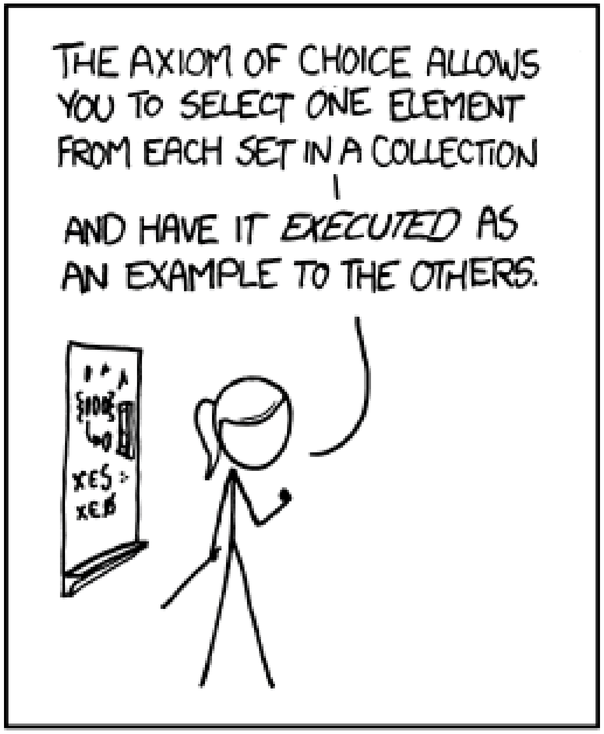
CSE 311: Foundations of Computing

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

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

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

Elim ∀: $\forall x\, P(x)$ ∴ P(a) for any a

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

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

outer connective

Direct Proof rule

The main connective is implication so Direct Proof Rule seems good

My First Predicate Logic Proof

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

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

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

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 ∃: P(c) for some c ∴ ∃x P(x)

Elim ∀: ∀x P(x) ∴ P(a) 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 ∃: P(c) for some c ∴ ∃x P(x)

Elim ∀: ∀x P(x) ∴ 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 ∀: 1.1
1.5.	$\exists x\, P(x)$	Intro ∃: ?
1.	$\forall x\, P(x) \rightarrow \exists x\, P(x)$	Direct Proof Rule

We could have picked any name or domain expression here.

That requires P(c) for some c.

c = a

My First Predicate Logic Proof

Intro ∃: P(c) for some c ∴ $\exists x\ P(x)$

Elim ∀: $\forall x\ P(x)$ ∴ P(a) 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 ∃: P(c) for some c ∴ $\exists x\, P(x)$

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

Working forwards as well as backwards:
In applying "Intro ∃" 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
Even(x) ≡ ∃y (x = 2·y)
Odd(x) ≡ ∃y (x = 2·y + 1)

Prove "There is an even number"

Formally: prove ∃x Even(x)

1.	**2 = 2·1**	**Arithmetic**
2.	∃y (**2 = 2**·y)	**Intro** ∃**: 1**
3.	Even(**2**)	**Definition of** Even**: 2**
4.	∃x Even(x)	**Intro** ∃**: 3**

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"

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"

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

1.	$\mathbf{2 = 2 \cdot 1}$	**Arithmetic**
2.	Prime(**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
Even(x) ≡ $\exists$y (x = 2·y)
Odd(x) ≡ $\exists$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 $\exists x\,(\mathrm{Even}(x) \wedge \mathrm{Prime}(x))$

1.	**2 = 2·1**	**Arithmetic**
2.	Prime(**2**)*	**Property of integers**
3.	$\exists$y (**2 = 2**·y)	**Intro $\exists$: 1**
4.	Even(**2**)	**Defn of Even: 3**
5.	Even(**2**) $\wedge$ Prime(**2**))	**Intro $\wedge$: 2, 4**
6.	$\exists$x (Even(x) $\wedge$ 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 ∀

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

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

Even and Odd

Intro ∀	"Let a be arbitrary*"...P(a) ∴ ∀x P(x)	Elim ∃	∃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. Even(a) → Even(a²)

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

Even and Odd

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

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) ∴ $\forall x\, P(x)$	$\exists x\, P(x)$ ∴ 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. $\text{Even}(\mathbf{a})\rightarrow\text{Even}(\mathbf{a}^2)$?
3. $\forall x\ (\text{Even}(x)\rightarrow\text{Even}(x^2))$ Intro ∀: 1,2

Even and Odd

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

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

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

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

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

    2.1 Even(**a**) Assumption

    2.6 Even($\mathbf{a}^2$) ?

2. Even(**a**)→Even($\mathbf{a}^2$) Direct proof rule
3. ∀x (Even(x)→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 ∀	"Let a be arbitrary*"...P(a) ∴ ∀x P(x)	Elim ∃	∃x P(x) ∴ P(c) for some *special*** c

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

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

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

Even and Odd

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

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

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

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

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 ∃ rule: ?
2.6	Even($\mathbf{a}^2$)	Definition of Even

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

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

Even and Odd

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

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

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

Formal proof of: ∀x (Even(x) → Even(x^2))

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

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

Even and Odd

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

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

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

Formal proof of: ∀x (Even(x) → Even(x^2))

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

2.1	Even(**a**)	Assumption
2.2	∃y (**a** = 2y)	Definition of Even
2.3	**a** = 2**b**	Elim ∃: **b** special depends on **a**
2.4	$\mathbf{a}^2 = 4\mathbf{b}^2 = 2(2\mathbf{b}^2)$	Algebra
2.5	∃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. ∀x (Even(x)→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 ∀: "Let a be arbitrary*"...P(a) ∴ ∀x P(x)

* in the domain of P

Nothing depends on a

Elim ∃: ∃x P(x) ∴ P(c) for some *special*** c

** c has to be a NEW name.

depends on

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 ∀: 1
4. $b \geq a$ — Elim ∃: b special depends on a
5. ~~$\forall x\, (b \geq x)$ — Intro ∀: 2,4~~
6. $\exists y \forall x\, (y \geq x)$ — Intro ∃ : 5

P(a)

∀x P(x)

P(x) "b ≥ x"

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. $\exists y\, (y \geq a)$ — 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!

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 ∃

P(c) for some c

∴ ∃x P(x)

Elim ∀

∀x P(x)

∴ P(a) **for any** a

Intro ∀

"**Let** a **be arbitrary***" ...P(a)

∴ ∀x P(x)

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

Elim ∃

∃x P(x)

∴ P(c) **for some *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, $a = 2b$ for some integer b (depending on a).	2.2 $\exists y \ (a = 2y)$ Definition 2.3 $a = 2b$ 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 $\exists y \ (a^2 = 2y)$ 2.6 $Even(a^2)$ Definition
Since a was arbitrary, it follows that the square of every even number is even. ■	2. $Even(a) \rightarrow Even(a^2)$ 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."

Even and Odd

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

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