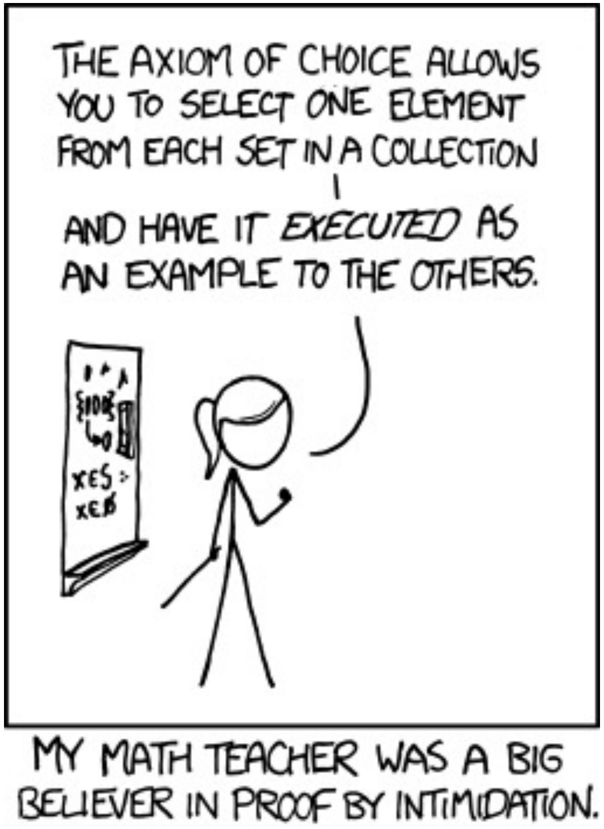
CSE 311: Foundations of Computing

Lecture 8: More inference proofs



Recap from last lecture: Logical inference

- **Given:** A list of (predicate/prop. logic) formulas as **facts**.
- **Question:** What other facts can be derived from those?

List of inference rules:

$$\frac{q \wedge r}{\therefore q, r} \qquad \frac{q, r}{\therefore q \wedge r} \qquad \frac{q \vee r, \neg q}{\therefore r} \qquad \frac{q, q \rightarrow r}{\therefore r}$$

$$\frac{q}{\therefore q \vee r} \qquad \frac{q \Rightarrow r}{\therefore q \rightarrow r}$$

Direct Proof Rule

Not like other rules

Recap from last lecture: Logical inference

- **Given:** A list of (predicate/prop. logic) formulas as **facts**.
- **Question:** What other facts can be derived from those?

List of inference rules:

$$\frac{q \wedge r}{\therefore\ q,\ r} \qquad \frac{q,\ r}{\therefore\ q \wedge r} \qquad \frac{q \vee r\ ,\ \neg q}{\therefore\ r} \qquad \frac{q,\ q \rightarrow r}{\therefore\ r}$$

$$\frac{q}{\therefore\ q \vee r} \qquad \frac{q \Rightarrow r}{\therefore\ q \rightarrow r}$$

Direct Proof Rule

Not like other rules

Example: Show that s follows from q, q $\rightarrow$ r, and r $\rightarrow$ s

Recap from last lecture: Logical inference

- <u>Given:</u> A list of (predicate/prop. logic) formulas as **facts**.
- <u>Question:</u> What other facts can be derived from those?

List of inference rules:

$$\frac{q \land r}{\therefore q, r} \qquad \frac{q, r}{\therefore q \land r} \qquad \frac{q \lor r, \neg q}{\therefore r} \qquad \frac{q, q \rightarrow r}{\therefore r}$$

$$\frac{q}{\therefore q \lor r} \qquad \frac{q \Rightarrow r}{\therefore q \rightarrow r}$$

Direct Proof Rule

Not like other rules

Example: Show that s follows from q, $q \rightarrow r$, and $r \rightarrow s$

1.	q	Given
2.	$q \rightarrow r$	Given
3.	$r \rightarrow s$	Given
4.		
5.		

Recap from last lecture: Logical inference

- **Given:** A list of (predicate/prop. logic) formulas as facts.
- **Question:** What other facts can be derived from those?

List of inference rules:

$$\frac{q \wedge r}{\therefore q, r} \qquad \frac{q, r}{\therefore q \wedge r} \qquad \frac{q \vee r, \neg q}{\therefore r} \qquad \frac{q, q \rightarrow r}{\therefore r}$$

$$\frac{q}{\therefore q \vee r} \qquad \frac{q \Rightarrow r}{\therefore q \rightarrow r}$$

Direct Proof Rule

Not like other rules

Example: Show that s follows from q, $q \rightarrow r$, and $r \rightarrow s$

1.	q	Given
2.	$q \rightarrow r$	Given
3.	$r \rightarrow s$	Given
4.	r	MP: 1, 2
5.	s	MP: 3, 4

To Prove An Implication: $A \to B$

- We use the direct proof rule
- The "pre-requisite" $A \Rightarrow B$ for the direct proof rule is **a proof** that "**Given** A, we can prove B."
- The direct proof rule:

  If you have such a proof then you can conclude that $A \to B$ is true

To Prove An Implication: $A \rightarrow B$

- We use the direct proof rule
- The "pre-requisite" $A \Rightarrow B$ for the direct proof rule is **a proof** that "**Given** A, we can prove B**.**"
- The direct proof rule:

  If you have such a proof then you can conclude that $A \rightarrow B$ is true

Example: Prove **$q \rightarrow (q \vee r)$.**

To Prove An Implication: $A \rightarrow B$

- We use the direct proof rule
- The "pre-requisite" $A \Rightarrow B$ for the direct proof rule is **a proof** that "**Given** A, we can prove B."
- The direct proof rule:

  If you have such a proof then you can conclude that $A \rightarrow B$ is true

Example: Prove $q \rightarrow (q \vee r)$.

proof subroutine

Indent proof subroutine $\Rightarrow$

1.	q	Assumption
2.	$q \vee r$	Intro $\vee$: 1
3.	$q \rightarrow (q \vee r)$	Direct Proof Rule

To Prove An Implication: $A \rightarrow B$ (cont.)

- A template for the application of the **direct proof rule**:

1. (...) Given
2. (...) Given
3. (...) Inferred fact
4. (...) Inferred fact
    - 5.1 A Assumption
    - 5.2 (...) Inferred fact
    - 5.3 (...) Inferred fact
    - 5.4 B Inferred fact
5. $A \rightarrow B$ Direct proof rule
6. (...) Inferred fact

- Possible to have nested direct proof rules

Proofs using the direct proof rule

Show that $q \rightarrow s$ follows from r and $(q \wedge r) \rightarrow s$

Proofs using the direct proof rule

Show that $q \rightarrow s$ follows from r and $(q \wedge r) \rightarrow s$

1. r Given
2. $(q \wedge r) \rightarrow s$ Given
3.

Proofs using the direct proof rule

Show that $q \rightarrow s$ follows from r and $(q \wedge r) \rightarrow s$

1. r Given
2. $(q \wedge r) \rightarrow s$ Given
   3.1. q Assumption
   3.2.
   3.3.
3.

Proofs using the direct proof rule

Show that $q \to s$ follows from r and $(q \wedge r) \to s$

1. r Given
2. $(q \wedge r) \to s$ Given
   - 3.1. q Assumption
   - 3.2. $q \wedge r$ Intro $\wedge$: 1, 3.1
   - 3.3.
3.

Proofs using the direct proof rule

Show that $q \rightarrow s$ follows from r and $(q \wedge r) \rightarrow s$

1. r Given
2. $(q \wedge r) \rightarrow s$ Given
   - 3.1. q Assumption
   - 3.2. $q \wedge r$ Intro $\wedge$: 1, 3.1
   - 3.3. s MP: 2, 3.2
3.

Proofs using the direct proof rule

Show that $q \rightarrow s$ follows from r and $(q \wedge r) \rightarrow s$

1. r Given
2. $(q \wedge r) \rightarrow s$ Given

This is a proof of $q \rightarrow s$

3.1.	q	Assumption
3.2.	$q \wedge r$	Intro $\wedge$: 1, 3.1
3.3.	s	MP: 2, 3.2

If we know q is true… Then, we've shown s is true

3. $q \rightarrow s$ Direct Proof Rule

Example

Prove: $(q \wedge r) \rightarrow (q \vee r)$

There MUST be an application of the Direct Proof Rule (or an equivalence) to prove this implication.

Where do we start? We have no givens…

Example

Prove: $(q \wedge r) \rightarrow (q \vee r)$

Example

Prove: $(q \wedge r) \rightarrow (q \vee r)$

1.1.	$q \wedge r$	Assumption
1.2.	q	Elim $\wedge$: 1.1
1.3.	$q \vee r$	Intro $\vee$: 1.2
1.	$(q \wedge r) \rightarrow (q \vee r)$	Direct Proof Rule

Lecture 8 Activity

- You will be assigned to **breakout rooms**. Please:
- Introduce yourself
- Choose someone to share screen, showing this PDF
- Given: $p \vee q$, $(r \wedge s) \rightarrow \neg q$, r.
- Show: $s \rightarrow p$ using inference rules
- Hint: You will need one Direct Proof Rule

Then fill out the poll everywhere for Activity Credit!
Go to pollev.com/thomas311 and login with your UW identity

Overview over inference rules:
https://courses.cs.washington.edu/courses/cse311/21sp/resources/inferencesPoster.pdf

Example

Prove: $((q \rightarrow r) \land (r \rightarrow s)) \rightarrow (q \rightarrow s)$

Example

Prove: $((q \rightarrow r) \wedge (r \rightarrow s)) \rightarrow (q \rightarrow s)$

1.1. $(q \rightarrow r) \wedge (r \rightarrow s)$ **Assumption**

1.2.

1.3.

1.4.1.

1.4.2.

1.4.3.

1.4. $q \rightarrow s$

1. $((q \rightarrow r) \wedge (r \rightarrow s)) \rightarrow (q \rightarrow s)$ **Direct Proof Rule**

Example

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

1.1. $(q \to r) \land (r \to s)$ Assumption

1.2. $q \to r$ $\land$ Elim: 1.1

1.3. $r \to s$ $\land$ Elim: 1.1

1.4.1.

1.4.2.

1.4.3.

1.4. $q \to s$

1. $((q \to r) \land (r \to s)) \to (q \to s)$ Direct Proof Rule

Example

Prove: $((q \to r) \wedge (r \to s)) \to (q \to s)$

1.1.	$(q \to r) \wedge (r \to s)$	Assumption
1.2.	$q \to r$	$\wedge$ Elim: 1.1
1.3.	$r \to s$	$\wedge$ Elim: 1.1
1.4.1.	q	Assumption
1.4.2.		
1.4.3.		
1.4.	$q \to s$	Direct Proof Rule
1.	$((q \to r) \wedge (r \to s)) \to (q \to s)$	Direct Proof Rule

Example

Prove: $((q \rightarrow r) \wedge (r \rightarrow s)) \rightarrow (q \rightarrow s)$

1.1. $(q \rightarrow r) \wedge (r \rightarrow s)$ **Assumption**

1.2. $q \rightarrow r$ **∧ Elim: 1.1**

1.3. $r \rightarrow s$ **∧ Elim: 1.1**

1.4.1. q **Assumption**

1.4.2. r **MP: 1.2, 1.4.1**

1.4.3.

1.4. $q \rightarrow s$ **Direct Proof Rule**

1. $((q \rightarrow r) \wedge (r \rightarrow s)) \rightarrow (q \rightarrow s)$ **Direct Proof Rule**

Example

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

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

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.

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

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

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

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

The main connective is implication so Direct Proof Rule seems good

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

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 ∴ $\exists x\, P(x)$

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

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 ∴ $\exists x\, P(x)$
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.	Let a be an object.	
1.3.	$P(a)$	Elim ∀: 1.1

We could have picked any name or domain expression here.

1.5.	$\exists x\, P(x)$	Intro ∃: ?

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

No holes. Just need to clean up.

1.1.	$\forall x\, P(x)$	Assumption
1.2.	Let a be an object.	
1.3.	$P(a)$	Elim ∀: 1.1
1.5.	$\exists x\, P(x)$	Intro ∃: 1.3

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.	Let a be an object.	
1.3.	$P(a)$	Elim ∀: 1.1
1.4.	$\exists x\, P(x)$	Intro ∃: 1.3

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

<u>Working forwards as well as backwards</u>:
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
$\text{Even}(x) \equiv \exists y\ (x = 2 \cdot y)$
$\text{Odd}(x) \equiv \exists y\ (x = 2 \cdot y + 1)$

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
$\text{Even}(x) \equiv \exists y\ (x = 2 \cdot y)$
$\text{Odd}(x) \equiv \exists y\ (x = 2 \cdot y + 1)$
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) ≡ $\exists$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 $\exists x\,(\text{Even}(x) \land \text{Prime}(x))$

1.	**2 = 2·1**	**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) ≡ ∃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 ∃x (Even(x) ∧ Prime(x))

1.	**2 = 2·1**	**Arithmetic**
2.	Prime(**2**)*	**Property of integers**
3.	∃y (**2 = 2**·y)	**Intro** ∃**: 1**
4.	Even(**2**)	**Defn of** Even**: 3**
5.	Even(**2**) ∧ Prime(**2**)	**Intro** ∧**: 2, 4**
6.	∃x (Even(x) ∧ Prime(x))	**Intro** ∃**: 5**

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

Inference Rules for Quantifiers: First look

Intro ∃

P(c) for some c

∴ $\exists x\, P(x)$

Elim ∀

$\forall x\, P(x)$

∴ P(a) **for any** a

Intro ∀

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

∴ $\forall x\, P(x)$

* in the domain of P

Elim ∃

$\exists x\, P(x)$

∴ P(c) **for some *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) ∴ $\forall x\, P(x)$	$\exists x\, P(x)$ ∴ P(c) for some *special*** c

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

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

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

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) ∴ $\forall x\, P(x)$	$\exists x\, P(x)$ ∴ 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

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

Elim ∃

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

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

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

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

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

Intro $\forall$	Elim $\exists$
"Let a be arbitrary*"...P(a)	$\exists x\, P(x)$
$\therefore\ \forall x\, P(x)$	$\therefore$ 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 $\text{Even}(\mathbf{a})$ — 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 $\forall$: 1,2

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
   - 2.5 $\exists y\,(\mathbf{a}^2 = 2y)$ — 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) ≡ ∃y (x=2y)
Odd(x) ≡ ∃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: $\forall x\,(\text{Even}(x) \rightarrow \text{Even}(x^2))$

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

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 $\exists y\,(\mathbf{a}^2 = 2y)$ — Intro ∃ rule
   - 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

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

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)

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

* in the domain of P

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

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

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. 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.