x and use this given to conclude that $P(a)$ is true.

This is called *universal instantiation*. Usually, if we have a given of the form $\exists x P(x)$, we should apply existential instantiation to it immediately. On the other hand, we won't be able to apply universal instantiation to a given of the form $\forall x P(x)$ unless we had an idea for a particular value a to plug in for x; we would probably wait until a suitable object a appears in the proof.
(next page)

Example
Suppose $\mathcal{F}$ and $\mathcal{G}$ are families of sets and $\mathcal{F} \cap \mathcal{G} \neq \emptyset$. Prove that $\bigcap \mathcal{F} \subseteq \bigcup \mathcal{G}$.

Scratch work
First we analyse the logical form of the goal by writing out the meaning of the subset: $\forall x(x \in \bigcap \mathcal{F} \to x \in \bigcup \mathcal{G})$. We could go further with the logical forms of the union and intersection, but the analysis done so far is sufficient for us to decide how to get started on the proof; their definitions might be required later, but it is usually best to do only as much of the analysis as is needed to determine the next step of the proof. Going further might introduce unnecessary complication.

We let x be arbitrary, assume $x \in \bigcap \mathcal{F}$, and try to prove $x \in \bigcup \mathcal{G}$.

Givens	*Goal*
$\mathcal{F} \cap \mathcal{G} \neq \emptyset$	$x \in \bigcup \mathcal{G}$
$x \in \bigcap \mathcal{F}$	

Now we further analyse the logical forms:

Givens	*Goal*
$\exists A(A \in \mathcal{F} \cap \mathcal{G})$	$\exists A \in \mathcal{G}(x \in A)$
$\forall A \in \mathcal{F}(x \in A)$	

To prove this new goal means we should try to find a value that would 'work' for A. The second given starts with $\forall A$, so we may not be able to use it until a likely value for A pops up during the course of the proof. The first given, however, starts with $\exists A$, so we should use it immediately; by existential instantiation, we introduce a name, say A_0, for this object, and treat $A_0 \in \mathcal{F} \cap \mathcal{G}$ as a given from now on. It would be redundant to continue to discuss the given statement $\exists A(A \in \mathcal{F} \cap \mathcal{G})$ so we will drop it from our list of givens.

Givens	*Goal*
$A_0 \in \mathcal{F}$	$\exists A \in \mathcal{G}(x \in A)$
$A_0 \in \mathcal{G}$	
$\forall A \in \mathcal{F}(x \in A)$	

An element to plug into the third given has now surfaced, plugging A_0 for A we can conclude that $x \in A_0$; we can treat this as a given. See that the goal can now be easily reached.

Although we translated the statements $x \in \bigcap \mathcal{F}, x \in \bigcup \mathcal{G}$, and $\mathcal{F} \cap \mathcal{G} \neq \emptyset$ into logical symbols in order to figure out how to use them in the proof; these translations are not usually written out it in the final proof—left to the reader to work out their logical forms in order to follow the reasoning.
(next page)

Example cont.
Solution

Theorem. *Suppose $\mathcal{F}$ and $\mathcal{G}$ are families of sets, and $\mathcal{F} \cap \mathcal{G} \neq \emptyset$. Then $\bigcap \mathcal{F} \subseteq \bigcup \mathcal{G}$.*

Proof. Suppose $x \in \bigcap \mathcal{F}$. Since $\mathcal{F} \cap \mathcal{G} = \emptyset$, we can let A_0 be an element of $\mathcal{F} \cap \mathcal{G}$. Thus, $A_0 \in \mathcal{F}$ and $A_0 \in \mathcal{G}$. Since $x \in \bigcap \mathcal{F}$ and $A_0 \in \mathcal{F}$, it follows that $x \in A_0$. But we also know that $A_0 \in \mathcal{G}$, so we can conclude that $x \in \bigcup \mathcal{G}$. $\square$

Another example
Suppose B is a set and $\mathcal{F}$ is a family of sets. Prove that if $\bigcup \mathcal{F} \subseteq B$ then $\mathcal{F} \subseteq \mathscr{P}(B)$

Scratch work
We assume $\bigcup \mathcal{F} \subseteq B$ and try to prove $\mathcal{F} \subseteq \mathscr{P}(B)$, which means $\forall x(x \in \mathcal{F} \rightarrow x \in \mathscr{P}(B))$, we let x be arbitrary, assume $x \in \mathcal{F}$, and set $x \in \mathscr{P}(B)$ as our goal. Note that x in this case is a set:

Givens	*Goal*
$\bigcup \mathcal{F} \subseteq B$	$x \in \mathscr{P}(B)$
$x \in \mathcal{F}$	

To further analyse this goal, we use the definition of the power statement $x \in \mathscr{P}(B) = x \subseteq B$; which further means $\forall y(y \in x \rightarrow y \in B)$. We must therefore introduce another arbitrary object into the proof; we let y be arbitrary, assume $y \in x$, and try to prove $y \in B$.

Givens	*Goal*
$\bigcup \mathcal{F} \subseteq B$	$y \in B$
$x \in \mathcal{F}$	
$y \in x$	

The first given can be written as $\forall z(z \in \bigcup \mathcal{F} \rightarrow z \in B)$, which further means $\forall z(\exists A \in \mathcal{F}(z \in A) \rightarrow z \in B)$

Givens	*Goal*
$\forall z(\exists A \in \mathcal{F}(z \in A) \rightarrow z \in B)$	$y \in B$
$x \in \mathcal{F}$	
$y \in x$	

The conclusion is now easily reachable.
(next page)

Example cont.
Solution

Theorem. *Suppose B is a set and $\mathcal{F}$ is a family of sets. If $\bigcup \mathcal{F} \subseteq B$ then $\mathcal{F} \subseteq \mathscr{P}(B)$.*

Proof. Suppose $\bigcup \mathcal{F} \subseteq B$. Let x be an arbitrary element of $\mathcal{F}$. Let y be an arbitrary element of x. Since $y \in x$ and $x \in \mathcal{F}$, $y \in \bigcup \mathcal{F}$. But since $\bigcup \mathcal{F} \subseteq B$, $y \in B$. Since y was an arbitrary element of x, we can conclude that $x \subseteq B$, so $x \in \mathscr{P}(B)$. But x was an arbitrary element of $\mathcal{F}$, so $\mathcal{F} \subseteq \mathscr{P}(B)$, as required. □

2.3.4 Example: For all integers a, b, c, if $a \mid b$ and $b \mid c$ then $a \mid c$

For this proof, we need the following definition:

Definition. For any integers x and y, we'll say that x *divides* y (or y *is divisible by* x) if $\exists k \in \mathbb{Z}(kx = y)$. We use the notation $x \mid y$ to mean 'x divides y' and $x \nmid y$ to mean 'x does not divide y'.

Theorem. *For all integers $a, b,$ and c, if $a \mid b$ and $b \mid c$ then $a \mid c$.*

Proof. Let a, b, and c be arbitrary integers and suppose $a \mid b$ and $b \mid c$. Since $a \mid b$, we can choose some integer m such that $ma = b$. Similarly, since $b \mid c$, we can choose an integer n such that $nb = c$. Therefore $c = nb = nma$, so since nm is an integer, $a \mid c$. □

2.4 Proofs involving conjunctions and biconditionals

2.4.1 Goals and givens of form $P \wedge Q$

This is fairly straightforward:

> To prove a goal of the form $P \wedge Q$:
> Prove P and Q separately.

In other words, a goal of the form $P \wedge Q$ is treated as two separate goals: P and Q. The same is true of givens of the form $P \wedge Q$:

> To use a given of the form $P \wedge Q$:
> Treat this given as two separate givens: P and Q.

We've already used these ideas in previous examples.

Example
Suppose $A \subseteq B$, and A and C are disjoint. Prove that $A \subseteq B \setminus C$.

Scratch work

Givens	*Goal*
$A \subseteq B$	$A \subseteq B \setminus C$
$A \cap C = \emptyset$	

The logical form of the goal has the form $\forall x(x \in A \to x \in B \setminus C)$, so we let x be arbitrary, assume $x \in A$, and try to prove $x \in B \setminus C$, which means $x \in B \wedge x \notin C$. As per our strategy we split this into two goals and prove them separately.

Givens	*Goal*
$A \subseteq B$	$x \in B$
$A \cap C = \emptyset$	$x \notin C$
$x \in A$	

The final proof will have the form

> Let x be arbitrary.
> > Suppose $x \in A$.
> > > [Proof of $x \in B$ goes here.]
> > > [Proof of $x \in B$ goes here.]
> > > Thus, $x \in B \wedge x \notin C$, so $x \in B \setminus C$.
> > Therefore $x \in A \to x \in B \setminus C$.
> Since x was arbitrary, $\forall x(x \in A \to x \in B \setminus C)$, so $A \subseteq B \setminus C$.

(next page)

Example cont.
The first goal, $x \in B$, follows from $x \in A$ and $A \subseteq B$; that much is clear. The second goal, $x \notin C$, follows from $x \in A$ and $A \cap C = \emptyset$; this can be seen from analysing the logical form of $A \cap C = \emptyset$:

$$\begin{aligned} A \cap C = \emptyset \text{ is equivalent to } & \neg\exists y(y \in A \wedge y \in C) && \text{(definition)} \\ =& \forall y \neg(y \in A \wedge y \in C) && \text{(Quantifier negation)} \\ =& \forall y(y \in A \rightarrow y \notin C) && \text{(definition)} \end{aligned}$$

From which we can conclude that $x \in A \rightarrow x \notin C$.

Solution

Theorem. *Suppose $A \subseteq B$, and A and C are disjoint. Then $A \subseteq B \setminus C$.*

Proof. Suppose $x \in A$. Since $A \subseteq B$, it follows that $x \in B$, and since A and C are disjoint, we must have $x \notin C$. Thus, $x \in B \setminus C$. Since x was an arbitrary element of A, we can conclude that $A \subseteq B \setminus C$. □

2.4.2 Goals and givens of the form $P \leftrightarrow Q$ (part 1)

$P \leftrightarrow Q$ is equivalent to $(P \to Q) \wedge (Q \to P)$; as per the previous strategy, this sshould be treated as two separate givens or goals: $P \to Q$ and $Q \to P$.

To prove a goal of the for $P \leftrightarrow Q$:
Prove $P \to Q$ and $Q \to P$ separately.

To use a given of the form $P \leftrightarrow Q$:
Treat this as two separate givens $P \to Q$ and $Q \to P$.

2.4.3 Example: Suppose x is an integer. Prove that x is even iff x^2 is even

We use the definition

Definition. An integer x is *even* if $\exists k \in \mathbb{Z}(x = 2k)$, and x is *odd* if $\exists k \in \mathbb{Z}(x = 2k + 1)$.

We also use the fact that every integer is either even or odd, but not both.

Example
Suppose x is an integer. Prove that x is even iff x^2 is even.

Scratch work
The goal is (x is even)$\leftrightarrow$(x^2 is even), so we prove the two goals (x is even)$\to$(x^2 is even) and (x^2 is even)$\to$(x is even) separately. So first:

Givens	*Goal*
$x \in \mathbb{Z}$	x^2 is even
x is even	

We reveal the logical forms by writing out the definition of *even*:

Givens	*Goal*
$x \in \mathbb{Z}$	$\exists j \in \mathbb{Z}(x^2 = 2j)$
$\exists k \in \mathbb{Z}(x = 2k)$	

The second given starts with $\exists k$, we immediately introduce k_0 to stand for some integer for which the enclosed statement is true: $k_0 \in \mathbb{Z}$, and $x = 2k_0$.

Givens	*Goal*
$x \in \mathbb{Z}$	$\exists j \in \mathbb{Z}(x^2 = 2j)$
$\exists k \in \mathbb{Z}(x = 2k)$	
$k_0 \in \mathbb{Z}$	
$x = 2k_0$	

We need an integer j such that $x^2 = 2j$. Plugging in $2k_0$ for x we get $x^2 = 4k_0^2 = 2(2k_0^2)$ See that $j = 2k_0^2$ is a possible choice.
(next page)

Example cont.
To prove the second goal (x^2 is even)$\rightarrow$(x is even), we'll prove the contrapositive (x is not even)$\rightarrow$(x is not even) instead. Since any integer is either even or odd but not both, this is equivalent to (x is odd)$\rightarrow$(x^2 is odd):

Givens	*Goal*
$x \in \mathbb{Z}$	x^2 is odd
x is odd	

Again we write out the definition of *odd* to reveal the logical forms:

Givens	*Goal*
$x \in \mathbb{Z}$	$\exists j \in \mathbb{Z}(x^2 = 2j + 1)$
$\exists k \in \mathbb{Z}(x = 2k + 1)$	

Considering the second given, we use existential instantiation:

Givens	*Goal*
$x \in \mathbb{Z}$	$\exists j \in \mathbb{Z}(x^2 = 2j + 1)$
$\exists k \in \mathbb{Z}(x = 2k + 1)$	
$k \in \mathbb{Z}$	
$x = 2k_0 + 1$	

We must now find an integer j such that $x^2 = 2j + 1$. Plugging in $2k_0 + 1$ for x we get $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, so $j = 2k^2 + 2k$ is a possible choice.

The two conditional statements we've proven can be thought of as representing the two directions $\rightarrow$ and $\leftarrow$. The two parts of the proof are sometimes labelled with the symbols $\rightarrow$ and $\leftarrow$.

In each part, we prove a statement that asserts the existence of a number with certain properties. We called this number j, but note that j was not mentioned explicily in the statement of the problem, so we choose not to mention it in the final proof.

Solution

Theorem. *Suppose x is an integer. Then x is even iff x^2 is even.*

Proof. ($\rightarrow$) Suppose x is even. Then for some integer k_0, $x = 2k_0$. Therefore $x^2 = 4k^2 = 2(2k^2)$, so since $2k^2$ is an integer, x^2 is even. Thus if x is even then x^2 is even.

($\leftarrow$) Suppose x is odd. Then $x = 2k + 1$ for some integer k. Therefore $x^2 = (2k+1)^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$, so since $(2k^2+2k)$ is an integer, x^2 is odd. Thus if x^2 is even then x is even. $\square$

2.4.4 Proving $\forall x \neg P(x) \leftrightarrow \neg \exists x P(x)$

Scratch work

($\rightarrow$) We first prove $\forall x \neg P(x) \rightarrow \neg \exists x P(x)$, so we assume $\forall x \neg P(x)$ and try to prove $\neg \exists x P(x)$. Our goal is a negated statement, and trying to rexpress it would require the use of the very equivalence we are trying to prove. We therefore try proof by contradiction:

Givens	*Goal*
$\forall x \neg P(x)$	Contradiction
$\exists x P(x)$	

The second given starts with and existential quantifier, so we use it immediately and let x_0 stand for some object for which the statement $P(x_0)$ is true. But now plugging x_0 into the first given we get $\neg P(x_0)$, which gives us the contradiction we need.

($\leftarrow$) For the other direction we assume $\neg \exists x P(x)$ and try to prove $\forall x \neg P(x)$. We let x be arbitrary and try to prove $\neg P(x)$; once again we have a negated goal that can't be reexpressed, so we use proof by contradiction:

Givens	*Goal*
$\neg \exists x P(x)$	Contradiction
$P(x)$	

The first line is a negated statement. This suggests that we could get our contradiction by proving $\exists x P(x)$. We therefore set this as our goal

Givens	*Goal*
$\neg \exists x P(x)$	$\exists x P(x)$
$P(x)$	

Our second given $P(x)$ tells us that our arbitrary x is the value we need to show the goal.

Solution

Theorem. $\forall x \neg P(x) \leftrightarrow \neg \exists x P(x)$.

Proof. ($\rightarrow$) Suppose $\forall x \neg P(x)$, and suppose $\exists x P(x)$. Then we can choose some x_0 such that $P(x_0)$ is true. But since $\forall x \neg P(x)$, we can conclude that $\neg P(x_0)$, which is a contradiction. Therefore $\forall x \neg P(x) \rightarrow \neg \exists x P(x)$.

($\leftarrow$) Suppose $\neg \exists x P(x)$. Let x be arbitrary, and suppose $P(x)$. Since we have a specific x for which $P(x)$ is true, it follows that $\exists x P(x)$, which is a contradiction; therefore $\neg P(x)$. Since x was arbitrary, we can conclude that $\forall x \neg P(x)$, so $\neg \exists x P(x) \rightarrow \forall x \neg P(x)$. $\square$

2.4.5 Goals and givens of the form $P \leftrightarrow Q$ (part 2)

Sometimes in a proof of a goal of the form $P \leftrightarrow Q$ the steps in the proof of $Q \to P$ are the same as the steps used to prove $P \to Q$, just in reverse order. In this case one might be able to simplify the proof by writing it as a string of equivalences, starting with P and ending with Q.

For example suppose one could prove $P \to R \to Q$ (which is $P \to R$ and $R \to Q$), and $Q \to R \to P$ (which is $Q \to R$ and $R \to P$). This would be the same as asserting that $P \leftrightarrow R \leftrightarrow Q$ ($P \leftrightarrow R$ and $R \leftrightarrow Q$); as such both statements imply the goal $P \leftrightarrow Q$. One would present this kind of proof by simply writing the string of equivalences

$$P \text{ iff } R \text{ iff } Q$$

Since this is just an abbreviation for 'P iff R and R iff Q (and therefore P iff Q)'.

Example
Suppose A, B, and C are sets. Prove that $A \cap (B \setminus C) = (A \cap B) \setminus C$.

Scratch work
The equation $A \cap (B \setminus C) = (A \cap B) \setminus C$ means $\forall x(x \in A \cap (B \setminus C) \leftrightarrow x \in (A \cap B) \setminus C)$; it can also mean $[A \cap (B \setminus C) \subseteq (A \cap B) \setminus C] \wedge [(A \cap B) \setminus C \subseteq A \cap (B \setminus C)]$.

This suggests two approaches to the proof: we could let x be arbitrary and then prove $x \in A \cap (B \setminus C) \leftrightarrow x \in (A \cap B) \setminus C)$, or we could prove the two statements $A \cap (B \setminus C) \subseteq (A \cap B) \setminus C$ and $(A \cap B) \setminus C \subseteq A \cap (B \setminus C)$.

In this case we use the first approach. Considering the first half ($\to$) of the equivalence, we assume $x \in A \cap (B \setminus C)$ and try to prove $x \in (A \cap B) \setminus C$:

Givens	*Goal*
$x \in A \cap (B \setminus C)$	$x \in (A \cap B) \setminus C$

To see the logical forms of the given and goal, we write out their definitions as follows:

$$x \in A \cap (B \setminus C) \text{ iff } x \in A \wedge x \in B \setminus C \text{ iff } x \in A \wedge x \in B \wedge x \notin C$$
$$x \in (A \cap B) \setminus C \text{ iff } x \in A \cap B \wedge x \notin C \text{ iff } x \in A \wedge x \in B \wedge x \notin C$$

At this point it is clear that the reasoning involved in the ($\leftarrow$) direction of the proof will be exactly the same, but with the given and goal columns reversed. As such we might try to shorten the proof by writing it as a string of equivalences. (next page)

Example cont.
Solution

Theorem. *Suppose A, B, and C are sets. Then $A \cap (B \setminus C) = (A \cap B) \setminus C$.*

Proof. Let x be arbitrary. Then

$$\begin{aligned} x \in A \cap (B \setminus C) &\text{ iff } x \in A \wedge x \in B \setminus C \\ &\text{iff } x \in A \wedge x \in B \wedge x \notin C \\ &\text{iff } x \in A \cap B \wedge x \notin C \\ &\text{iff } x \in (A \cap B) \setminus C \end{aligned}$$

Thus, $\forall x(x \in A \cap (B \setminus C) \leftrightarrow x \in (A \cap B) \setminus C)$, so $A \cap (B \setminus C) = (A \cap B) \setminus C$. □

Another example
A similar technique can be used when proving equations. Consider proving that for any real numbers a and b,

$$(a+b)^2 - 4(a-b)^2 = (3b-a)(3a-b)$$

Scratch work
The goal has the form $\forall a \forall b[(a+b)^2 - 4(a-b)^2 = (3b-a)(3a-b)]$; so we start by letting a and b be arbitrary real numbers and try to prove the equation. Multiplying our both sides gives us:

$$\begin{aligned} (a+b)^2 - 4(a-b)^2 &= a^2 + 2ab + b^2 - 4(a^2 - 2ab + b^2) \\ &= -3a^2 + 10ab - 3b^2; \\ (3b-a)(3a-b) &= 9ab - 3a^2 - 3b^2 + ab = -3a^2 + 10ab - 3b^2 \end{aligned}$$

Clearly both sides are equal. The simplest way to write the proof is using a string of equalities.

Solution

Theorem. *For any real numbers a and b.*

$$(a+b)^2 - 4(a-b)^2 = (3b-a)(3a-b)$$

Proof. Let a and b be arbitrary real numbers. Then

$$\begin{aligned} (a+b)^2 - 4(a-b)^2 &= a^2 + 2ab + b^2 - 4(a^2 - 2ab + b^2) \\ &= -3a^2 + 10ab - 3b^2 \\ &= ab - 3a^2 - 3b^2 + ab = (3b-a)(3a-b) \end{aligned}$$

□

2.4.6 Example: For every integer n, $6 \mid n$ iff $2 \mid n$ and $3 \mid n$

Theorem. *For every integer n, $6 \mid n$ iff $2 \mid n$ and $3 \mid n$.*

Proof. ($\rightarrow$) Suppose $6 \mid n$. Then we can choose an integer k such that $6k = n$. Therefore $n = 6k = 2(3k)$, so $2 \mid n$, and similarly $n = 6k = 3(2k)$, so $3 \mid n$.

($\leftarrow$) Suppose $2 \mid n$ and $3 \mid n$. Then we can choose integers j and k such that $n = 2j$ and $n = 3k$. Therefore $6(j-k) = 6j - 6k = 3(2j) - 2(3k) = 3n - 2n = n$, so $6 \mid n$. □

2.5 Proofs involving disjunctions

Suppose one of the givens in the proof has the form $P \vee Q$. One way to do the proof would be to consider these two possibilities in turn—first assume that P is true and use this assumption to prove the goal, then assume Q is true and give another proof of the goal.

Although we don't know which of these assumptions is correct, the given $P \vee Q$ means that *one* of then must be correct, and that whichever one it is, we would have then shown that it implies the goal.

The two possibilities considered separately in this type of proof—the possibility that P is true and the possibility that Q is true—are called *cases*. The given $P \vee Q$ justifies the use of these two cases by guaranteeing that these cases cover all of the possibilities; we say in this situation that the cases are *exhaustive*. Any proof can be broken into two or more cases at an time, as long as the cases are exhaustive.

To use a given of the form $P \vee Q$:

Break the proof into cases. For case 1, assume P is true and use this assumption to prove the goal. For case 2, assume Q is true and give another proof of the goal.

Scratch work
Before using strategy:

Givens	*Goal*
$P \vee Q$	—
—	

After using strategy:

Case 1:

Givens	*Goal*
P	—
—	

Case 2:

Givens	*Goal*
Q	—
—	

Form of final proof:

Case 1. P is true.
[Proof of goal goes here.]
Case 2. Q is true.
[Proof of goal goes here.]
Since we know $P \vee Q$, these cases cover all the possibilities. Therefore the goal must be true.

(next page)

Example
Suppose that A, B, and C are sets. Prove that if $A \subseteq C$ and $B \subseteq C$ then $A \cup B \subseteq C$.

Scratch work
We assume that $A \subseteq C$ and $B \subseteq C$ and prove $A \cup B \subseteq C$. Writing out the goal using logical symbols gives us the following givens and goal:

Givens	*Goal*
$A \subseteq C$	$\forall x(x \in A \cup B \to x \in C)$
$B \subseteq C$	

We let x be arbitrary, assume $x \in A \cup B$, and try to prove $x \in C$. Thus we now have a new given $x \in A \cup B$, which we write as $x \in A \vee x \in B$, and our goal is now $x \in C$:

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

The goal cannot be analysed any further at this point, so we look at the givens. The first and second givens are useful if we ever come across objects that are elements of A or B. Moving on to the third given, because it has the form $P \vee Q$, we try proof by cases; for the first case we assume $x \in A$ and for the second $x \in B$. For the first case we have

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

We've come across an element of A; using our first given we can conclude that $x \in C$ proving our goal. The reasoning for the second case is similar, using the second given instead of the first.

Solution

Theorem. *Suppose that A, B, and C are sets. If $A \subseteq C$ and $B \subseteq C$ then $A \cup B \subseteq C$.*

Proof. Suppose $A \subseteq C$ and $B \subseteq C$, and let x be an arbitrary element of $A \cup B$. Then either $x \in A$ or $x \in B$.

Case 1. $x \in A$. Then since $A \subseteq C$, $x \in C$.

Case 2. $x \in B$. Then since $B \subseteq C$, $x \in C$.

Since we know that either $x \in A$ or $x \in B$, these cases cover all the possibilities, so we can conclude that $x \in C$. Since x was an arbitrary element of $A \cup B$, this means that $A \cup B \subseteq C$. □

(next page)

Cont.
Note that the cases in this proof are not exclusive—it is possible for both $x \in A$ and $x \in B$ to be true, so some values of x might fall under both cases. There is nothing wrong with this; the cases in a proof by cases must cover all possibilities, there is no harm in covering some possibilities more than once—the cases must be exhaustive, they need not be exclusive.

2.5.1 Goal of form $P \vee Q$ (part 1)

Proof by cases is sometimes also helpful if one is proving a goal of the form $P \vee Q$. If one can prove P in some cases and Q in others, then as long as the cases are exhaustive then one can conclude that $P \vee Q$ is true.

This method is particularly useful if one of the givens also has the form of a disjunction, since that would naturally imply a proof by cases.

> To prove a goal of the form $P \vee Q$:
> Break the proof into cases. In each case, either prove P or Q.

Example
Suppose that A, B and C are sets. Prove that $A \setminus (B \setminus C) \subseteq (A \setminus B) \cup C$.

Scratch work
The goal has the form $\forall x(x \in A \setminus (B \setminus C) \to x \in (A \setminus B) \cup C)$, we let x be arbitrary, assume $x \in A \setminus (B \setminus C)$, and try to prove $x \in (A \setminus B) \cup C$. Writing these statements out in logical symbols gives us

Givens	*Goal*
$x \in A \wedge \neg(x \in B \wedge x \notin C)$	$(x \in A \wedge x \notin B) \vee x \in C$

We split the given into two separate givens $x \in A$ and $\neg(x \in B \wedge x \notin C)$, and since the second is a negated statement we use De Morgan's law to reexpress it as a positive statement $x \notin B \vee x \in C$:

Givens	*Goal*
$x \in A$ $x \notin B \vee x \in C$	$(x \in A \wedge x \notin B) \vee x \in C$

Now the second given and the goal are both disjunctions, so we try considering the two cases $x \notin B$ and $x \in C$ suggested by the second given.
(next page)

Example cont.
If in each case we can either prove $x \in A \wedge x \notin B$ or $x \in C$, then the proof will be complete. For the first case we assume $x \notin B$

Givens	*Goal*
$x \in A$	$(x \in A \wedge x \notin B) \vee x \in C$
$x \notin B$	

In this case the goal is clearly true. For the second case we assume $x \in C$, and once again the goal is clearly true.

Solution

Theorem. *Suppose that A, B, and C are sets. Then $A \setminus (B \setminus C) \subseteq (A \setminus B) \cup C$.*

Proof. Suppose $x \in A \setminus (B \setminus C)$. Then $x \in A$ and $x \notin B \setminus C$. Since $x \notin B \setminus C$ it follows that either $x \notin B$ or $x \in C$. We will consider these cases separately.

Case 1. $x \notin B$. Then since $x \in A$, $x \in A \setminus B$, so $x \in (A \setminus B) \cup C$.
Case 2. $x \in C$. Then clearly $x \in (A \setminus B) \cup C$.

Since x was an arbitrary element of $A \setminus (B \setminus C)$, we can conclude that $A \setminus (B \setminus C) \subseteq (A \setminus B) \cup C$. □

2.5.2 Example: For integer x, the remainder when x^2 is divided by 4 is either 0 or 1

Sometimes one may find it useful to break a proof into cases even if the cases are not naturally suggested by a given of the form $P \vee Q$. Any proof can be broken into cases at any time, as long as the cases exhaust all of the possibilities.

Example
Prove that for every integer x, the remainder when x^2 is divided by 4 is either 0 or 1.

Scratch work
We start by letting x be an arbitrary integer and then try to prove that the remainder when x^2 is divided by 4 is either 0 or 1:

Givens	*Goal*
$x \in \mathbb{Z}$	($x^2 \div 4$ has remainder 0) $\vee$ ($x^2 \div 4$ has remainder 1)

(next page)

Cont.
Since the goal is a disjunction, breaking the proof into cases seems like a probable approach, but there is no given that suggests what cases to use. However, trying out a few values for x suggests the right cases

x	x^2	quotient of $x^2 \div 4$	remainder of $x^2 \div 4$
1	1	0	1
2	4	1	0
3	9	2	1
4	16	4	0
5	25	6	1
6	36	9	0

It appears that the remainder is 0 when x is even and 1 when x is odd. These are the cases we will use. Thus for case 1 we assume x is even and try to prove that the remainder is 0, and for case 2 we assume x is odd and prove that the remainder is 1. Because every integer is either even or odd, these cases are exhaustive.

Filling in the definition of *even*, here are our givens and goal for case 1:

Givens	*Goal*
$x \in \mathbb{Z}$	$x^2 \div 4$ has remainder 0
$\exists k \in \mathbb{Z}(x = 2k)$	

Immediately using the second given and letting k stand for some particular integer in which $x = 2k$, then $x^2 = (2k)^2 = 4k^2$, so clearly when we divide x^2 by 4 the quotient is k^2 and the remainder is 0. Case 2 is quite similar:

Givens	*Goal*
$x \in \mathbb{Z}$	$x^2 \div 4$ has remainder 1
$\exists k \in \mathbb{Z}(x = 2k + 1)$	

Once again we use the second given immediately and let k stand for an integer for which $x = 2k + 1$. Then $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$, so when x^2 is divided by 4 the quotient is $k^2 + k$ and the remainder is 1.

Solution

Theorem. *For every integer x, the remainder when x^2 is divided by 4 is either 0 or 1.*

Proof. Suppose x is an integer, we consider two cases.

Case 1. x is even. Then $x = 2k$ for some integer k, so $x^2 = 4k^2$. Clearly the remainder when x^2 is divided by 4 is 0.

Case 2. x is odd. Then $x = 2k+1$ for some integer k, so $x^2 = 4k^2+4k+1 = 4(k^2 + k) + 1$. Clearly in this case the remainder when x^2 is divided by 4 is 1. □

2.5.3 Goal of form $P \vee Q$ (part 2)

Sometimes in a proof with a goal of the form $P \vee Q$ it may be difficult to figure out how to break the proof into cases. Another strategy would be to simply assume that P is true in case 1 and assume that it is false in case 2; since P is either true or false, these cases are exhaustive.

In the first case, since one assumes P is true, the goal $P \vee Q$ is certainly true and no further reasoning is required. In the second case we assume P is false, and the only way for the goal $P \vee Q$ to be true is if Q is true; thus to complete this case one should try to prove Q.

> To prove a goal of the form $P \vee Q$:
> If P is true, then clearly the goal $P \vee Q$ is true, so one only needs to consider the case where P is false; one can complete the proof by proving that for that case Q is true.

Scratch work
Before using strategy:

Givens	*Goal*
—	$P \vee Q$
—	

After using strategy:

Givens	*Goal*
—	Q
—	
$\neg P$	

Form of final proof:

> If P is true, then of course $P \vee Q$ is true. Now suppose P is false.
> [Proof of Q goes here.]
> Thus $P \vee Q$ is true.

Note that this strategy is the same transformation one would use when proving the goal $\neg P \to Q$. This isn't suprising given that the statements $P \vee Q$ and $\neg P \to Q$ are equivalent.

Note that the roles of P and Q could also be reversed in this strategy—we can also prove $P \vee Q$ by assuming that Q is false and proving P.
(next page)

Example
Prove that for every real number x, if $x^2 \geq x$ then either $x \leq 0$ or $x \geq 1$.

Scratch work
Our goal is $\forall x(x^2 \geq x \to (x \leq 0 \vee x \geq 1))$, so to start we let x be an arbitrary real number, assume $x^2 \geq x$, and set $x \leq 0 \vee x \geq 1$ as our goal:

Givens	*Goal*
$x^2 \geq x$	$x \leq 0 \vee x \geq 1$

As per our strategy, to prove this we can either assume $x > 0$ and prove $x \geq 1$ or assume $x < 1$ and prove $x \leq 0$. We take the first approach.

Givens	*Goal*
$x^2 \geq x$	$x \geq 1$
$x > 0$	

The proof is now easy. Since $x > 0$, we can divide the given inequality $x^2 \geq x$ by x to get the goal $x \geq 1$.

Solution

Theorem. *For every real number x, if $x^2 \geq x$ then either $x \leq 0$ or $x \geq 1$.*

Proof. Suppose $x^2 \geq x$. If $x \leq 0$, then of course $x \leq 0$ or $x \geq 1$. Now suppose $x > 0$. Then we can divide both sides of the inequality $x^2 \geq x$ by x to conclude that $x \geq 1$. Thus either $x \leq 0$ or $x \geq 1$. □

2.5.4 Given of form $P \vee Q$ (part 2)

The equivalence of $P \vee Q$ and $\neg P \rightarrow Q$ suggests a rule of inference called *disjunctive syllogism* for using a given statement of the form $P \vee Q$:

> To use a given of the form $P \vee Q$:
> If one knows $\neg P$, or if one can prove P is false, then one can use this given to conclude that Q is true. Similarly if given $\neg Q$ or if one can prove Q is false, then one can conclude that P is true.

2.6 Existence and Uniqueness proofs

We consider proofs in which the goal has the form $\exists! x P(x)$, meaning 'there is exactly one x such that $P(x)$'. This can be thought as an abbreviation for the formula $\exists x(P(x) \wedge \neg\exists y(P(y) \wedge y \neq x))$.

As discussed, we could prove this goal by finding a particular x for which we could prove both $P(x)$ and $\neg\exists y(P(y) \wedge y \neq x))$. The second part would involve proving a negated statement, but we can reexpress it as an equivalent positive statement:

$$\begin{aligned} &\neg\exists y(P(y) \wedge y \neq x)) \\ &\quad \text{is equivalent to } \forall y \neg(P(y) \wedge y \neq x) && \text{(quantifier negation law)} \\ &\text{which is equivalent to } \forall y(P(y) \to y = x) && \text{(conditional law)} \end{aligned}$$

Thus see that $\exists! x P(x)$ could also be written as $\exists x(P(x) \wedge \forall y(P(y) \to y = x))$. We can prove that the following are all equivalent:

1. $\exists x(P(x) \wedge \forall y(P(y) \to y = x))$
2. $\exists x \forall y(P(y) \leftrightarrow y = x)$
3. $\exists x P(x) \wedge \forall y \forall z((P(y) \wedge P(z)) \to y = z)$

Scratch work
We have three biconditionals to prove: statement 1 iff statement 2, statement 1 iff statement 3, and statement 2 iff statement 3. Rather that proving 6 different conditionals, we will prove that statement 1 implies statement 2, statement 2 implies statement 3, and statement 3 implies statement 1.

Although we will not give a separate proof of the reverse direction, they are implied by these three proofs; for instance statement 2 implies 3 which implies 1, so statement 2 implies statement 1.

Because we'll be proving three conditional statements, our proof will have three parts, which we will label $1 \to 2, 2 \to 3$, and $3 \to 1$. We'll need to consider each part separately.
(next page)

1→2: $\exists x(P(x) \wedge \forall y(P(y) \to y = x)) \to \exists x \forall y(P(y) \leftrightarrow y = x)$
We assume statement 1 and prove statement 2. Given the existential quantifier in the given we choose a name, say x_0, for some object where both $P(x_0)$ and $\forall y(P(y) \to y = x_0)$:

Givens	*Goal*
$P(x_0)$	$\exists x \forall y(P(y) \leftrightarrow y = x)$
$\forall y(P(y) \to y = x_0)$	

Our goal starts with an existential quantifier, so we should try to find a value of x that makes the rest of the statement come out true. The obvious choice here is $x = x_0$; plugging in x_0, we must now prove $\forall y(P(y) \leftrightarrow y = x_0)$. We let y be arbitrary and prove both directions of the biconditional. $(\to)$ is clear by the second given. For $(\leftarrow)$, suppose $y = x_0$; since we have $P(x_0)$ as a given, we have $P(y)$.

2→3: $\exists x \forall y(P(y) \leftrightarrow y = x) \to \exists x P(x) \wedge \forall y \forall z((P(y) \wedge P(z)) \to y = z)$
As per our usual strategy for existential given statements, we let x_0 be some object such that $\forall y(P(y) \leftrightarrow y = x_0)$. The goal is a conjunction, so we treat it as two separate goals:

Givens	*Goal*
$\forall y(P(y) \leftrightarrow y = x_0)$	$\exists x P(x)$
	$\forall y \forall z((P(y) \wedge P(z)) \to y = z)$

To prove the first goal we choose $x = x_0$ and try to prove $P(x_0)$; plugging in x_0 for y in the given, we get $P(x_0) \leftrightarrow x_0 = x_0$. Since $x_0 = x_0$ is always true, we get $P(x_0)$ by the $\leftarrow$ direction of the bicondidtional. For the second goal, we let y and z be arbitrary, assume $P(y)$ and $P(z)$, and try to prove $y = z$:

Givens	*Goal*
$\forall y(P(y) \leftrightarrow y = x_0)$	$y = z$
$P(y)$	
$P(z)$	

Plugging in each of y and z into the first given we get $P(y) \leftrightarrow y = x_0$ and $P(z) \leftrightarrow z = x_0$. Since we've assumed $P(y)$ and $P(z)$ we use the $\to$ directions of these biconditionals to conclude that $y = x_0$ and $z = x_0$; our goal $y = z$ clearly follows.
(next page)

3→1:$\exists x P(x) \wedge \forall y \forall z((P(y) \wedge P(z)) \to y = z) \to \exists x(P(x) \wedge \forall y(P(y) \to y = x))$
We treat the given conjunction as two separate givens. The first is an existential statement so we let x_0 stand for some object such that $P(x_0)$ is true. The goal is an existential statement, we let $x = x_0$, leaving us with this situation:

Givens	*Goal*
$P(x_0)$	$P(x_0) \wedge \forall y(P(y) \to y = x_0)$
$\forall y \forall z((P(y) \wedge P(z)) \to y = z)$	

The first part of the goal is already proven. We only need to consider the second; we let y be arbitrary, assume $P(y)$ and make $y = x_0$ our goal:

Givens	*Goal*
$P(x_0)$	$y = x_0$
$\forall y \forall z((P(y) \wedge P(z)) \to y = z)$	
$P(y)$	

We know both $P(y)$ and $P(x_0)$. The goal follows from the second given.

Solution

Theorem. *The following are equivalent:*

1. $\exists x(P(x) \wedge \forall y(P(y) \to y = x))$
2. $\exists x \forall y(P(y) \leftrightarrow y = x)$
3. $\exists x P(x) \wedge \forall y \forall z((P(y) \wedge P(z)) \to y = z)$

Proof. $1 \to 2$. By statement 1, we can let x_0 be some object such that $P(x_0)$ and $\forall y(P(y) \to y = x_0)$ To prove statement 2 we will show that $\forall y(P(y) \leftrightarrow y = x_0)$. Let y be arbitrary. We already know the $\to$ direction of the biconditional. For the $\leftarrow$ direction, suppose $y = x_0$. Then since we know $P(x_0)$, we can conclude $P(y)$.

$2 \to 3$. By statement 2, choose x_0 such that $\forall y(P(y) \leftrightarrow y = x_0)$. Then, in particular, $P(x_0) \leftrightarrow x_0 = x_0$, and since clearly $x_0 = x_0$, it follows that $P(x_0)$ is true. Thus $\exists x P(x)$. To prove the second half of statement 3, let y and z be arbitrary and suppose $P(y)$ and $P(z)$. Then by our choice of x_0 (as something for which $\forall y(P(y) \leftrightarrow y = x_0)$ is true), it follows that $y = x_0$ and $z = x_0$, so $y = z$.

$3 \to 1$. By the first half of statement 3, let x_0 be some object such that $P(x_0)$. We will prove that $\forall y(P(y) \to y = x_0)$, so suppose $P(y)$. Since we have both $P(x_0)$ and $P(y)$, by the second half of statement 3 we can conclude that $y = x_0$, as required. □

2.6.1 Strategies and examples

As per the previous section, the following are equivalent:

1. $\exists x(P(x) \wedge \forall y(P(y) \rightarrow y = x))$
2. $\exists x \forall y(P(y) \leftrightarrow y = x)$
3. $\exists x P(x) \wedge \forall y \forall z((P(y) \wedge P(z)) \rightarrow y = z)$

Since all three of the statements in the theorem are equivalent to $\exists! x P(x)$, we can prove a goal of this form by proving any of the three statements in the theorem. The most common approach is using statement 3:

> To prove a goal of the form $\exists! x P(x)$:
> Prove $\exists x P(x)$ and $\forall y \forall z((P(y) \wedge P(z)) \rightarrow y = z)$. The first of these goals shows *existence*, the next *uniqueness*.

Form of final proof:

> Existence: [Proof of $\exists x P(x)$ goes here.]
> Uniqueness: [Proof of $\forall y \forall z((P(y) \wedge P(z)) \rightarrow y = z)$ goes here.]

Example
Prove that there is a unique set A such that for every set B, $A \cup B = B$.

Scratch work
Our goal is $\exists! A P(A)$, where $P(A)$ is the statement $\forall B(A \cup B = B)$. As per our strategy we prove existence and uniqueness separately.

For the existence half of the proof we must show $\exists A P(A)$, so we try to find a value of A that makes $P(A)$ true. There is no formula for finding this A, but one might eventually realise that the right choice is $A = \emptyset$. Plugging in this value we see that to complete the existence half of the proof we must show $\forall B(\emptyset \cup B = B)$, which is clearly true (this can be proven).

For the uniqueness half of the proof we prove $\forall C \forall D((P(C) \wedge P(D)) \rightarrow C = D)$. We let C and D be arbitrary, assume $P(C)$ and $P(D)$, and prove $C = D$:

Givens	*Goal*
$\forall B(C \cup B = B)$	$C = D$
$\forall B(D \cup B = B)$	

We plug in D for B in the first given, and C for B in the second. We get $C \cup D = D$ and $D \cup C = C$. But clearly $C \cup D = D \cup C$ (this can be proven). The goal $C = D$ follows immediately.
(next page)

Example cont.
Solution

Theorem. *There is a unique set A such that for every set B, $A \cup B = B$.*

Proof. Existence: Clearly $\forall B(\emptyset \cup B = B)$, so $\emptyset$ has the required property.

Uniqueness: Suppose $\forall B(C \cup B = B)$ and $\forall B(D \cup B = B)$. Applying the first of these assumptions to D we see that $C \cup D = D$, and applying the second to C we get $D \cup C = C$. But clearly $C \cup D = D \cup C$, so $C = D$. □

Alternative approach
The other equivalences can also be used. Statement 1 leads to the strategy:

> To prove a goal of the for $\exists! x P(x)$:
> Prove $\exists x(P(x) \wedge \forall y(P(y) \to y = x))$, using strategies from previous sections.

Example
Prove that for every real number x, if $x \neq 2$ then there is a unique real number y such that $2y/(y+1) = x$.

Scratch work
Our goal is $\forall x(x \neq 2 \to \exists! y(2y/(y_1) = x))$. We let x be arbitrary, assume $x \neq 2$, and prove $\exists! y(2y/(y+1) = x)$. As per our strategy, we can prove this goal by proving the equivalent statement

$$\exists y \left(\frac{2y}{y+1} = x \wedge \forall z \left(\frac{2z}{z+1} = x \to z = y \right) \right)$$

We start by trying to find some y that will make the equation $2y/(y+1) = x$ come out true. In other words, we solve this equation for y:

$$\frac{2y}{y+1} = x \implies 2y = x(y+1) \implies y(2-x) = x \implies y = \frac{x}{2-x}$$

Note that we have $x \neq 2$ so the last step makes sense. These steps will not appear in the proof; we simply let $y = x/(2-x)$ and try to prove $2/(y+1) = x$ and $\forall z(2z/(z+1) = x \to z = y)$.

Givens	*Goal*
$x \neq 2$	$\frac{2y}{y+1} = x$
$y = \frac{x}{2-x}$	$\forall z \left(\frac{2z}{z+1} = x \to z = y \right)$

The first goal is easy to verify by simply plugging in our candidate y.
(next page)

Example cont.
For the second goal, we let z be arbitrary, assume $2z(z+1) = x$, and prove $z = y$:

Givens	*Goal*
$x \neq 2$	$z = y$
$y = \frac{x}{2-x}$	
$\frac{2z}{z+1} = x$	

We can now show that $z = y$ by solving for z in the third given:

$$\frac{2z}{z+1} = x \implies 2z = x(z+1) \implies z(2-x) = x \implies z = \frac{x}{2-x} = y$$

Note that the steps we use here are exactly the same as the steps we used earlier in solving for y. This is a common pattern in existence and uniqueness proofs. Although the scratch work for figuring out an existence proof should not appear in the proof, this scratch work, or reasoning similar to it, can be sometimes used to demonstrate uniqueness.

Solution

Theorem. *For every real number x, if $x \neq 2$ then there is a unique real number y such that $2y/(y+1) = x$.*

Proof. Let x be an arbitrary real number, and suppose $x \neq 2$. Let $y = x/(2-x)$, which is defined since $x \neq 2$. Then

$$\frac{2y}{y+1} = \frac{\frac{2x}{2-x}}{\frac{x}{2-x}+1} = \frac{\frac{2x}{2-x}}{\frac{2}{2-x}} = \frac{2x}{2} = x$$

To see that this solution is unique, suppose $2z/(z+1) = x$. Then $2z = x(z+1)$, so $z(2-x) = x$. Since $x \neq 2$ we can divide both sides by $2-x$ to get $z = x/(2-x) = y$. □

2.6.2 Given of the form $\exists! x P(x)$

The three statements discussed earlier can also be used for givens of the form $\exists! x P(x)$. Once again, statement 3 of the theorem is the one used most often.

> To use a given of the form $\exists! x P(x)$:
> Treat this as two given statements $\exists x P(x)$ and $\forall y \forall z((P(y) \wedge P(z)) \rightarrow y = z)$. To use the first statement one should probably choose some x_0 to stand for some object where $P(x_0)$ is true. For the second, if one ever comes across two objects y and z such that $P(y)$ and $P(z)$ are both true, then one can conclude that $y = z$.

Example
Suppose A, B and C are sets, A and B are not disjoint, A and C are not disjoint, and A has exactly one element. Prove that B and C are not disjoint.

Scratch work

Givens	*Goal*
$A \cap B = \emptyset$	$B \cap C = \emptyset$
$A \cap C = \emptyset$	
$\exists! x(x \in A)$	

We treat the last given as two separate givens, as suggested by our strategy. We also analyse the logical forms of the other givens and the goal.

Givens	*Goal*
$\exists x(x \in A \wedge x \in B)$	$\exists x(x \in B \wedge x \in C)$
$\exists x(x \in A \wedge x \in C)$	
$\exists x(x \in A)$	
$\forall y \forall z((y \in A \wedge z \in A) \rightarrow y = z)$	

The first given tells use that we can choose a name, say b, for something such that $b \in A$ and $b \in B$. Similarly, by the second given we can let c be something such that $c \in A$ and $c \in C$. At this point the third given is redundant; we already know that there's something in A, so we may as well skip to the last given.

We know $b \in A$ and $c \in A$, so by the last given we can conclude that $b = c$. Since $b \in B$ and $b = c \in C$, we have found something that is an element of both B and C, as is required to prove the goal.
(next page)

Example cont.
Solution

Theorem. *Suppose A, B and C are sets, A and B are not disjoint, A and C are not disjoint, and A has exactly one element. Then B and C are not disjoint.*

Proof. Since A and B are not disjoint, we can let b be something such that $b \in A$ and $b \in B$. Similarly, since A and C are not disjoint, then there is some object c such that $c \in A$ and $c \in C$. Since A has only one element, we must have $b = c$. Thus $b = c \in B \cap C$ and therefore B and C are not disjoint. □

Appendix A

Exercises

A.1 Ch 3

A.1.1 $\exists x(P(x) \to Q(x))$ is equivalent to $\forall x P(x) \to \exists x Q(x)$

Using logical equivalences:

$$\begin{aligned}
\exists x(P(x) \to Q(x)) &= \exists x[\neg(P(x) \wedge \neg Q(x))] && \text{(Definition)} \\
&= \neg\forall x[P(x) \wedge \neg Q(x)] && \text{(Quantifier negation)} \\
&= \neg[\forall x P(x) \wedge \forall x \neg Q(x)] && \text{(Distributivity over conjuction)} \\
&= \neg[\forall x P(x) \wedge \neg\exists x Q(x)] && \text{(Quantifier negation)} \\
&= \forall x P(x) \to \exists x Q(x) && \text{(Definition)}
\end{aligned}$$

A.1.2 If $\exists x(P(x) \to Q(x))$, then $\forall x P(x) \to \exists x Q(x)$

Proof. Suppose $\exists x(P(x) \to Q(x))$. Then we can choose some x_0 such that $P(x_0) \to Q(x_0)$. Now suppose that $\forall x P(x)$. Then in particular, $P(x_0)$, and since $P(x_0) \to Q(x_0)$, it follows that $Q(x_0)$. Since we have found a particular value of x for which $Q(x)$ holds, we can conclude that $\exists x Q(x)$. Thus $\forall x P(x) \to \exists x Q(x)$. □

A.1.3