Logic
It’s so easy even computers can do it!
Logic
It's so easy even computers can do it!

OK, It's not that easy!
New Kinds of Propositions
(First-Order) Predicate Calculus

<table>
<thead>
<tr>
<th>x</th>
<th>Winged(x)</th>
<th>Flies(x)</th>
<th>Pink(x)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Jabberwock</td>
<td>TRUE</td>
<td>TRUE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Flamingo</td>
<td>TRUE</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
</tbody>
</table>

- **Universal quantifier:** $\forall x \text{ Winged}(x)$
  
  means $\text{Winged}(\text{Alice}) \land \text{Winged}(J'\text{wock}) \land \text{Winged}(\text{Flamingo})$

- **Existential quantifier:** $\exists x \text{ Winged}(x)$

  means $\text{Winged}(\text{Alice}) \lor \text{Winged}(J'\text{wock}) \lor \text{Winged}(\text{Flamingo})$
# The Looking Glass

Reflection changes $T \land F$ to $F \land T$ (resp.)

$\lor \land$ are reflected as $\land \lor$ (resp.)

$\forall \land \exists$ are reflected as $\exists \land \forall$ (resp.)

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$p \land q$</th>
<th>$\neg p$</th>
<th>$\neg q$</th>
<th>$\neg p \lor \neg q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\lor$</td>
<td>$\land$</td>
<td>$\land$</td>
<td>$\lor$</td>
<td>$\land$</td>
<td>$\lor$</td>
</tr>
<tr>
<td>$\forall x \text{ Pred}(x)$</td>
<td>$\exists x \neg \text{ Pred}(x)$</td>
<td>$\exists x \neg \text{ Pred}(x)$</td>
<td>$\forall x \neg \text{ Pred}(x)$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Another example

<table>
<thead>
<tr>
<th>x</th>
<th>y</th>
<th>Likes(x,y)</th>
<th>x=y</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>Alice</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td>Jabberwock</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Flamingo</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Jabberwock</td>
<td>FALSE</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td>Flamingo</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Alice</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Jabberwock</td>
<td>FALSE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Flamingo</td>
<td>TRUE</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
</tbody>
</table>

∀x,y (x=y) → Likes(x,y)

∀x,y Likes(x,y) → (x=y)
Another example

<table>
<thead>
<tr>
<th>x</th>
<th>y</th>
<th>Likes(x,y)</th>
<th>x=y</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>Alice</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td></td>
<td>Jabberwock</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td></td>
<td>Flamingo</td>
<td>TRUE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Jabberwock</td>
<td>Alice</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td></td>
<td>Jabberwock</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td></td>
<td>Flamingo</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Flamingo</td>
<td>Alice</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td></td>
<td>Jabberwock</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td></td>
<td>Flamingo</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
</tbody>
</table>

∀x,y (x=y) → Likes(x,y)

Everyone likes themselves (True)

∀x,y Likes(x,y) → (x=y)
Another example

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>Likes(x,y)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>Alice</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td>Alice</td>
<td>Jabberwock</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Alice</td>
<td>Flamingo</td>
<td>TRUE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Jabberwock</td>
<td>Alice</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Jabberwock</td>
<td>Jabberwock</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td>Jabberwock</td>
<td>Flamingo</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Flamingo</td>
<td>Alice</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Flamingo</td>
<td>Jabberwock</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Flamingo</td>
<td>Flamingo</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
</tbody>
</table>

\( \forall x, y \ (x=y) \rightarrow \text{Likes}(x,y) \)

\( \forall x, y \ \text{Likes}(x,y) \rightarrow (x=y) \)

Everyone likes themselves (True)

Everyone likes only themselves, if at all anyone (False)
Question

Everyone who flies is winged

A. \( \forall x \text{ Flies}(x) \lor \text{Winged}(x) \)
B. \( \forall x \text{ Flies}(x) \land \text{Winged}(x) \)
C. \( \forall x \text{ Flies}(x) \rightarrow \text{Winged}(x) \)
D. \( \forall x \text{ Flies}(x) \leftrightarrow \text{Winged}(x) \)
E. \( \forall x \text{ Flies}(x) \leftarrow \text{Winged}(x) \)
Everyone who flies is winged

A. $\forall x \; \text{Flies}(x) \lor \text{Winged}(x)$
B. $\forall x \; \text{Flies}(x) \land \text{Winged}(x)$
C. $\forall x \; \text{Flies}(x) \rightarrow \text{Winged}(x)$
D. $\forall x \; \text{Flies}(x) \leftrightarrow \text{Winged}(x)$
E. $\forall x \; \text{Flies}(x) \leftarrow \text{Winged}(x)$

If anyone flies then he/she/it is winged
∀x P(x) → R \quad (R \text{ independent of } x)

If for any x, P(x) holds, then R holds

A. \((\forall x \ P(x)) \rightarrow R\)
B. \(\exists x \ P(x) \rightarrow R\)
C. \((\exists x \ P(x)) \rightarrow R\)
D. \((\exists x \ P(x)) \lor R\)
E. \((\forall x \ P(x)) \land R\)
Moving the Quantifiers
Moving the Quantifiers

\( \forall x \ P(x) \rightarrow R \)  \((R\ \text{independent of } x)\)

If for any \( x \) \( P(x) \) holds, then \( R \) holds
Moving the Quantifiers

\[ \forall x \ P(x) \rightarrow R \quad (R \text{ independent of } x) \]
If for any \( x \) \( P(x) \) holds, then \( R \) holds

\[ \forall x \ \neg P(x) \lor R \equiv (\forall x \ \neg P(x)) \lor R \]
\[ \equiv \neg (\exists x \ P(x)) \lor R \]
\[ \equiv (\exists x \ P(x)) \rightarrow R \]
Moving the Quantifiers

\( \forall x \ P(x) \rightarrow R \)  \( (R \ \text{independent of} \ x) \)
If for any \( x \) \( P(x) \) holds, then \( R \) holds

\( \forall x \ \neg P(x) \lor R \equiv (\forall x \ \neg P(x)) \lor R \)
\( \equiv \neg (\exists x \ P(x)) \lor R \)
\( \equiv (\exists x \ P(x)) \rightarrow R \)

\( \exists x \ P(x) \rightarrow R \)  \( (R \ \text{independent of} \ x) \)
Either for some \( x \) \( P(x) \) is false (and hence \( P(x) \rightarrow R \) vacuously true) or else \( R \) holds
Moving the Quantifiers

\[ \forall x \ P(x) \rightarrow R \quad (R \text{ independent of } x) \]
If for any \( x \) \( P(x) \) holds, then \( R \) holds

\[ \forall x \ \neg P(x) \vee R \equiv (\forall x \ \neg P(x)) \vee R \]
\[ \equiv \neg(\exists x \ P(x)) \vee R \]
\[ \equiv (\exists x \ P(x)) \rightarrow R \]

\[ \exists x \ P(x) \rightarrow R \quad (R \text{ independent of } x) \]
Either for some \( x \) \( P(x) \) is false (and hence \( P(x) \rightarrow R \) vacuously true) or else \( R \) holds

\[ \exists x \ \neg P(x) \vee R \equiv (\exists x \ \neg P(x)) \vee R \]
\[ \equiv \neg(\forall x \ P(x)) \vee R \]
\[ \equiv (\forall x \ P(x)) \rightarrow R \]
Moving the Quantifiers

- $\forall x \forall y P(x,y) \equiv \forall y \forall x P(x,y)$
- $\exists x \exists y P(x,y) \equiv \exists y \exists x P(x,y)$

When $R$ is independent of $x$

- $\forall x P(x) \lor R \equiv (\forall x P(x)) \lor R$
- $\exists x P(x) \lor R \equiv (\exists x P(x)) \lor R$
- $\forall x R \rightarrow P(x) \equiv R \rightarrow (\forall x P(x))$
- $\exists x R \rightarrow P(x) \equiv R \rightarrow (\exists x P(x))$
- $\forall x P(x) \rightarrow R \equiv (\exists x P(x)) \rightarrow R$
- $\exists x P(x) \rightarrow R \equiv (\forall x P(x)) \rightarrow R$
Moving the Quantifiers

\[ \forall x \; \forall y \; P(x,y) \equiv \forall y \; \forall x \; P(x,y) \]

\[ \exists x \; \exists y \; P(x,y) \equiv \exists y \; \exists x \; P(x,y) \]

When \( R \) is independent of \( x \)

\[ \forall x \; P(x) \lor R \equiv (\forall x \; P(x)) \lor R \]

\[ \exists x \; P(x) \lor R \equiv (\exists x \; P(x)) \lor R \]

\[ \forall x \; R \to P(x) \equiv R \to (\forall x \; P(x)) \]

\[ \forall x \; P(x) \to R \equiv (\exists x \; P(x)) \to R \]

\[ \exists x \; P(x) \to R \equiv (\forall x \; P(x)) \to R \]

\[ \exists x \; P(x) \land R \equiv (\exists x \; P(x)) \land R \]

\[ \forall x \; P(x) \land R \equiv (\forall x \; P(x)) \land R \]

\[ \exists x \; R \to P(x) \equiv R \to (\exists x \; P(x)) \]

\[ \exists x \; P(x) \to R \equiv (\forall x \; P(x)) \to R \]

\[ \forall x \; P(x) \to R \equiv (\exists x \; P(x)) \to R \]

\[ \exists x \; P(x) \to R \equiv (\forall x \; P(x)) \to R \]

not the mirror!
Moving the Quantifiers

- $\forall x \forall y P(x,y) \equiv \forall y \forall x P(x,y)$
- $\exists x \exists y P(x,y) \equiv \exists y \exists x P(x,y)$
- When $R$ is independent of $x$
  - $\forall x P(x) \lor R \equiv (\forall x P(x)) \lor R$
  - $\exists x P(x) \lor R \equiv (\exists x P(x)) \lor R$
  - $\forall x R \rightarrow P(x) \equiv R \rightarrow (\forall x P(x))$
  - $\exists x R \rightarrow P(x) \equiv R \rightarrow (\exists x P(x))$
  - $\forall x P(x) \rightarrow R \equiv (\exists x P(x)) \rightarrow R$
  - $\exists x P(x) \rightarrow R \equiv (\forall x P(x)) \rightarrow R$
- $(\forall x P(x)) \land (\forall x Q(x)) \equiv \forall x (P(x) \land Q(x))$
Moving the Quantifiers

∀x∀y P(x,y) ≡ ∀y∀x P(x,y)

∃x∃y P(x,y) ≡ ∃y∃x P(x,y)

When $R$ is independent of $x$

∀x P(x) ∨ R ≡ (∀x P(x)) ∨ R
∃x P(x) ∨ R ≡ (∃x P(x)) ∨ R
∀x R → P(x) ≡ R → (∀x P(x))
∀x P(x) → R ≡ (∃x P(x)) → R

(∀x P(x)) ∧ (∀x Q(x)) ≡ ∀x (P(x) ∧ Q(x))

But (∀x P(x)) ∨ (∀x Q(x)) ≠ ∀x (P(x) ∨ Q(x))
Moving the Quantifiers

\[ \forall x \forall y \, P(x,y) \equiv \forall y \, \forall x \, P(x,y) \]

\[ \exists x \, \exists y \, P(x,y) \equiv \exists y \, \exists x \, P(x,y) \]

When \( R \) is independent of \( x \)

\[ \forall x \, P(x) \lor R \equiv (\forall x \, P(x)) \lor R \]

\[ \exists x \, P(x) \lor R \equiv (\exists x \, P(x)) \lor R \]

\[ \forall x \, R \to P(x) \equiv R \to (\forall x \, P(x)) \]

\[ \forall x \, P(x) \to R \equiv (\exists x \, P(x)) \to R \]

\[ (\forall x \, P(x)) \land (\forall x \, Q(x)) \equiv \forall x \, (P(x) \land Q(x)) \]

But \( (\forall x \, P(x)) \lor (\forall x \, Q(x)) \not\equiv \forall x \, (P(x) \lor Q(x)) \)

\[ (\exists x \, P(x)) \lor (\exists x \, Q(x)) \equiv \exists x \, (P(x) \lor Q(x)) \]
Moving the Quantifiers

∀x ∀y P(x,y) ≡ ∀y ∀x P(x,y)

∃x ∃y P(x,y) ≡ ∃y ∃x P(x,y)

When R is independent of x

∀x P(x) ∨ R ≡ (∀x P(x)) ∨ R

∃x P(x) ∨ R ≡ (∃x P(x)) ∨ R

∀x R → P(x) ≡ R → (∀x P(x))

∃x R → P(x) ≡ R → (∃x P(x))

(∀x P(x)) ∧ (∀x Q(x)) ≡ ∀x (P(x) ∧ Q(x))

But (∀x P(x)) ∨ (∀x Q(x)) ⊈ ∀x (P(x) ∨ Q(x))

(∃x P(x)) ∨ (∃x Q(x)) ≡ ∃x (P(x) ∨ Q(x))

But (∃x P(x)) ∧ (∃x Q(x)) ⊈ ∃x (P(x) ∧ Q(x))

not the mirror!
\( \forall x, y \, \text{Pink}(x) \rightarrow \text{Flies}(y) \)

A. If anyone is pink, he/she/it flies
B. If no one flies, someone is not pink
C. If anyone is pink, everyone flies
D. If anyone is pink, someone flies
E. If everyone is pink, everyone flies
Answer
Answer

∀x∀y P(x) → Q(y)

∀x P(x) → (∀y Q(y))
∀x  ∀y  P(x) → Q(y)

∀x  P(x) → (∀y  Q(y))

∀x  P(x) → R ≡ ( ∃x  P(x) ) → R
∀x  ∀y  P(x) → Q(y)

∀x  P(x) → (∀y Q(y))

∀x  P(x) → R  ≡  ( ∃x  P(x) ) → R

∀x,y  P(x) → Q(y)  ≡  ( ∃x  P(x) ) → ( ∀y  Q(y) )
Example

“If someone flies, everyone flies” is the same as which one(s)?

1. \((\exists x \text{ Flies}(x)) \rightarrow (\forall x \text{ Flies}(x))\)
2. \(\forall x,y \text{ Flies}(x) \leftrightarrow \text{ Flies}(y)\)
3. \(\exists x \forall y \text{ Flies}(x) \leftrightarrow \text{ Flies}(y)\)
4. \(\exists x \forall y \text{ Flies}(x) \rightarrow \text{ Flies}(y)\)
"If someone flies, everyone flies" is the same as which one(s)?

1. \((\exists x \text{ Flies}(x)) \rightarrow (\forall x \text{ Flies}(x))\)
2. \(\forall x,y \text{ Flies}(x) \leftrightarrow \text{ Flies}(y)\)
3. \(\exists x \forall y \text{ Flies}(x) \leftrightarrow \text{ Flies}(y)\)
4. \(\exists x \forall y \text{ Flies}(x) \rightarrow \text{ Flies}(y)\)

Always true! (a.k.a, tautology)
But why?
Proofs: Logic in Action
Using Logic
Using Logic

Logic is used to deduce results in any (mathematically defined) system.
Using Logic

Logic is used to deduce results in any (mathematically defined) system

Typically a human endeavor
Using Logic

- Logic is used to deduce results in any (mathematically defined) system
- Typically a human endeavor
- But can be automated if the system is relatively simple
Using Logic

- Logic is used to deduce results in any (mathematically defined) system
- Typically a human endeavor
- But can be automated if the system is relatively simple
- Artificial Intelligence!
What are we proving?
What are we proving?

We are proving propositions
What are we proving?

- We are proving propositions
- Often called Theorems, Lemmas, Claims, ...
What are we proving?

We are proving propositions

Often called Theorems, Lemmas, Claims, ...

Propositions use various predicates already specified as Definitions
What are we proving?

- We are proving propositions
  - Often called Theorems, Lemmas, Claims, ...
- Propositions use various predicates already specified as Definitions
- e.g. All positive even numbers are larger than 1
What are we proving?

We are proving propositions
Often called Theorems, Lemmas, Claims, ...
Propositions use various predicates already specified as Definitions
e.g. All positive even numbers are larger than 1
∀x∈ℤ ( Positive(x) ∧ Even(x) ) → Greater(x,1)
What are we proving?

- We are proving propositions
  - Often called Theorems, Lemmas, Claims, ...
- Propositions use various predicates already specified as Definitions
  - e.g. All positive even numbers are larger than 1
    - $\forall x \in \mathbb{Z} \ ( \text{Positive}(x) \land \text{Even}(x) ) \rightarrow \text{Greater}(x,1)$
- These predicates are specific to the system (here arithmetic).
  - The system will have its own “axioms” too (e.g., $\forall x \ x+0=x$)
What are we proving?

- We are proving propositions
  - Often called Theorems, Lemmas, Claims, ...
  - Propositions use various predicates already specified as Definitions
  - e.g. All positive even numbers are larger than 1
    \[ \forall x \in \mathbb{Z} \ ( \text{Positive}(x) \land \text{Even}(x) ) \rightarrow \text{Greater}(x,1) \]
  - These predicates are specific to the system (here arithmetic).
    The system will have its own “axioms” too (e.g., \( \forall x \ x+0=x \))
  - For us, numbers (reals, integers, rationals) and other systems like sets, graphs, functions, ...
What are we proving?

- We are proving propositions
  - Often called Theorems, Lemmas, Claims, ...
- Propositions use various predicates already specified as Definitions
  - e.g. All positive even numbers are larger than 1
    \[ \forall x \in \mathbb{Z} \ ( \text{Positive}(x) \land \text{Even}(x) ) \rightarrow \text{Greater}(x,1) \]
- These predicates are specific to the system (here arithmetic). The system will have its own “axioms” too (e.g., \( \forall x \ x+0=x \))
  - For us, numbers (reals, integers, rationals) and other systems like sets, graphs, functions, ...
- Goal: Use logical operations to establish the truth of a given proposition, starting from the axioms (or already proven propositions) in a system
Example

Our system here is that of integers (comes with the set of integers $\mathbb{Z}$ and operations like $+$, $-$, $\times$, $/$, exponentiation...)
Example

- Our system here is that of integers (comes with the set of integers $\mathbb{Z}$ and operations like $+$, $-$, $\times$, $\div$, exponentiation...)

- We will not attempt to formally define this system!
Our system here is that of integers (comes with the set of integers $\mathbb{Z}$ and operations like $+$, $-$, $\times$, $/$, exponentiation...)

We will not attempt to formally define this system!

**Definition:** An integer $x$ is said to be odd if there is an integer $y$ s.t. $x=2y+1$
Example

Our system here is that of integers (comes with the set of integers $\mathbb{Z}$ and operations like $+$, $-$, $\ast$, $/$, exponentiation...)

We will not attempt to formally define this system!

**Definition:** An integer $x$ is said to be odd if there is an integer $y$ s.t. $x = 2y + 1$

"if" used by convention; actually means "iff"
Our system here is that of integers (comes with the set of integers $\mathbb{Z}$ and operations like $+,-,\times,\div$, exponentiation...)

We will not attempt to formally define this system!

**Definition:** An integer $x$ is said to be odd if there is an integer $y$ s.t. $x=2y+1$

$\text{Odd}(x) \equiv \exists y \in \mathbb{Z} \ (x = 2y+1)$

"if" used by convention; actually means "iff"
Example

Our system here is that of integers (comes with the set of integers \( \mathbb{Z} \) and operations like +, -, *, /, exponentiation...)

We will not attempt to formally define this system!

Definition: An integer \( x \) is said to be odd if there is an integer \( y \) s.t. \( x = 2y + 1 \)

\[ \text{Odd}(x) \equiv \exists y \in \mathbb{Z} \ (x = 2y + 1) \]

Proposition: If \( x \) is an odd integer, so is \( x^2 \)

“if” used by convention; actually means “iff”
Example

Our system here is that of integers (comes with the set of integers $\mathbb{Z}$ and operations like +, -, *, /, exponentiation...)

We will not attempt to formally define this system!

**Definition**: An integer $x$ is said to be odd if there is an integer $y$ s.t. $x = 2y + 1$

$\text{Odd}(x) \equiv \exists y \in \mathbb{Z} \ (x = 2y + 1)$

**Proposition**: If $x$ is an odd integer, so is $x^2$

$\forall x \in \mathbb{Z} \ \text{Odd}(x) \rightarrow \text{Odd}(x^2)$
Example

Def: $\text{Odd}(x) \equiv \exists y \in \mathbb{Z} \ (x = 2y + 1)$
Example

- Def: $\text{Odd}(x) \equiv \exists y \in \mathbb{Z} \ (x = 2y+1)$
- Proposition: $\forall x \in \mathbb{Z} \ \text{Odd}(x) \rightarrow \text{Odd}(x^2)$
Example

- **Def:** Odd(x) \( \equiv \exists y \in \mathbb{Z} \ (x = 2y + 1) \)
- **Proposition:** \( \forall x \in \mathbb{Z} \) Odd(x) \( \rightarrow \) Odd\((x^2)\)
- **Proof:** (should be written in more readable English)
Example

- **Def:** $\text{Odd}(x) \equiv \exists y \in \mathbb{Z} \ (x = 2y+1)$
- **Proposition:** $\forall x \in \mathbb{Z} \ \text{Odd}(x) \rightarrow \text{Odd}(x^2)$
- **Proof:** *(should be written in more readable English)*
  - Let $x$ be an arbitrary element of $\mathbb{Z}$
Example

\( \text{Def: Odd}(x) \equiv \exists y \in \mathbb{Z} \ (x = 2y + 1) \)

Proposition: \( \forall x \in \mathbb{Z} \ \text{Odd}(x) \rightarrow \text{Odd}(x^2) \)

Proof: (should be written in more readable English)

- Let \( x \) be an arbitrary element of \( \mathbb{Z} \)
- Suppose \( \text{Odd}(x) \). Then, we need to show \( \text{Odd}(x^2) \).
Example

- Def: \( \text{Odd}(x) \equiv \exists y \in \mathbb{Z} \ (x = 2y+1) \)
- Proposition: \( \forall x \in \mathbb{Z} \ \text{Odd}(x) \rightarrow \text{Odd}(x^2) \)
- Proof: (should be written in more readable English)
  - Let \( x \) be an arbitrary element of \( \mathbb{Z} \)
  - Suppose \( \text{Odd}(x) \). Then, we need to show \( \text{Odd}(x^2) \).
  - Then by definition, \( \exists y \in \mathbb{Z} \ x = 2y+1 \).
Example

Def: Odd(x) ≡ ∃y ∈ ℤ (x = 2y + 1)

Proposition: ∀x ∈ ℤ Odd(x) → Odd(x²)

Proof: (should be written in more readable English)
- Let x be an arbitrary element of ℤ
- Suppose Odd(x). Then, we need to show Odd(x²).
- Then by definition, ∃y ∈ ℤ x = 2y + 1.
- Then, \( x^2 = (2y + 1)^2 \)
  \[ = 4y^2 + 4y + 1 \]
  \[ = 2(2y^2 + 2y) + 1. \] From arithmetic.
Example

- **Def:** $\text{Odd}(x) \equiv \exists y \in \mathbb{Z} \ (x = 2y+1)$

- **Proposition:** $\forall x \in \mathbb{Z} \ \text{Odd}(x) \rightarrow \text{Odd}(x^2)$

- **Proof:** (should be written in more readable English)
  
  Let $x$ be an arbitrary element of $\mathbb{Z}$

  Suppose $\text{Odd}(x)$. Then, we need to show $\text{Odd}(x^2)$.

  Then by definition, $\exists y \in \mathbb{Z} \ x=2y+1$.

  Then, $x^2 = (2y+1)^2$

  $= 4y^2 + 4y + 1$

  $= 2(2y^2+2y) + 1$. From arithmetic.

  $\exists w \in \mathbb{Z} \ (2y^2+2y)=w$. From arithmetic.
Example

- **Def:** \( \text{Odd}(x) \equiv \exists y \in \mathbb{Z} \ (x = 2y+1) \)

- **Proposition:** \( \forall x \in \mathbb{Z} \ \text{Odd}(x) \rightarrow \text{Odd}(x^2) \)

- **Proof:** (should be written in more readable English)
  
  Let \( x \) be an arbitrary element of \( \mathbb{Z} \).
  
  Suppose \( \text{Odd}(x) \). Then, we need to show \( \text{Odd}(x^2) \).
  
  Then by definition, \( \exists y \in \mathbb{Z} \ x = 2y+1 \).
  
  Then, \( x^2 = (2y+1)^2 \)
  
  \[ = 4y^2 + 4y + 1 \]
  
  \[ = 2(2y^2+2y) + 1 \quad \text{From arithmetic.} \]
  
  \( \exists w \in \mathbb{Z} \ (2y^2+2y) = w \). \quad \text{From arithmetic.} \)
  
  Hence, \( \exists w \in \mathbb{Z} \ x^2 = 2w+1 \)
Example

Def: Odd(x) ≡ ∃y ∈ ℤ (x = 2y+1)

Proposition: ∀x ∈ ℤ Odd(x) → Odd(x²)

Proof: (should be written in more readable English)

Let x be an arbitrary element of ℤ

Suppose Odd(x). Then, we need to show Odd(x²).

Then by definition, ∃y ∈ ℤ x=2y+1.

Then, x² = (2y+1)²
= 4y² + 4y + 1
= 2(2y²+2y) + 1. From arithmetic.

∃w ∈ ℤ (2y²+2y) = w. From arithmetic.

Hence, ∃w ∈ ℤ x² = 2w+1

By definition Odd(x²). QED.
Template

To prove $\forall x \ P(x) \rightarrow Q(x)$
To prove $\forall x \ P(x) \rightarrow Q(x)$

Let $x$ be an arbitrary element (in the domain of the predicates $P$ and $Q$)
Template

To prove $\forall x \ P(x) \rightarrow Q(x)$

Let $x$ be an arbitrary element (in the domain of the predicates $P$ and $Q$)

Assume $P(x)$ holds (call this $p_0$)
To prove $\forall x \ P(x) \rightarrow Q(x)$

- Let $x$ be an arbitrary element (in the domain of the predicates $P$ and $Q$)
- Assume $P(x)$ holds (call this $p_0$)
- Derive propositions $p_1, p_2, ..., p_n$ where for each $i$, either $p_i$ is an axiom or an already proven proposition in the system, or $(p_0 \land p_1 \land ... \land p_{i-1}) \rightarrow p_i$
To prove $\forall x \ P(x) \rightarrow Q(x)$

Let $x$ be an arbitrary element (in the domain of the predicates $P$ and $Q$)

Assume $P(x)$ holds (call this $p_0$)

Derive propositions $p_1, p_2, ..., p_n$ where for each $i$, either $p_i$ is an axiom or an already proven proposition in the system, or $(p_0 \land p_1 \land ... \land p_{i-1}) \rightarrow p_i$

Usually one or two propositions so far imply the next
To prove \( \forall x \; P(x) \rightarrow Q(x) \)

Let \( x \) be an arbitrary element (in the domain of the predicates \( P \) and \( Q \))

Assume \( P(x) \) holds (call this \( p_0 \))

Derive propositions \( p_1, p_2, \ldots, p_n \) where for each i, either \( p_i \) is an axiom or an already proven proposition in the system, or \( (p_0 \land p_1 \land \ldots \land p_{i-1}) \rightarrow p_i \)

Usually one or two propositions so far imply the next.

\( p_n \) should be \( Q(x) \).
To prove $\forall x \ P(x) \rightarrow Q(x)$

Let $x$ be an arbitrary element (in the domain of the predicates $P$ and $Q$)

Assume $P(x)$ holds (call this $p_0$)

Derive propositions $p_1, p_2, \ldots, p_n$ where for each $i$, either $p_i$ is an axiom or an already proven proposition in the system, or $(p_0 \land p_1 \land \ldots \land p_{i-1}) \rightarrow p_i$

Usually one or two propositions so far imply the next

$p_n$ should be $Q(x)$.

More generally, to prove $\forall x \ P(x)$, will typically need to use system-specific arguments
Template

To prove $\exists x \ P(x)$
Template

To prove $\exists x \ P(x)$

Demonstrate a particular value of $x$ s.t. $P(x)$ holds
Template

To prove $\exists x \ P(x)$

Demonstrate a particular value of $x$ s.t. $P(x)$ holds

e.g. to prove $\exists x \ P(x) \rightarrow Q(x)$
Template

To prove $\exists x \ P(x)$

Demonstrate a particular value of $x$ s.t. $P(x)$ holds

e.g. to prove $\exists x \ P(x) \rightarrow Q(x)$

find an $x$ s.t. $P(x) \rightarrow Q(x)$ holds
Template

To prove $\exists x \ P(x)$

Demonstrate a particular value of $x$ s.t. $P(x)$ holds

e.g. to prove $\exists x \ P(x) \rightarrow Q(x)$

find an $x$ s.t. $P(x) \rightarrow Q(x)$ holds

if you can find an $x$ s.t. $P(x)$ is false, done!
To prove $\exists x \ P(x)$

Demonstrate a particular value of $x$ s.t. $P(x)$ holds

e.g. to prove $\exists x \ P(x) \rightarrow Q(x)$

find an $x$ s.t. $P(x) \rightarrow Q(x)$ holds

if you can find an $x$ s.t. $P(x)$ is false, done!

or, you can find an $x$ s.t. $Q(x)$ is true, done!
To prove $\exists x \ P(x)$

Demonstrate a particular value of $x$ s.t. $P(x)$ holds

e.g. to prove $\exists x \ P(x) \rightarrow Q(x)$

find an $x$ s.t. $P(x) \rightarrow Q(x)$ holds

if you can find an $x$ s.t. $P(x)$ is false, done!

or, you can find an $x$ s.t. $Q(x)$ is true, done!

(May not be easy to show either, but still may be able to find an $x$ and argue $\neg P(x) \lor Q(x)$)
To prove $\exists x \ P(x)$

- Demonstrate a particular value of $x$ s.t. $P(x)$ holds

  e.g. to prove $\exists x \ P(x) \to Q(x)$

  find an $x$ s.t. $P(x) \to Q(x)$ holds

    if you can find an $x$ s.t. $P(x)$ is false, done!

    or, you can find an $x$ s.t. $Q(x)$ is true, done!

    (May not be easy to show either, but still may be able to
    find an $x$ and argue $\neg P(x) \lor Q(x)$)

    (May not be able to find one, but still show one exists!)
To prove $\exists x \ P(x)$

Demonstrate a particular value of $x$ s.t. $P(x)$ holds

e.g. to prove $\exists x \ P(x) \rightarrow Q(x)$

find an $x$ s.t. $P(x) \rightarrow Q(x)$ holds

if you can find an $x$ s.t. $P(x)$ is false, done!

or, you can find an $x$ s.t. $Q(x)$ is true, done!

(May not be easy to show either, but still may be able to find an $x$ and argue $\neg P(x) \lor Q(x)$)

(May not be able to find one, but still show one exists!)

e.g. to prove $\neg \forall x \ P(x)$
Template

To prove $\exists x \ P(x)$

Demonstrate a particular value of $x$ s.t. $P(x)$ holds

e.g. to prove $\exists x \ P(x) \rightarrow Q(x)$

find an $x$ s.t. $P(x) \rightarrow Q(x)$ holds

if you can find an $x$ s.t. $P(x)$ is false, done!

or, you can find an $x$ s.t. $Q(x)$ is true, done!

(May not be easy to show either, but still may be able to find an $x$ and argue $\neg P(x) \lor Q(x)$)

(May not be able to find one, but still show one exists!)

e.g. to prove $\neg \forall x \ P(x)$

prove $\exists x \ \neg P(x)$ : enough to demonstrate an $x$ s.t. $P(x)$ is false
Rewriting
Rewriting

Sometimes it is helpful to first rewrite the proposition into an equivalent proposition.
Rewriting

Sometimes it is helpful to first rewrite the proposition into an equivalent proposition.

Can change negations using the “mirror”.
Rewriting

- Sometimes it is helpful to first rewrite the proposition into an equivalent proposition.
- Can change negations using the “mirror”.
- Can use contrapositive.
Rewriting

Sometimes it is helpful to first rewrite the proposition into an equivalent proposition.

- Can change negations using the “mirror”
- Can use contrapositive

\[ \forall x \ P(x) \rightarrow Q(x) \equiv \forall x \ \neg Q(x) \rightarrow \neg P(x) \]
Rewriting

- Sometimes it is helpful to first rewrite the proposition into an equivalent proposition
- Can change negations using the "mirror"
- Can use contrapositive

\[ \forall x \ P(x) \rightarrow Q(x) \equiv \forall x \ \neg Q(x) \rightarrow \neg P(x) \]

- e.g. \( \forall x,y \in \mathbb{Z}^+ \ x \cdot y > 25 \rightarrow (x \geq 6) \lor (y \geq 6) \)
Rewriting

- Sometimes it is helpful to first rewrite the proposition into an equivalent proposition.
- Can change negations using the “mirror”:
  \[ \forall x \ P(x) \rightarrow Q(x) \equiv \forall x \ \neg Q(x) \rightarrow \neg P(x) \]
- Can use contrapositive:
  \[ \forall x, y \in \mathbb{Z}^+ \ x \cdot y > 25 \rightarrow (x \geq 6) \lor (y \geq 6) \]
  \[ \forall x, y \in \mathbb{Z}^+ \ (x < 6) \land (y < 6) \rightarrow x \cdot y \leq 25 \]
Rewriting

- Sometimes it is helpful to first rewrite the proposition into an equivalent proposition.
- Can change negations using the “mirror”.
- Can use contrapositive.

\[ \forall x \ P(x) \rightarrow Q(x) \equiv \forall x \ \neg Q(x) \rightarrow \neg P(x) \]

- e.g. \[ \forall x,y \in \mathbb{Z}^+ \ x.y > 25 \rightarrow (x \geq 6) \lor (y \geq 6) \]

\[ \forall x,y \in \mathbb{Z}^+ \ (x < 6) \land (y < 6) \rightarrow x.y \leq 25 \]

- \[ \exists x \ P(x) \rightarrow Q(x) \equiv \exists x \ \neg Q(x) \rightarrow \neg P(x) \]
Examples
Valid proof, when you can execute it. May or may not be possible/true for a given problem.
Valid proof, when you can execute it. May or may not be possible/true for a given problem.

\[ \forall x \ P(x) \]
Examples

∀x P(x)

Let x be an arbitrary element
Show Q(x) → P(x)
Show Q(x) holds
Then P(x) \[\text{Because, } (Q(x) \land (Q(x) \rightarrow P(x))) \rightarrow P(x).\]
Examples

∀x P(x)

Let x be an arbitrary element
Show Q(x) → P(x)
Show Q(x) holds
Then P(x) Because, (Q(x) ∧ (Q(x) → P(x))) → P(x).

At this point, we have reduced the problem of proving P(x) to the problem of proving Q(x).

Valid proof, when you can execute it. May or may not be possible/true for a given problem.
Examples

∀x \, P(x)

Let x be an arbitrary element
Show Q(x) \rightarrow P(x)
Show Q(x) holds
Then P(x) \quad Because, \quad (Q(x) \land (Q(x) \rightarrow P(x))) \rightarrow P(x).

∃x \, \neg Q(x)

Valid proof, when you can execute it. May or may not be possible/true for a given problem.

At this point, we have \text{reduced} the problem of proving P(x) to the problem of proving Q(x)
Examples

 ∀x P(x)

 Let x be an arbitrary element
 Show Q(x) → P(x)
 Show Q(x) holds
 Then P(x)  Because, (Q(x) ∧ (Q(x) → P(x))) → P(x).

 ∃x ¬Q(x)

 Show ∃x P(x) ∨ ¬Q(x)
 Show ∀x ¬P(x)

Valid proof, when you can execute it. May or may not be possible/true for a given problem.

At this point, we have reduced the problem of proving P(x) to the problem of proving Q(x).
Examples

- Let \( x \) be an arbitrary element
  - Show \( Q(x) \rightarrow P(x) \)
  - Show \( Q(x) \) holds
  - Then \( P(x) \) (Because, \( (Q(x) \land (Q(x) \rightarrow P(x))) \rightarrow P(x) \)).

- Show \( \exists x \neg Q(x) \)
  - Show \( \exists x \ P(x) \lor \neg Q(x) \)
  - Show \( \forall x \neg P(x) \)

Valid proof, when you can execute it. May or may not be possible/true for a given problem.

At this point, we have \textbf{reduced} the problem of proving \( P(x) \) to the problem of proving \( Q(x) \).

If we demonstrate an element \( x \) s.t. \( P(x) \lor \neg Q(x) \) holds, now enough to show that for that \( x \), \( P(x) \) holds.
Examples

∀x \ P(x)

Let x be an arbitrary element
Show Q(x) → P(x)
Show Q(x) holds
Then P(x)  Because, \((Q(x) \land (Q(x) \rightarrow P(x)))) \rightarrow P(x)\).

∃x \lnot Q(x)

Show \(\exists x \ P(x) \lor \lnot Q(x)\)
Show \(\forall x \lnot P(x)\)

Show \(\forall x \lnot Q(x)\) (Much more than needed, but OK)

At this point, we have reduced the problem of proving P(x) to the problem of proving Q(x)

If we demonstrate an element x s.t. P(x) \lor \lnot Q(x) holds, now enough to show that for that x, P(x) holds

Valid proof, when you can execute it. May or may not be possible/true for a given problem.
Valid proof, when you can execute it. May or may not be possible/true for a given problem.
Examples

Valid proof, when you can execute it. May or may not be possible/true for a given problem.

\( \exists x \ P(x) \land Q(x) \equiv \forall x \ \neg P(x) \lor \neg Q(x) \)
Valid proof, when you can execute it. May or may not be possible/true for a given problem.

\[ \exists x \ P(x) \land Q(x) \equiv \forall x \ \neg P(x) \lor \neg Q(x) \]
Examples

\[ \exists x \ P(x) \land Q(x) \equiv \forall x \ \neg P(x) \lor \neg Q(x) \]

Show \( \forall x \ \neg Q(x) \)
Examples

Valid proof, when you can execute it. May or may not be possible/true for a given problem.

\[ \exists x \ P(x) \land Q(x) \equiv \forall x \ \neg P(x) \lor \neg Q(x) \]

Show \( \forall x \ \neg Q(x) \)

Show \( \forall x \ \neg P(x) \) (and just for fun, show say, \( \exists x \ P(x) \lor \neg Q(x) \))
Examples

\[ \exists x \ P(x) \land Q(x) \equiv \forall x \ \neg P(x) \lor \neg Q(x) \]

Show \[ \forall x \ \neg Q(x) \]

Show \[ \forall x \ \neg P(x) \] (and just for fun, show say, \[ \exists x \ P(x) \lor \neg Q(x) \])

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

\[ \exists x \ P(x) \land Q(x) \equiv \forall x \ \neg P(x) \lor \neg Q(x) \]

Show \( \forall x \ \neg Q(x) \)

Show \( \forall x \ \neg P(x) \) (and just for fun, show say, \( \exists x \ P(x) \lor \neg Q(x) \))

\( \exists x \ P(x) \)

Show \( P(0) \)

Valid proof, when you can execute it. May or may not be possible/true for a given problem.
Examples

∀x P(x) ∧ Q(x) ≡ ∀x ¬P(x) ∨ ¬Q(x)

Show ∀x ¬Q(x)

Show ∀x ¬P(x) (and just for fun, show say, ∃x P(x) ∨ ¬Q(x))

∃x P(x)

Show P(0)

¬ ∀x P(x) ≡ ∃x ¬P(x)
Examples

$\exists x \ P(x) \land Q(x) \equiv \forall x \ \neg P(x) \lor \neg Q(x)$

Show $\forall x \ \neg Q(x)$

Show $\forall x \ \neg P(x)$ (and just for fun, show say, $\exists x \ P(x) \lor \neg Q(x)$)

$\exists x \ P(x)$

Show $P(0)$

$\neg \forall x \ P(x) \equiv \exists x \ \neg P(x)$

Show $\neg P(0)$
Examples

- \( \exists x \ P(x) \land Q(x) \equiv \forall x \ \neg P(x) \lor \neg Q(x) \)
  
- Show \( \forall x \ \neg Q(x) \)
  
- Show \( \forall x \ \neg P(x) \) (and just for fun, show say, \( \exists x \ P(x) \lor \neg Q(x) \) )
  
- \( \exists x \ P(x) \)
  
- Show \( P(0) \)
  
- \( \neg \forall x \ P(x) \equiv \exists x \ \neg P(x) \)
  
- Show \( \neg P(0) \)

Valid proof, when you can execute it. May or may not be possible/true for a given problem.