Conjunction

Conjunctive statements are of the form

\[ P \text{ and } Q \]

or, in other words,

both \( P \) and also \( Q \) hold

or, in symbols,

\[ P \land Q \quad \text{or} \quad P \& Q \]
The proof strategy for conjunction:

To prove a goal of the form

\[ P \land Q \]

first prove \( P \) and subsequently prove \( Q \) (or vice versa).
Proof pattern:
In order to prove \( P \land Q \)

1. Write: Firstly, we prove \( P \). and provide a proof of \( P \).
2. Write: Secondly, we prove \( Q \). and provide a proof of \( Q \).
Scratch work:

Before using the strategy

Assumptions  Goal

\[ P \land Q \]

: 

After using the strategy

\[ P \]

\[ Q \]

: 

: 
The use of conjunctions:

To use an assumption of the form \( P \land Q \), treat it as two separate assumptions: \( P \) and \( Q \).
Theorem 20  For every integer \( n \), we have that \( 6 \mid n \) iff \( 2 \mid n \) and \( 3 \mid n \).

**Proof:**  

\( \forall n \in \mathbb{Z}, \ 6 \mid n \iff 2 \mid n \) \& \( 3 \mid n \).  

Let \( n \) be an integer.  

**RTP:** \( 6 \mid n \iff 2 \mid n \) \& \( 3 \mid n \).  

\( \Rightarrow \) Ass. \( 6 \mid n \), i.e. \( n = 6k \) for an integer \( k \).  

\[ 
\therefore \quad n = k \cdot 6 \quad \therefore \quad n = 2 \cdot (k \cdot 3) \quad \therefore \quad 2 \mid n. 
\]

\[ 
\therefore \quad n = 3 \cdot (k \cdot 2) \quad \therefore \quad 3 \mid n. \quad \therefore \quad 2 \mid n \) \& \( 3 \mid n. \)

\( \Leftarrow \) Ass. \( 2 \mid n \) and \( 3 \mid n \), i.e.  

\[ 
\therefore \quad n = 2i \quad \text{and} \quad n = 3j \quad \text{for integers} \ i, j.
\]

\[ 
\therefore \quad 3 \cdot n = 3 \cdot 2 \cdot i = 6i
\]

\[ 
\therefore \quad 2 \cdot n = 2 \cdot 3 \cdot j = 6j
\]

\[ 
\therefore \quad \text{whence} \quad n = 3 \cdot n - 2 \cdot n = 6i - 6j = 6(i - j).
\]

\[ 
\therefore \quad 6 \mid n.
\]
**Existential quantification**

Existential statements are of the form

there exists an individual \( x \) in the universe of discourse for which the property \( P(x) \) holds

or, in other words,

for some individual \( x \) in the universe of discourse, the property \( P(x) \) holds

or, in symbols,

\[
\exists x. P(x)
\]
Example: The Pigeonhole Principle.

Let $n$ be a positive integer. If $n + 1$ letters are put in $n$ pigeonholes then there will be a pigeonhole with more than one letter.
Theorem 21 (Intermediate value theorem) Let $f$ be a real-valued continuous function on an interval $[a, b]$. For every $y$ in between $f(a)$ and $f(b)$, there exists $v$ in between $a$ and $b$ such that $f(v) = y$.

Intuition:
The main proof strategy for existential statements:

To prove a goal of the form

$$\exists x. \, P(x)$$

find a *witness* for the existential statement; that is, a value of \( x \), say \( w \), for which you think \( P(x) \) will be true, and show that indeed \( P(w) \), i.e. the predicate \( P(x) \) instantiated with the value \( w \), holds.
Proof pattern:
In order to prove $\exists x. P(x)$

1. Write: Let $w = \ldots$ (the witness you decided on).
2. Provide a proof of $P(w)$. 

$\exists y. P(y)$

$\forall x. (\exists y. y + 1 = x)$

$\forall y. (\forall x. x + 1) \lor (\exists x. x + 1)$
Scratch work:

Before using the strategy

Assumptions

\[ \exists x. P(x) \]

After using the strategy

Assumptions

\[ P(w) \]

\[ w = \ldots \text{(the witness you decided on)} \]
Proposition 22 \textit{For every positive integer $k$, there exist natural numbers $i$ and $j$ such that $4 \cdot k = i^2 - j^2$.}

\textbf{Proof:} Let $k$ be a positive integer. RTP \textit{Exist $i$ and $j$ such that $4k = i^2 - j^2$.}

Want numbers $i_0$ and $j_0$, not nos, s.t.

\[ 4k = i_0^2 - j_0^2. \]

Take $i_0 = k + 1$, $j_0 = k - 1$.

Then $i_0^2 - j_0^2 = (k + 1)^2 - (k - 1)^2$

\[ = k^2 + 2k + 1 - k^2 - 2k + 1 = 4k. \]

\[ \therefore \text{ Exist } i, j \text{ s. t. } 4k = i^2 - j^2. \]
The use of existential statements:

To use an assumption of the form $\exists x. P(x)$, introduce a new variable $x_0$ into the proof to stand for some individual for which the property $P(x)$ holds. This means that you can now assume $P(x_0)$ true.
Theorem 24  For all integers \( l, m, n \), if \( l \mid m \) and \( m \mid n \) then \( l \mid n \).

Proof:  Let \( l, m, n \) be integers. RTP \( l \mid m \) \( \& \) \( m \mid n \) \( \Rightarrow \) \( l \mid n \).

Assume \( l \mid m \) \( \& \) \( m \mid n \), ie. \( \exists i. m = i \cdot l \) and \( \exists j. n = j \cdot m \).

So there are witnesses \( i_0, j_0 \) such that \( m = i_0 \cdot l \) and \( n = j_0 \cdot m \).

RTP. \( \exists k. n = k \cdot l \). Want \( k_0 \equiv k \cdot i_0 \cdot j_0 \).

We have \( n = j_0 \cdot m = j_0 \cdot i_0 \cdot l = (j_0 \cdot i_0) \cdot l \).

So \( k_0 = j_0 \cdot i_0 \) is a witness for \( \exists k. n = k \cdot l \).
Unique existence

The notation

$$\exists! x. P(x)$$

stands for

the *unique existence* of an $x$ for which the property $P(x)$ holds.

That is,

$$\exists x. P(x) \land \left( \forall y. \forall z. (P(y) \land P(z)) \Rightarrow y = z \right)$$
Disjunction

Disjunctive statements are of the form

\[ P \text{ or } Q \]

or, in other words,

either \( P, Q, \) or both hold

or, in symbols,

\[ P \lor Q \]