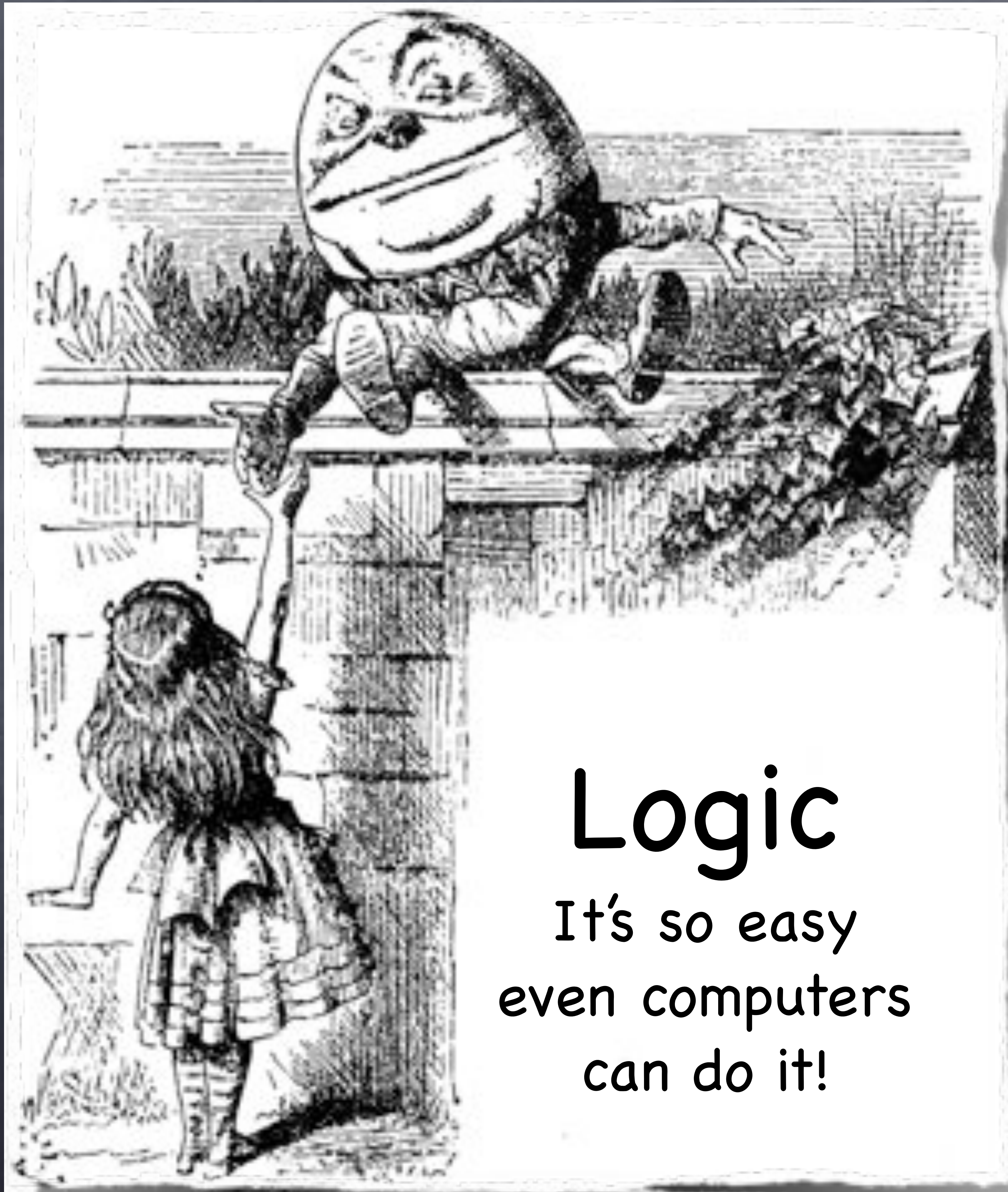
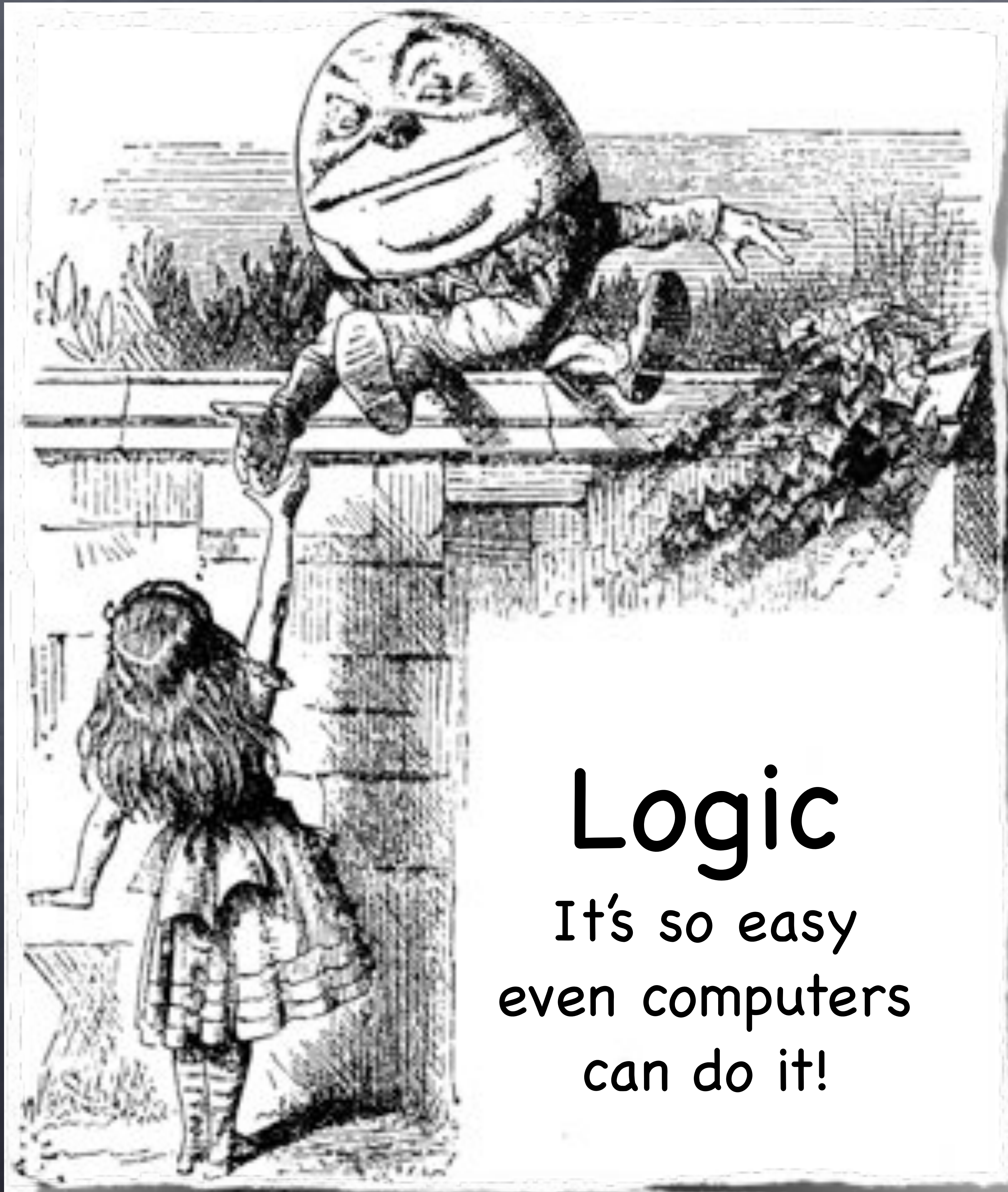


Logic

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

x	Winged(x)	Flies(x)	Pink(x)
Alice	FALSE	FALSE	FALSE
Jabberwock	TRUE	TRUE	FALSE
Flamingo	TRUE	TRUE	TRUE

- Universal quantifier: $\forall x$ Winged(x)
  means Winged(Alice) $\wedge$ Winged(J'wock) $\wedge$ Winged(Flamingo)
- Existential quantifier: $\exists x$ Winged(x)
  means Winged(Alice) $\vee$ Winged(J'wock) $\vee$ Winged(Flamingo)

The Looking Glass

- Reflection changes T & F to F & T (resp.)
  - $\vee$ & $\wedge$ are reflected as $\wedge$ & $\vee$ (resp.)
  - $\forall$ & $\exists$ are reflected as $\exists$ & $\forall$ (resp.)

p, q  $p \wedge q$	$\neg p$, $\neg q$  $\neg p \vee \neg q$
p, q  $p \vee q$	$\neg p$, $\neg q$  $\neg p \wedge \neg q$
$\forall x\ \mathrm{Pred}(x)$	$\exists x\ \neg\mathrm{Pred}(x)$
$\exists x\ \mathrm{Pred}(x)$	$\forall x\ \neg\mathrm{Pred}(x)$

Another example

x	y	Likes(x,y)	x=y
Alice	Alice	TRUE	TRUE
	Jabberwock	FALSE	FALSE
	Flamingo	TRUE	FALSE
Jabberwock	Alice	FALSE	FALSE
	Jabberwock	TRUE	TRUE
	Flamingo	FALSE	FALSE
Flamingo	Alice	FALSE	FALSE
	Jabberwock	FALSE	FALSE
	Flamingo	TRUE	TRUE

- $\forall x,y \ (x=y) \rightarrow Likes(x,y)$
- $\forall x,y \ Likes(x,y) \rightarrow (x=y)$

Another example

x	y	Likes(x,y)	x=y
Alice	Alice	TRUE	TRUE
	Jabberwock	FALSE	FALSE
	Flamingo	TRUE	FALSE
Jabberwock	Alice	FALSE	FALSE
	Jabberwock	TRUE	TRUE
	Flamingo	FALSE	FALSE
Flamingo	Alice	FALSE	FALSE
	Jabberwock	FALSE	FALSE
	Flamingo	TRUE	TRUE

- $\forall x,y \ \ (x=y) \rightarrow Likes(x,y)$
    - Everyone likes themselves (True)
- $\forall x,y \ \ Likes(x,y) \rightarrow (x=y)$

Another example

x	y	Likes(x,y)	x=y
Alice	Alice	TRUE	TRUE
	Jabberwock	FALSE	FALSE
	Flamingo	TRUE	FALSE
Jabberwock	Alice	FALSE	FALSE
	Jabberwock	TRUE	TRUE
	Flamingo	FALSE	FALSE
Flamingo	Alice	FALSE	FALSE
	Jabberwock	FALSE	FALSE
	Flamingo	TRUE	TRUE

- $\forall x,y \;\; (x=y) \rightarrow Likes(x,y)$
  - Everyone likes themselves (True)
- $\forall x,y \;\; Likes(x,y) \rightarrow (x=y)$
  - Everyone likes only themselves, if at all anyone (False)

Question

- Everyone who flies is winged

A. $\forall x \quad Flies(x) \lor Winged(x)$

B. $\forall x \quad Flies(x) \land Winged(x)$

C. $\forall x \quad Flies(x) \rightarrow Winged(x)$

D. $\forall x \quad Flies(x) \leftrightarrow Winged(x)$

E. $\forall x \quad Flies(x) \leftarrow Winged(x)$

Question

- Everyone who flies is winged

  A. $\forall x \;\; Flies(x) \vee Winged(x)$

  B. $\forall x \;\; Flies(x) \wedge Winged(x)$

  C. $\forall x \;\; Flies(x) \rightarrow Winged(x)$

  D. $\forall x \;\; Flies(x) \leftrightarrow Winged(x)$

  E. $\forall x \;\; Flies(x) \leftarrow Winged(x)$

- If anyone flies then he/she/it is winged

Question

- $\forall x\ \underline{P(x) \rightarrow R}$ (R 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. $(\ \exists x\ P(x)\ ) \vee R$

  E. $(\ \forall x\ P(x)\ ) \wedge R$

Moving the Quantifiers

Moving the Quantifiers

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

Moving the Quantifiers

- $\forall x\ \underline{P(x) \rightarrow R}$ (R independent of x)
  If for any x P(x) holds, then R holds
  - $\forall x\ \neg P(x) \vee R \equiv (\forall x\ \neg P(x)) \vee R$
    $\equiv \neg(\exists x\ P(x)) \vee R$
    $\equiv (\exists x\ P(x)) \rightarrow R$

Moving the Quantifiers

- $\forall x\ \underline{P(x) \rightarrow R}$ (R independent of x)
  If for any x P(x) holds, then R holds
  - $\forall x\ \neg P(x) \vee R \equiv (\forall x\ \neg P(x)) \vee R$
    $\equiv \neg(\exists x\ P(x)) \vee R$
    $\equiv (\exists x\ P(x)) \rightarrow R$
- $\exists x\ \underline{P(x) \rightarrow R}$ (R 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

- $\forall x\ \underline{P(x) \rightarrow R}$ (R independent of x)
  If for any x P(x) holds, then R holds
  - $$\begin{aligned} \forall x\ \neg P(x) \vee R &\equiv (\forall x\ \neg P(x)) \vee R \\ &\equiv \neg(\exists x\ P(x)) \vee R \\ &\equiv (\exists x\ P(x)) \rightarrow R \end{aligned}$$
- $\exists x\ \underline{P(x) \rightarrow R}$ (R independent of x)
  Either for some x P(x) is false (and hence $P(x) \rightarrow R$ vacuously true) or else R holds
  - $$\begin{aligned} \exists x\ \neg P(x) \vee R &\equiv (\exists x\ \neg P(x)) \vee R \\ &\equiv \neg(\forall x\ P(x)) \vee R \\ &\equiv (\forall x\ P(x)) \rightarrow R \end{aligned}$$

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

$\forall x\ P(x) \vee R \equiv (\forall x\ P(x)\ ) \vee R$

$\exists x\ P(x) \vee R \equiv (\exists x\ P(x)\ ) \vee R$

$\forall x\ R \rightarrow P(x) \equiv R \rightarrow (\forall x\ P(x))$

$\forall x\ P(x) \rightarrow R \equiv (\exists x\ P(x)) \rightarrow R$

$\exists x\ P(x) \wedge R \equiv (\exists x\ P(x)) \wedge R$

$\forall x\ P(x) \wedge R \equiv (\forall x\ P(x)) \wedge R$

$\exists x\ R \rightarrow P(x) \equiv R \rightarrow (\exists x\ P(x))$

$\exists x\ P(x) \rightarrow R \equiv (\forall x\ P(x)) \rightarrow R$

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

$\forall x\ P(x) \vee R \equiv (\forall x\ P(x)) \vee R$	$\exists x\ P(x) \wedge R \equiv (\exists x\ P(x)) \wedge R$
$\exists x\ P(x) \vee R \equiv (\exists x\ P(x)) \vee R$	$\forall x\ P(x) \wedge R \equiv (\forall x\ P(x)) \wedge R$
$\forall x\ R \rightarrow P(x) \equiv R \rightarrow (\forall x\ P(x))$	$\exists x\ R \rightarrow P(x) \equiv R \rightarrow (\exists x\ P(x))$
$\forall x\ P(x) \rightarrow R \equiv (\exists x\ P(x)) \rightarrow R$	$\exists x\ P(x) \rightarrow R \equiv (\forall x\ P(x)) \rightarrow R$

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

$\forall x\ P(x) \lor R \equiv (\forall x\ P(x)) \lor R$

$\exists x\ P(x) \lor R \equiv (\exists x\ P(x)) \lor R$

$\forall x\ R \to P(x) \equiv R \to (\forall x\ P(x))$

$\forall x\ P(x) \to R \equiv (\exists x\ P(x)) \to R$

$\exists x\ P(x) \land R \equiv (\exists x\ P(x)) \land R$

$\forall x\ P(x) \land R \equiv (\forall x\ P(x)) \land R$

$\exists x\ R \to P(x) \equiv R \to (\exists x\ P(x))$

$\exists x\ P(x) \to R \equiv (\forall x\ P(x)) \to R$

not the mirror!

- $(\forall x\ P(x)) \land (\forall x\ Q(x)) \equiv \forall x\ (P(x) \land Q(x))$

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

$\forall x\ P(x) \vee R \equiv (\forall x\ P(x)\ ) \vee R$

$\exists x\ P(x) \vee R \equiv (\exists x\ P(x)\ ) \vee R$

$\forall x\ R \rightarrow P(x) \equiv R \rightarrow (\forall x\ P(x))$

$\forall x\ P(x) \rightarrow R \equiv (\exists x\ P(x)) \rightarrow R$

$\exists x\ P(x) \wedge R \equiv (\exists x\ P(x)) \wedge R$

$\forall x\ P(x) \wedge R \equiv (\forall x\ P(x)) \wedge R$

$\exists x\ R \rightarrow P(x) \equiv R \rightarrow (\exists x\ P(x))$

$\exists x\ P(x) \rightarrow R \equiv (\forall x\ P(x)) \rightarrow R$

not the mirror!

- $(\forall x\ P(x)) \wedge (\forall x\ Q(x)) \equiv \forall x\ (P(x) \wedge Q(x))$
  - But $(\forall x\ P(x)) \vee (\forall x\ Q(x)) \not\equiv \forall x\ (P(x) \vee Q(x))$

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

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

$$\exists x\ P(x) \land R \equiv (\exists x\ P(x)) \land R$$
$$\forall x\ P(x) \land R \equiv (\forall x\ P(x)) \land R$$
$$\exists x\ R \rightarrow P(x) \equiv R \rightarrow (\exists x\ P(x))$$
$$\exists x\ P(x) \rightarrow R \equiv (\forall x\ P(x)) \rightarrow R$$

not the mirror!

- $(\forall x\ P(x)) \land (\forall x\ Q(x)) \equiv \forall x\ (P(x) \land Q(x))$
  - 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

- $\forall x\ \forall y\ P(x,y) \equiv \forall y\ \forall x\ P(x,y)$
- $\exists x\ \exists y\ P(x,y) \equiv \exists y\ \exists x\ P(x,y)$
- When R is independent of x

$\forall x\ P(x) \lor R \equiv (\forall x\ P(x)) \lor R$

$\exists x\ P(x) \lor R \equiv (\exists x\ P(x)) \lor R$

$\forall x\ R \rightarrow P(x) \equiv R \rightarrow (\forall x\ P(x))$

$\forall x\ P(x) \rightarrow R \equiv (\exists x\ P(x)) \rightarrow R$

$\exists x\ P(x) \land R \equiv (\exists x\ P(x)) \land R$

$\forall x\ P(x) \land R \equiv (\forall x\ P(x)) \land R$

$\exists x\ R \rightarrow P(x) \equiv R \rightarrow (\exists x\ P(x))$

$\exists x\ P(x) \rightarrow R \equiv (\forall x\ P(x)) \rightarrow R$

not the mirror!

- $(\forall x\ P(x)) \land (\forall x\ Q(x)) \equiv \forall x\ (P(x) \land Q(x))$
  - But $(\forall x\ P(x)) \lor (\forall x\ Q(x)) \not\equiv \forall x\ (P(x) \lor Q(x))$
- $(\exists x\ P(x)) \lor (\exists x\ Q(x)) \equiv \exists x\ (P(x) \lor Q(x))$
  - But $(\exists x\ P(x)) \land (\exists x\ Q(x)) \not\equiv \exists x\ (P(x) \land Q(x))$

Question

- $\forall x,y \ \ Pink(x) \rightarrow Flies(y)$

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

- $\forall x \ \ \underline{\forall y \ \ P(x) \rightarrow Q(y)}$
  - $\forall x \ \ \underline{P(x) \rightarrow (\forall y \ Q(y))}$

Answer

- $\forall x \ \ \underline{\forall y \ \ P(x) \rightarrow Q(y)}$
  - $\forall x \ \ \underline{P(x) \rightarrow (\forall y \ Q(y))}$
- $\forall x \ \ P(x) \rightarrow R \equiv (\ \exists x \ P(x)\ ) \rightarrow R$

Answer

- $\forall x \quad \underline{\forall y \quad P(x) \rightarrow Q(y)}$
  - $\forall x \quad \underline{P(x) \rightarrow (\forall y \; Q(y))}$
- $\forall x \quad P(x) \rightarrow R \equiv (\exists x \; P(x)) \rightarrow R$
- $\underline{\forall x,y \quad P(x) \rightarrow Q(y)} \equiv \underline{(\exists x \; P(x)) \rightarrow (\forall y \; Q(y))}$

Example

Example

- "If someone flies, everyone flies" is the same as which one(s)?

1. $(\exists x \; Flies(x)) \rightarrow (\forall x \; Flies(x))$
2. $\forall x,y \; Flies(x) \leftrightarrow Flies(y)$
3. $\exists x \; \forall y \; Flies(x) \leftrightarrow Flies(y)$
4. $\exists x \; \forall y \; Flies(x) \rightarrow Flies(y)$

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. $\exists x\ \forall y \text{ Flies}(x) \rightarrow \text{Flies}(y)$

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 <u>propositions</u>
  - 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 <u>propositions</u>
  - Often called Theorems, Lemmas, Claims, …
- Propositions use various predicates already specified as <u>Definitions</u>
- e.g. All positive even numbers are larger than 1

What are we proving?

- We are proving <u>propositions</u>
  - Often called Theorems, Lemmas, Claims, ...
- Propositions use various predicates already specified as <u>Definitions</u>
- e.g. All positive even numbers are larger than 1
  - $\forall x \in \mathbb{Z}\ (\ \underline{\text{Positive}}(x) \wedge \underline{\text{Even}}(x)\ ) \rightarrow \underline{\text{Greater}}(x,1)$

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
  - $\forall x \in \mathbb{Z}$ (Positive(x) $\wedge$ Even(x)) $\rightarrow$ 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
  - $\forall x \in \mathbb{Z}$ (Positive(x) $\wedge$ Even(x)) $\rightarrow$ 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
  - $\forall x \in \mathbb{Z}$ (Positive(x) $\wedge$ Even(x)) $\rightarrow$ 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

Example

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

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!

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. $x=2y+1$

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!
- <u>Definition</u>: 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"

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

"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. $x=2y+1$
  - $\mathrm{Odd}(x) \equiv \exists y \in \mathbb{Z}\ (x = 2y+1)$

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

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

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

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

- Proposition: If x is an odd integer, so is x^2
    - $\forall x \in \mathbb{Z} \ \ \mathrm{Odd}(x) \rightarrow \mathrm{Odd}(x^2)$

Example

Example

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

Example

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

Example

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

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)
  - Let x be an arbitrary element of $\mathbb{Z}$

Example

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

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

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)
  - Let x be an arbitrary element of $\mathbb{Z}$
  - Suppose Odd(x). Then, we need to show 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: 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)
  - Let x be an arbitrary element of $\mathbb{Z}$
  - Suppose Odd(x). Then, we need to show 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.
  - Hence, $\exists w \in \mathbb{Z}\ x^2 = 2w+1$

Example

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

Template

Template

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

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)

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)

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)
  - 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 $(p_0 \wedge p_1 \wedge \ldots \wedge p_{i-1}) \rightarrow p_i$

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)
  - 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 $(p_0 \wedge p_1 \wedge \ldots \wedge p_{i-1}) \rightarrow p_i$
    - Usually one or two propositions so far imply the next

Template

- To prove $\forall x\, P(x) \to Q(x)$
  - 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 $(p_0 \wedge p_1 \wedge \ldots \wedge p_{i-1}) \to p_i$
    - Usually one or two propositions so far imply the next
  - p_n should be $Q(x)$.

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)
  - 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 $(p_0 \wedge p_1 \wedge \ldots \wedge p_{i-1}) \rightarrow p_i$
    - 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

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!

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!

Template

- To prove $\exists x\ P(x)$
  - Demonstrate a particular value of x s.t. $P(x)$ holds
- e.g. to prove $\exists x\ P(x) \to Q(x)$
  - 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 $\neg P(x) \vee Q(x)$)

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
    - 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 $\neg P(x) \vee Q(x)$)
  - (May not be able to find one, but still show one exists!)

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 $\neg P(x) \vee Q(x)$)
  - (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 $\neg P(x) \vee Q(x)$)
  - (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 <u>equivalent</u> proposition
  - Can change negations using the "mirror"

Rewriting

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

Rewriting

- Sometimes it is helpful to first rewrite the proposition into an <u>equivalent</u> 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 <u>equivalent</u> 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. $\forall x,y \in \mathbb{Z}^+\ \ x.y > 25 \rightarrow (x \geq 6) \vee (y \geq 6)$

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. $\forall x,y \in \mathbb{Z}^+\ \ x.y > 25 \rightarrow (x \geq 6) \lor (y \geq 6)$
        - $\forall x,y \in \mathbb{Z}^+\ \ (x<6) \land (y<6) \rightarrow x.y \leq 25$

Rewriting

- Sometimes it is helpful to first rewrite the proposition into an <u>equivalent</u> 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. $\forall x,y \in \mathbb{Z}^+\ \ x.y > 25 \rightarrow (x \geq 6) \vee (y \geq 6)$
        - $\forall x,y \in \mathbb{Z}^+\ \ (x<6) \wedge (y<6) \rightarrow x.y \leq 25$
    - $\exists x\ P(x) \rightarrow Q(x) \equiv \exists x\ \neg Q(x) \rightarrow \neg P(x)$

Examples

Examples

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.

- $\forall x\ P(x)$

Examples

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

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

Examples

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

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

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

Examples

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

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

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

- $\exists x\, \neg Q(x)$

Examples

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

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

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

- $\exists x\ \neg Q(x)$
  - 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.

Examples

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

At this point, we have **<u>reduced</u>** the problem of proving P(x) to the problem of proving Q(x)

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

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

Examples

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

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

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

- $\exists x\ \neg Q(x)$
  - Show $\exists x\ P(x) \vee \neg Q(x)$
    Show $\forall x\ \neg P(x)$
  - Show $\forall x\ \neg Q(x)$ (Much more than needed, but OK)

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

Examples

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.

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

Examples

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

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

Rewrite

Examples

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

- $\nexists x\ P(x) \wedge Q(x) \equiv \forall x\ \neg P(x) \vee \neg Q(x)$

  Rewrite

  - 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.

- $\nexists x\ P(x) \wedge Q(x) \equiv \forall x\ \neg P(x) \vee \neg Q(x)$

Rewrite

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

Examples

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

- $\nexists x\ P(x) \wedge Q(x) \equiv \forall x\ \neg P(x) \vee \neg Q(x)$

  Rewrite

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

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

Examples

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

  Rewrite

  - 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 $P(0)$

Examples

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

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

  Rewrite

  - 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 $P(0)$
- $\neg\ \forall x\ P(x) \equiv \exists x\ \neg P(x)$

Examples

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

- $\nexists x\ P(x) \wedge Q(x) \equiv \forall x\ \neg P(x) \vee \neg Q(x)$

Rewrite

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

Examples

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

- $\nexists x\ P(x) \wedge Q(x) \equiv \forall x\ \neg P(x) \vee \neg Q(x)$

  Rewrite

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

  Rewrite

  - Show $\neg P(0)$