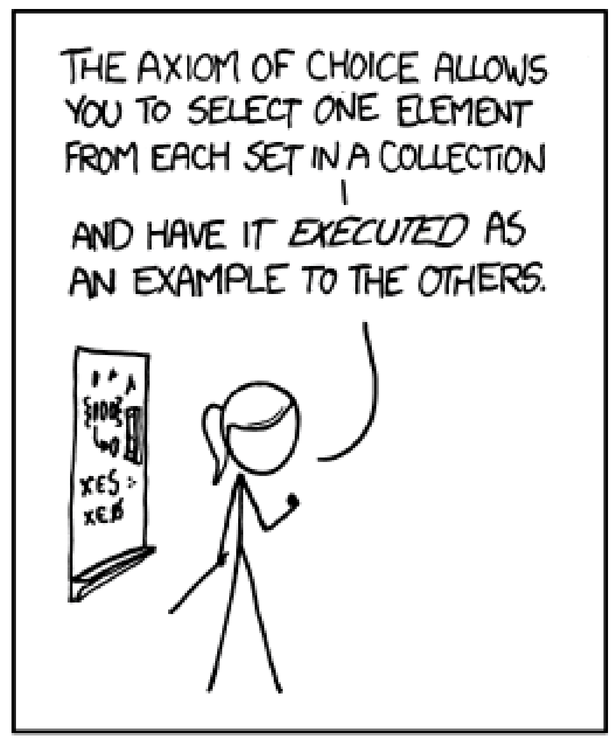
# CSE 311: Foundations of Computing

## Lecture 8: Predicate Logic Proofs

Please pick up
HW 2 Solutions

HW 3 is posted




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:** $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$

| | | |
|---|---|---|
| 1.1. | $(p \rightarrow q) \wedge (q \rightarrow r)$ | Assumption |
| 1.2. | $p \rightarrow q$ | $\wedge$ Elim: 1.1 |
| 1.3. | $q \rightarrow r$ | $\wedge$ 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. | $p \rightarrow r$ | Direct Proof Rule |
| 1. | $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$ | Direct Proof Rule |

## Last class: One General Proof Strategy

1. Look at the rules for introducing connectives to see how you would build up the formula you want to prove from pieces of what is given

2. Use the rules for eliminating connectives to break down the given formulas so that you get the pieces you need to do 1.

3. Write the proof beginning with what you figured out for 2 followed by 1.

# Last Class: Some Inference Rules for Quantifiers

**Intro ∃**

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

**Elim ∀**

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

# Last Class: 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

# Last Class: Predicate Logic Proof

| | | |
|---|---|---|
| Intro $\exists$ | P(c) for some c | |
| | $\therefore$ $\exists$x P(x) | |

| | | |
|---|---|---|
| Elim $\forall$ | $\forall$x P(x) | |
| | $\therefore$ P(a) 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 |

# 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 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** $\exists x\ \text{Even}(x)$

| | | |
|---|---|---|
| 2. | $2 = 2 \cdot 1$ | Math |
| 3. | $\exists y\ (2 = 2 \cdot y)$ | Intro $\exists$: 2 |
| 4. | $\text{Even}(2)$ | by defn from 3 |
| 5. | $\exists x\ \text{Even}(x)$ | Intro $\exists$: 4 |

# 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.** | $\exists y\ (\mathbf{2 = 2} \cdot y)$ | **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 |
|---|
| Even(x) $\equiv \exists y\ (x = 2 \cdot y)$ |
| Odd(x) $\equiv \exists y\ (x = 2 \cdot y + 1)$ |
| 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 |
| --- |
| Even(x) ≡ ∃y (x = 2·y) |
| Odd(x) ≡ ∃y (x = 2·y + 1) |
| Prime(x) ≡ "x > 1 and x≠a·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. $2 = 2\cdot1$ **Arithmetic**
2. Prime(2) **Property of integers**

$2 = 2 \cdot 1$

$\exists y\ (2 = 2 \cdot y)$

Even(2)

Prime(2)

Even(2) $\land$ Prime(2)

$\exists x\,(\text{Even}(x) \land \text{Prime}(x))$ Intro $\exists$:

* 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** $\exists x\ (\text{Even}(x) \wedge \text{Prime}(x))$

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

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

# Inference Rules for Quantifiers: First look

Intro ∃

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

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

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!

# Even and Odd

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

| Intro ∀ | Elim ∃ |
|---|---|
| "**Let** a **be arbitrary***"...P(a) | $\exists x\, P(x)$ |
| ∴ $\forall x\, P(x)$ | ∴ 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 arbitrary

2. Even(a) → Even(a²)

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

# Even and Odd

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

| | |
|---|---|
| Intro $\forall$: $\dfrac{\text{"Let a be arbitrary*"...P(a)}}{\therefore\ \forall x\, P(x)}$ | 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:** $\forall x\,(\text{Even}(x) \to \text{Even}(x^2))$

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

2.1 Even(a) Assumption

2.10 Even(a²)

2. Even(**a**)$\to$Even(**a**$^2$) ? Direct Proof Rule
3. $\forall x\,(\text{Even}(x)\to\text{Even}(x^2))$ 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

1. Let a be an arbitrary integer
2.1 Even(a) Assumption
2.6 Even($a^2$)
2. Even(a)→Even($a^2$) Direct proof rule
3. ∀x (Even(x)→Even($x^2$)) Intro ∀: 1,2

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

**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 $\exists y\,(a=2y)$ by Defn

  2.5 $\exists y\,(a^2=2y)$

  2.6 Even($\mathbf{a}^2$) ? by Defn from 2.5

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

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

# Even and Odd

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

**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 |
| **2.2** | $\exists y\,(\mathbf{a} = 2y)$ | Definition of Even |
| 2.3 | $a = 2 \cdot b$ | Elim ∃ : b special depends on a |
| 2.4 | $a^2 = (2b)^2 = 4b^2 = 2\cdot(2b^2)$ | Math |
| **2.5** | $\exists y\,(\mathbf{a}^2 = 2y)$ | ? |
| **2.6** | Even($\mathbf{a}^2$) | Definition of Even |

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

# Even and Odd

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

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

**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 $\exists y\,(\mathbf{a} = 2y)$ — Definition of Even

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

## Even and Odd

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

| | |
|---|---|
| Intro $\forall$: $\dfrac{\text{"Let a be arbitrary*"...}P(a)}{\therefore\ \forall x\, P(x)}$ | 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 |
| 2.2 | $\exists y$ (**a** = 2y) | Definition of Even |
| 2.3 | **a** = 2**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 |

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

2. Even(**a**)$\rightarrow$Even($\mathbf{a}^2$) — Direct proof rule
3. $\forall x$ (Even(x)$\rightarrow$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 $\forall$: $\dfrac{\text{“Let } a \text{ be arbitrary*”} \ldots P(a)}{\therefore\ \forall x\, P(x)}$

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

**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 |
| 2.3 | $\mathbf{a} = 2\mathbf{b}$ | Elim $\exists$: **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 $\exists$ rule |
| 2.6 | $\text{Even}(\mathbf{a}^2)$ | Definition of Even |

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

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 $\forall$: 1,2

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

**There are extra conditions on using these rules:**

Intro $\forall$

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

* in the domain of P

nothing depends on a

Elim $\exists$

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

** 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 |

# 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) ∴ $\forall x\ P(x)$

* in the domain of P

Elim $\exists$: $\exists x\ P(x)$ ∴ 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**

**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 $\forall$: "Let a be arbitrary*"...P(a) ∴ $\forall x\, P(x)$

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

Elim $\exists$: $\exists x\, P(x)$ ∴ P(c) for some *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 $\exists$

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

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. No other name in P depends on a

Elim $\exists$

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

** 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**

$\text{Even}(x) \equiv \exists y\ (x = 2 \cdot y)$

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

**Prove "There is an even integer"**

**Proof:**

| | | | |
|---|---|---|---|
| $2 = 2 \cdot 1$ | 1. | $2 = 2 \cdot 1$ | Arithmetic |
| so 2 equals 2 times an integer. | 2. | $\exists y\ (2 = 2 \cdot y)$ | Intro $\exists$: 1 |
| Therefore 2 is even. | 3. | $\text{Even}(2)$ | Defn of Even: 2 |
| Therefore, there is an even integer ■ | 4. | $\exists x\ \text{Even}(x)$ | Intro $\exists$: 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**<br>**2.1** Even(**a**) Assumption |
| **Then, by definition, a = 2b for some integer b (depending on a).** | **2.2** $\exists y$ (**a** = 2y) Definition<br>**2.3** **a** = 2**b** **b** special depends on **a** |
| **Squaring both sides, we get** $a^2 = 4b^2 = 2(2b^2)$. | **2.4** $a^2 = 4b^2 = 2(2b^2)$ Algebra |
| **Since** $2b^2$ **is an integer, by definition,** $a^2$ **is even.** | **2.5** $\exists y\ (a^2 = 2y)$<br>**2.6** Even($a^2$) Definition |
| **Since a was arbitrary, it follows that the square of every even number is even.** ■ | **2.** Even(a)$\rightarrow$Even($a^2$)<br>**3.** $\forall x$ (Even(x)$\rightarrow$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."**

Let a be an arbitrary odd number

Then $a = 2b+1$ for some integer b

$a^2 = (2b+1)^2 = 4b^2 + 4b + 1$

$= 2(2b^2 + 2b) + 1$

$\therefore a^2$ is $2 \times$ some integer $+1$

$\therefore a^2$ is odd

1. Let a be arbitrary
2. Odd(a) Assumption
3. $\exists y\ (a = 2y+1)$ by defn
4. $a = 2b+1$ Elim $\exists$ b special depends a
5. $a^2 = (2b+1)^2$ Alg
   $= 4b^2 + 4b + 1$
   $= 2(2b^2 + 2b) + 1$
6. $\exists y\ (a^2 = 2 \cdot y + 1)$ Intro $\exists$
7. Odd($a^2$) by def

$2 \to 7$

# 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