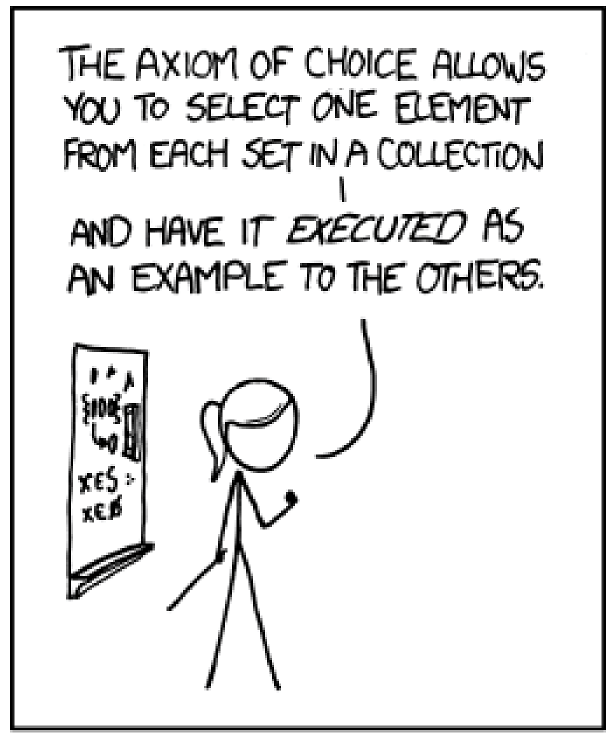
CSE 311: Foundations of Computing

Lecture 8: Predicate Logic Proofs



MY MATH TEACHER WAS A BIG BELIEVER IN PROOF BY INTIMIDATION.

Last class: Propositional Inference Rules

Two inference rules per binary connective, one to eliminate it and one to introduce it

Elim ∧

$$\frac{A \wedge B}{\therefore A, B}$$

Intro ∧

$$\frac{A \,;\, B}{\therefore A \wedge B}$$

Elim ∨

$$\frac{A \vee B \,;\, \neg A}{\therefore B}$$

Intro ∨

$$\frac{A}{\therefore A \vee B,\ B \vee A}$$

Modus Ponens

$$\frac{A \,;\, A \rightarrow B}{\therefore B}$$

Direct Proof Rule

$$\frac{A \Rightarrow B}{\therefore A \rightarrow B}$$

Not like other rules

Last class: Example

Prove: $((p \to q) \land (q \to r)) \to (p \to r)$

1.1.	$(p \to q) \land (q \to r)$	Assumption
1.2.	$p \to q$	$\land$ Elim: 1.1
1.3.	$q \to r$	$\land$ Elim: 1.1
1.4.1.	p	Assumption
1.4.2.	q	MP: 1.2, 1.4.1
1.4.3.	r	MP: 1.3, 1.4.2
1.4.	$p \to r$	Direct Proof Rule
1.	$((p \to q) \land (q \to r)) \to (p \to r)$	Direct Proof Rule

Inference Rules for Quantifiers: First look

Intro ∃

$$\frac{P(c) \text{ for some } c}{\therefore \quad \exists x\, P(x)}$$

Elim ∀

$$\frac{\forall x\, P(x)}{\therefore \; P(a) \textbf{ for any } a}$$

Intro ∀

$$\frac{\text{“}\textbf{Let } a \textbf{ be arbitrary}^{*}\text{”}\ldots P(a)}{\therefore \quad \forall x\, P(x)}$$

* in the domain of P

Elim ∃

$$\frac{\exists x\, P(x)}{\therefore \; P(c) \textbf{ for some } \textbf{\textit{special}}^{**}\ c}$$

** By special, we mean that c is a name for a value where P(c) is true. We can't use anything else about that value, so c has to be a NEW name!

Predicate Logic Proofs

- Can use
  - Predicate logic inference rules

    whole formulas only
  - Predicate logic equivalences (De Morgan's)

    even on subformulas
  - Propositional logic inference rules

    whole formulas only
  - Propositional logic equivalences

    even on subformulas

My First Predicate Logic Proof

Intro $\exists$ $\dfrac{\text{P(c) for some c}}{\therefore \quad \exists x\, P(x)}$

Elim $\forall$ $\dfrac{\forall x\, P(x)}{\therefore \quad \text{P(a) for any a}}$

Prove $\forall x\, P(x) \to \exists x\, P(x)$

5. $\forall x\, P(x) \to \exists x\, P(x)$?

The main connective is implication so Direct Proof Rule seems good

My First Predicate Logic Proof

Intro ∃ $\dfrac{P(c) \text{ for some } c}{\therefore \ \exists x\, P(x)}$

Elim ∀ $\dfrac{\forall x\, P(x)}{\therefore \ P(a) \text{ for any } a}$

Prove $\forall x\, P(x) \rightarrow \exists x\, P(x)$

1.1. $\forall x\, P(x)$ Assumption

We need an ∃ we don't have
so "intro ∃" rule makes sense

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

1. $\forall x\, P(x) \rightarrow \exists x\, P(x)$ Direct Proof Rule

My First Predicate Logic Proof

Intro ∃ $\dfrac{P(c) \text{ for some } c}{\therefore\ \exists x\, P(x)}$

Elim ∀ $\dfrac{\forall x\, P(x)}{\therefore\ P(a) \text{ for any } a}$

Prove $\forall x\, P(x) \rightarrow \exists x\, P(x)$

1.1. $\forall x\, P(x)$ Assumption

We need an ∃ we don't have
so "intro ∃" rule makes sense

1.5. $\exists x\, P(x)$ Intro ∃: ?

That requires P(c)
for some c.

1. $\forall x\, P(x) \rightarrow \exists x\, P(x)$ Direct Proof Rule

My First Predicate Logic Proof

Intro ∃ $\dfrac{P(c) \text{ for some } c}{\therefore\ \exists x\, P(x)}$

Elim ∀ $\dfrac{\forall x\, P(x)}{\therefore\ P(a) \text{ for any } a}$

Prove $\forall x\, P(x) \rightarrow \exists x\, P(x)$

1.1. $\forall x\, P(x)$ Assumption

1.2 $P(a)$ Elim ∀: 1.1

We could have picked any name or domain expression here.

1.5. $\exists x\, P(x)$ Intro ∃: ?

That requires P(c) for some c.

1. $\forall x\, P(x) \rightarrow \exists x\, P(x)$ Direct Proof Rule

My First Predicate Logic Proof

Intro ∃ $\dfrac{P(c) \text{ for some } c}{\therefore \quad \exists x\, P(x)}$

Elim ∀ $\dfrac{\forall x\, P(x)}{\therefore\ P(a) \text{ for any } a}$

Prove $\forall x\, P(x) \rightarrow \exists x\, P(x)$

No holes. Just need to clean up.

1.1. $\forall x\, P(x)$ Assumption

1.2 $P(a)$ Elim ∀: 1.1

1.5. $\exists x\, P(x)$ Intro ∃: 1.2

1. $\forall x\, P(x) \rightarrow \exists x\, P(x)$ Direct Proof Rule

My First Predicate Logic Proof

Intro $\exists$: $\dfrac{P(c) \text{ for some } c}{\therefore\ \exists x\, P(x)}$

Elim $\forall$: $\dfrac{\forall x\, P(x)}{\therefore\ P(a) \text{ for any } a}$

Prove $\forall x\ P(x) \rightarrow \exists x\ P(x)$

1.1.	$\forall x\, P(x)$	Assumption
1.2	$P(a)$	Elim $\forall$: 1.1
1.3.	$\exists x\, P(x)$	Intro $\exists$: 1.2
1.	$\forall x\, P(x) \rightarrow \exists x\, P(x)$	Direct Proof Rule

Working forwards as well as backwards:
In applying "Intro $\exists$" rule we didn't know what expression we might be able to prove P(c) for, so we worked forwards to figure out what might work.

Predicate Logic Proofs with more content

- In propositional logic we could just write down other propositional logic statements as "givens"

- Here, we also want to be able to use domain knowledge so proofs are about something specific
- Example:

Domain of Discourse
Integers

- Given the basic properties of arithmetic on integers, define:

Predicate Definitions
$\text{Even}(x) \equiv \exists y\ (x = 2 \cdot y)$
$\text{Odd}(x) \equiv \exists y\ (x = 2 \cdot y + 1)$

A Not so Odd Example

Domain of Discourse
Integers

Predicate Definitions
$\text{Even}(x) \equiv \exists y\ (x = 2 \cdot y)$
$\text{Odd}(x) \equiv \exists y\ (x = 2 \cdot y + 1)$

Prove “There is an even number”

Formally: prove $\exists x\ \text{Even}(x)$

A Not so Odd Example

Domain of Discourse
Integers

Predicate Definitions
$\text{Even}(x) \equiv \exists y\ (x = 2 \cdot y)$
$\text{Odd}(x) \equiv \exists y\ (x = 2 \cdot y + 1)$

Prove "There is an even number"

Formally: prove $\exists x\ \text{Even}(x)$

1.	$\mathbf{2 = 2 \cdot 1}$	**Arithmetic**
2.	$\exists y\ (\mathbf{2} = \mathbf{2} \cdot y)$	**Intro** $\exists$**: 1**
3.	$\text{Even}(\mathbf{2})$	**Definition of** Even**: 2**
4.	$\exists x\ \text{Even}(x)$	**Intro** $\exists$**: 3**

A Prime Example

Domain of Discourse
Integers

Predicate Definitions
$\text{Even}(x) \equiv \exists y\ (x = 2 \cdot y)$ $\text{Odd}(x) \equiv \exists y\ (x = 2 \cdot y + 1)$ $\text{Prime}(x) \equiv$ "$x > 1$ and $x \neq a \cdot b$ for all integers a, b with $1 < a < x$"

Prove "There is an even prime number"

A Prime Example

Domain of Discourse
Integers

Predicate Definitions
$\text{Even}(x) \equiv \exists y\ (x = 2 \cdot y)$
$\text{Odd}(x) \equiv \exists y\ (x = 2 \cdot y + 1)$
$\text{Prime}(x) \equiv$ "$x > 1$ and $x \neq a \cdot b$ for all integers a, b with $1 < a < x$"

Prove "There is an even prime number"

Formally: prove $\exists x\ (\text{Even}(x) \wedge \text{Prime}(x))$

1.	$\mathbf{2 = 2 \cdot 1}$	**Arithmetic**
2.	$\text{Prime}(\mathbf{2})$ *	**Property of integers**

*** Later we will further break down** "Prime" **using quantifiers to prove statements like this**

A Prime Example

Domain of Discourse
Integers

Predicate Definitions
$\text{Even}(x) \equiv \exists y\ (x = 2\cdot y)$
$\text{Odd}(x) \equiv \exists y\ (x = 2\cdot y + 1)$
$\text{Prime}(x) \equiv$ "x > 1 and $x \neq a\cdot b$ for all integers a, b with $1<a<x$"

Prove "There is an even prime number"

Formally: prove $\exists x\ (\text{Even}(x) \land \text{Prime}(x))$

1.	$2 = 2\cdot 1$	**Arithmetic**
2.	$\text{Prime}(2)$*	**Property of integers**
3.	$\exists y\ (2 = 2\cdot y)$	**Intro** $\exists$: **1**
4.	$\text{Even}(2)$	**Defn of** Even: **3**
5.	$\text{Even}(2) \land \text{Prime}(2))$	**Intro** $\land$: **2, 4**
6.	$\exists x\ (\text{Even}(x) \land \text{Prime}(x))$	**Intro** $\exists$: **5**

* **Later we will further break down** "Prime" **using quantifiers to prove statements like this**

Inference Rules for Quantifiers: First look

Intro $\exists$

$$\frac{P(c) \text{ for some } c}{\therefore \quad \exists x\, P(x)}$$

Elim $\forall$

$$\frac{\forall x\, P(x)}{\therefore \quad P(a) \textbf{ for any } a}$$

Intro $\forall$

$$\frac{\text{“}\textbf{Let } a \textbf{ be arbitrary}^{*}\text{”} \ldots P(a)}{\therefore \quad \forall x\, P(x)}$$

* in the domain of P

Elim $\exists$

$$\frac{\exists x\, P(x)}{\therefore\ P(c) \textbf{ for some } \textbf{\textit{special}}^{**}\ c}$$

** By special, we mean that c is a name for a value where P(c) is true. We can’t use anything else about that value, so c has to be a NEW name!

Even and Odd

Even(x) $\equiv \exists y\ (x=2y)$
Odd(x) $\equiv \exists y\ (x=2y+1)$
Domain: Integers

Intro $\forall$	Elim $\exists$
"**Let** a **be arbitrary***"...P(a) / $\therefore\ \forall x\, P(x)$	$\exists x\, P(x)$ / $\therefore$ P(c) **for some *special*** ** c

Prove: "The square of every even number is even."

Formal proof of: $\forall x\,(\text{Even}(x) \rightarrow \text{Even}(x^2))$

3. $\forall x\,(\text{Even}(x)\rightarrow\text{Even}(x^2))$?

Even and Odd

$\text{Even}(x) \equiv \exists y\ (x=2y)$
$\text{Odd}(x) \equiv \exists y\ (x=2y+1)$
Domain: Integers

Intro $\forall$	Elim $\exists$
$\dfrac{\text{“Let } a \text{ be arbitrary*”} \ldots P(a)}{\therefore \quad \forall x\, P(x)}$	$\dfrac{\exists x\, P(x)}{\therefore P(c) \text{ for some } \textit{special}\text{** } c}$

Prove: “The square of every even number is even.”

Formal proof of: $\forall x\,(\text{Even}(x) \rightarrow \text{Even}(x^2))$

1. Let **a** be an arbitrary integer

2. $\text{Even}(\mathbf{a}) \rightarrow \text{Even}(\mathbf{a}^2)$?
3. $\forall x\,(\text{Even}(x) \rightarrow \text{Even}(x^2))$ Intro $\forall$: 1,2

Even(x) $\equiv \exists y\ (x=2y)$
Odd(x) $\equiv \exists y\ (x=2y+1)$
Domain: Integers

Even and Odd

Intro $\forall$: $\dfrac{\text{"Let } a \text{ be arbitrary*"} \ldots P(a)}{\therefore\ \forall x\, P(x)}$	Elim $\exists$: $\dfrac{\exists x\, P(x)}{\therefore\ P(c) \text{ for some special** } c}$

Prove: "The square of every even number is even."

Formal proof of: $\forall x\,(\text{Even}(x) \rightarrow \text{Even}(x^2))$

1. Let **a** be an arbitrary integer
   - 2.1 Even(**a**) — Assumption
   - **2.6** Even($\mathbf{a}^2$) — ?
2. Even(**a**)$\rightarrow$Even($\mathbf{a}^2$) — Direct proof rule
3. $\forall x\,(\text{Even}(x)\rightarrow\text{Even}(x^2))$ — Intro $\forall$: 1,2

Even and Odd

$\text{Even}(x) \equiv \exists y\ (x=2y)$
$\text{Odd}(x) \equiv \exists y\ (x=2y+1)$
Domain: Integers

Intro ∀: $\dfrac{\text{“Let } a \text{ be arbitrary*”} \ldots P(a)}{\therefore\ \forall x\, P(x)}$

Elim ∃: $\dfrac{\exists x\, P(x)}{\therefore\ P(c) \text{ for some } \textit{special}^{**}\ c}$

Prove: “The square of every even number is even.”

Formal proof of: $\forall x\,(\text{Even}(x) \rightarrow \text{Even}(x^2))$

1. Let **a** be an arbitrary integer

2.1	$\text{Even}(\mathbf{a})$	Assumption
2.2	$\exists y\,(\mathbf{a} = 2y)$	Definition of Even
2.5	$\exists y\,(\mathbf{a}^2 = 2y)$	?
2.6	$\text{Even}(\mathbf{a}^2)$	Definition of Even

2. $\text{Even}(\mathbf{a}) \rightarrow \text{Even}(\mathbf{a}^2)$ — Direct proof rule
3. $\forall x\,(\text{Even}(x) \rightarrow \text{Even}(x^2))$ — Intro ∀: 1,2

Even(x) ≡ ∃y (x=2y)
Odd(x) ≡ ∃y (x=2y+1)
Domain: Integers

Even and Odd

Intro ∀	$\dfrac{\text{“Let } a \text{ be arbitrary*”}\ldots P(a)}{\therefore\ \forall x\, P(x)}$	
Elim ∃	$\dfrac{\exists x\, P(x)}{\therefore\ P(c) \text{ for some } \textit{special**}\ c}$	

Prove: “The square of every even number is even.”

Formal proof of: $\forall x\,(\text{Even}(x) \rightarrow \text{Even}(x^2))$

1. Let **a** be an arbitrary integer
    - 2.1 Even(**a**) — Assumption
    - 2.2 $\exists y\,(a = 2y)$ — Definition of Even
    - 2.5 $\exists y\,(a^2 = 2y)$ — Intro ∃ rule: ?
    - 2.6 Even(a^2) — Definition of Even
2. Even(**a**)→Even(a^2) — Direct proof rule
3. $\forall x\,(\text{Even}(x) \rightarrow \text{Even}(x^2))$ — Intro ∀: 1,2

Need $a^2 = 2c$ for some c

Even and Odd

Even(x) $\equiv \exists y\ (x=2y)$
Odd(x) $\equiv \exists y\ (x=2y+1)$
Domain: Integers

Intro $\forall$		Elim $\exists$	
	"Let a be arbitrary*"...P(a) / $\therefore\ \forall x\ P(x)$		$\exists x\ P(x)$ / $\therefore$ P(c) for some *special*** c

Prove: "The square of every even number is even."

Formal proof of: $\forall x\ (\text{Even}(x) \rightarrow \text{Even}(x^2))$

1. Let **a** be an arbitrary integer
    - 2.1 Even(**a**) — Assumption
    - 2.2 $\exists y\ (\mathbf{a} = 2y)$ — Definition of Even
    - 2.3 $\mathbf{a} = 2\mathbf{b}$ — Elim $\exists$: **b** special depends on **a**
    - 2.5 $\exists y\ (\mathbf{a}^2 = 2y)$ — Intro $\exists$ rule: ?
    - 2.6 Even($\mathbf{a}^2$) — Definition of Even
2. Even(**a**)$\rightarrow$Even($\mathbf{a}^2$) — Direct proof rule
3. $\forall x\ (\text{Even}(x)\rightarrow\text{Even}(x^2))$ — Intro $\forall$: 1,2

Need $\mathbf{a}^2 = 2\mathbf{c}$ for some **c**

Even(x) ≡ $\exists y\ (x=2y)$
Odd(x) ≡ $\exists y\ (x=2y+1)$
Domain: Integers

Even and Odd

Intro ∀	"Let a be arbitrary*"...P(a) ∴ $\forall x\, P(x)$	Elim ∃	$\exists x\, P(x)$ ∴ P(c) for some *special*** c

Prove: "The square of every even number is even."

Formal proof of: $\forall x\, (\text{Even}(x) \rightarrow \text{Even}(x^2))$

1. Let **a** be an arbitrary integer

2.1	Even(**a**)	Assumption
2.2	$\exists y\, (\mathbf{a} = 2y)$	Definition of Even
2.3	$\mathbf{a} = 2\mathbf{b}$	Elim ∃: **b** special depends on **a**
2.4	$\mathbf{a}^2 = 4\mathbf{b}^2 = 2(2\mathbf{b}^2)$	Algebra
2.5	$\exists y\, (\mathbf{a}^2 = 2y)$	Intro ∃ rule
2.6	Even($\mathbf{a}^2$)	Definition of Even

Used $\mathbf{a}^2 = 2c$ for $c=2\mathbf{b}^2$

2. Even(**a**)→Even($\mathbf{a}^2$) Direct proof rule
3. $\forall x\, (\text{Even}(x)\rightarrow\text{Even}(x^2))$ Intro ∀: 1,2

Why did we need to say that b depends on a?

There are extra conditions on using these rules:

Intro $\forall$ — "Let a be arbitrary*"...P(a) $\therefore$ $\forall x\, P(x)$

* in the domain of P

Elim $\exists$ — $\exists x\, P(x)$ $\therefore$ P(c) for some *special*** c

** c has to be a NEW name.

Over integer domain: $\forall x\, \exists y\, (y \geq x)$ **is True but** $\exists y \forall x\, (y \geq x)$ **is False**

BAD "PROOF"

1. $\forall x\, \exists y\, (y \geq x)$ — Given
2. Let **a** be an arbitrary integer
3. $\exists y\, (y \geq \mathbf{a})$ — Elim $\forall$: **1**
4. $\mathbf{b} \geq \mathbf{a}$ — Elim $\exists$: **b** special depends on **a**
5. $\forall x\, (\mathbf{b} \geq x)$ — Intro $\forall$: **2,4**
6. $\exists y \forall x\, (y \geq x)$ — Intro $\exists$: **5**

Why did we need to say that b depends on a?

There are extra conditions on using these rules:

Intro $\forall$: $\dfrac{\text{“Let } a \text{ be arbitrary*”} \ldots P(a)}{\therefore \quad \forall x\, P(x)}$

* in the domain of P

Elim $\exists$: $\dfrac{\exists x\, P(x)}{\therefore P(c) \text{ for some } \textit{special}^{**}\ c}$

** c has to be a NEW name.

Over integer domain: $\forall x\, \exists y\, (y \geq x)$ **is True but** $\exists y \forall x\, (y \geq x)$ **is False**

BAD “PROOF”

1. $\forall x\, \exists y\, (y \geq x)$ — Given
2. Let **a** be an arbitrary integer
3. $\exists y\, (y \geq \mathbf{a})$ — Elim $\forall$: **1**
4. $\mathbf{b} \geq \mathbf{a}$ — Elim $\exists$: **b** special depends on **a**
5. $\forall x\, (\mathbf{b} \geq x)$ — Intro $\forall$: **2,4**
6. $\exists y \forall x\, (y \geq x)$ — Intro $\exists$: **5**

Can’t get rid of a since another name in the same line, b, depends on it!

Why did we need to say that b depends on a?

There are extra conditions on using these rules:

Intro $\forall$: $\dfrac{\text{"Let } a \text{ be arbitrary*"} \ldots P(a)}{\therefore\ \forall x\, P(x)}$

* in the domain of P. No other name in P depends on a

Elim $\exists$: $\dfrac{\exists x\, P(x)}{\therefore\ P(c) \text{ for some } \textit{special}^{**}\ c}$

** c is a NEW name. List all dependencies for c.

Over integer domain: $\forall x\, \exists y\, (y \geq x)$ is True but $\exists y \forall x\, (y \geq x)$ is False

BAD "PROOF"

1. $\forall x\, \exists y\, (y \geq x)$ Given
2. Let a be an arbitrary integer
3. $\exists y\, (y \geq a)$ Elim $\forall$: 1
4. $b \geq a$ Elim $\exists$: b special depends on a
5. ~~$\forall x\, (b \geq x)$ Intro $\forall$: 2,4~~
6. $\exists y \forall x\, (y \geq x)$ Intro $\exists$: 5

Can't get rid of a since another name in the same line, b, depends on it!

Inference Rules for Quantifiers: Full version

Intro ∃

$$\frac{P(c) \text{ for some } c}{\therefore \quad \exists x\, P(x)}$$

Elim ∀

$$\frac{\forall x\, P(x)}{\therefore \quad P(a) \textbf{ for any } a}$$

Intro ∀

$$\frac{\text{“}\textbf{Let } a \textbf{ be arbitrary}^{*}\text{”} \ldots P(a)}{\therefore \quad \forall x\, P(x)}$$

* in the domain of P. No other name in P depends on a

Elim ∃

$$\frac{\exists x\, P(x)}{\therefore\ P(c) \textbf{ for some } \textbf{\textit{special}}^{**}\ c}$$

** c is a NEW name.
List all dependencies for c.

English Proofs

- We often write proofs in English rather than as fully formal proofs
  - They are more natural to read

- English proofs follow the structure of the corresponding formal proofs
  - Formal proof methods help to understand how proofs really work in English…

    … and give clues for how to produce them.

An English Proof

Predicate Definitions

Even(x) ≡ ∃y (x = 2·y)

Odd(x) ≡ ∃y (x = 2·y + 1)

Prove "There is an even integer"

Proof:

2 = 2·1	1.	**2 = 2·1**	**Arithmetic**
so 2 equals 2 times an integer.	2.	∃y (**2** = **2**·y)	**Intro ∃: 1**
Therefore 2 is even.	3.	Even(**2**)	**Defn of** Even: **2**
Therefore, there is an even integer ■	4.	∃x Even(x)	**Intro ∃: 3**

English Even and Odd

Even(x) $\equiv \exists y\ (x=2y)$
Odd(x) $\equiv \exists y\ (x=2y+1)$
Domain: Integers

Prove "The square of every even integer is even."

Proof: Let **a** be an arbitrary even integer.

1. Let **a** be an arbitrary integer
   2.1 Even(**a**) Assumption

Then, by definition, **a** = 2**b** for some integer **b** (depending on **a**).

   2.2 $\exists y\ (\mathbf{a} = 2y)$ Definition
   2.3 **a** = 2**b** — **b** special depends on **a**

Squaring both sides, we get $\mathbf{a}^2 = 4\mathbf{b}^2 = 2(2\mathbf{b}^2)$.

   2.4 $\mathbf{a}^2 = 4\mathbf{b}^2 = 2(2\mathbf{b}^2)$ Algebra

Since $2\mathbf{b}^2$ is an integer, by definition, $\mathbf{a}^2$ is even.

   2.5 $\exists y\ (\mathbf{a}^2 = 2y)$
   2.6 Even($\mathbf{a}^2$) Definition

Since **a** was arbitrary, it follows that the square of every even number is even. ■

2. Even(**a**)$\rightarrow$Even($\mathbf{a}^2$)
3. $\forall x\ (\text{Even}(x)\rightarrow\text{Even}(x^2))$

Even and Odd

Predicate Definitions

Even(x) $\equiv \exists y\ (x = 2y)$

Odd(x) $\equiv \exists y\ (x = 2y + 1)$

Domain of Discourse

Integers

Prove "The square of every odd number is odd."

Even and Odd

Predicate Definitions
Even(x) $\equiv \exists y\ (x = 2y)$
Odd(x) $\equiv \exists y\ (x = 2y + 1)$

Domain of Discourse
Integers

Prove "The square of every odd number is odd."

Proof: Let b be an arbitrary odd number.

Then, b = 2c+1 for some integer c (depending on b).

Therefore, $b^2 = (2c+1)^2 = 4c^2 + 4c + 1 = 2(2c^2 + 2c) + 1$.

Since $2c^2+2c$ is an integer, b^2 is odd. The statement follows since b was arbitrary. ■

Proofs

- Formal proofs follow simple well-defined rules and should be easy to check
  - In the same way that code should be easy to execute
- English proofs correspond to those rules but are designed to be easier for humans to read
  - Easily checkable in principle