CSE 311: Foundations of Computing

Lecture 8: More inference proofs

The Axiom of Choice allows you to select one element from each set in a collection and have it executed as an example to the others.

My math teacher was a big believer in proof by intimidation.
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:**

- \( q \land r \quad q, r \quad q \lor r, \neg q \quad q, q \rightarrow r \)
  \[ \therefore q, r \quad \therefore q \land r \quad \therefore r \quad \therefore r \]

- \( q \quad q \Rightarrow r \quad q \Rightarrow r \)
  \[ \therefore q \lor r \quad \therefore q \rightarrow r \]

**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:

\[
\begin{align*}
\text{q \land r} & \quad \text{q, r} & \quad \text{q \lor r, \neg q} & \quad \text{q, q \rightarrow r} \\
\therefore q, r & \quad \therefore q \land r & \quad \therefore r & \quad \therefore r
\end{align*}
\]

\[
\begin{align*}
\text{q} & \quad \text{q \Rightarrow r} \\
\therefore q \lor r & \quad \therefore q \rightarrow r
\end{align*}
\]

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

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

List of inference rules:

- \[ \frac{q \land r}{\therefore q, r} \]
- \[ \frac{q, r}{\therefore q \land r} \]
- \[ \frac{q \lor r, \neg q}{\therefore r} \]
- \[ \frac{q, q \rightarrow r}{\therefore r} \]
- \[ \frac{q \neg \rightarrow r}{\therefore q \rightarrow r} \]

**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:

- \( \frac{q \land r}{q, r} \)
- \( \frac{q, r}{q \land r} \)
- \( \frac{q \lor r, \neg q}{r} \)
- \( \frac{q, q \rightarrow r}{r} \)
- \( \frac{q \rightarrow r}{q \lor r} \)
- \( \frac{q \Rightarrow r}{q ightarrow r} \)

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: $A \rightarrow B$

- 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
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 \( q \rightarrow (q \lor r) \).
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 $q \rightarrow (q \lor r)$.

Indent proof subroutine

1. $q$ Assumption
2. $q \lor r$ Intro $\lor$: 1
3. $q \rightarrow (q \lor r)$ 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 $(q \land r) \rightarrow s$
Proofs using the direct proof rule

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

1. \( r \) Given
2. \( (q \land r) \rightarrow s \) Given
3.
Proofs using the direct proof rule

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

1. \( r \) Given

2. \( (q \land r) \rightarrow s \) Given

3.1. \( q \) Assumption

3.2.

3.3.

3.
Proofs using the direct proof rule

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

1. $r$ Given
2. $(q \land r) \rightarrow s$ Given
   3.1. $q$ Assumption
   3.2. $q \land r$ Intro $\land$: 1, 3.1
3.3.
3.
Proofs using the direct proof rule

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

1. $r$ Given

2. $(q \land r) \rightarrow s$ Given
   
   3.1. $q$ Assumption
   
   3.2. $q \land r$ Intro $\land$: 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 \( (q \land r) \rightarrow s \)

1. \( r \) \hspace{1em} Given
2. \( (q \land r) \rightarrow s \) \hspace{1em} Given

This is a proof of \( q \rightarrow s \)

3.1. \( q \) \hspace{1em} Assumption
3.2. \( q \land r \) \hspace{1em} Intro \( \land \hspace{1em} 1, 3.1 \)
3.3. \( s \) \hspace{1em} MP: 2, 3.2

If we know \( q \) is true...

Then, we’ve shown \( s \) is true

3. \( q \rightarrow s \) \hspace{1em} Direct Proof Rule
Example

Prove: \((q \land r) \rightarrow (q \lor r)\)

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: \((q \land r) \rightarrow (q \lor r)\)
Example

Prove: \((q \land r) \rightarrow (q \lor r)\)

1.1. \(q \land r\) \hspace{2cm} \text{Assumption}
1.2. \(q\) \hspace{2cm} \text{Elim} \land: 1.1
1.3. \(q \lor r\) \hspace{2cm} \text{Intro} \lor: 1.2

1. \((q \land r) \rightarrow (q \lor r)\) \hspace{2cm} \text{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: \( p \lor q, (r \land s) \rightarrow \neg q, r. \)
- 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:
Example

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

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

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

1.2.

1.3.

1.4.1.

1.4.2.

1.4.3.

1.4. $q \rightarrow s$

1. $(q \rightarrow r) \land (r \rightarrow s) \rightarrow (q \rightarrow s)$ 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: \(((q \rightarrow r) \land (r \rightarrow s)) \rightarrow (q \rightarrow s)\)

1.1. \((q \rightarrow r) \land (r \rightarrow s)\) Assumption

1.2. \(q \rightarrow r\) \land Elim: 1.1

1.3. \(r \rightarrow s\) \land Elim: 1.1

1.4.1. \(q\) Assumption

1.4.2.

1.4.3.

1.4. \(q \rightarrow s\) Direct Proof Rule

1. \(((q \rightarrow r) \land (r \rightarrow s)) \rightarrow (q \rightarrow s)\) Direct Proof Rule
Example

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

1.1. \((q \rightarrow r) \land (r \rightarrow s)\) Assumption
1.2. \(q \rightarrow r\) \quad \land \text{Elim: 1.1}
1.3. \(r \rightarrow s\) \quad \land \text{Elim: 1.1}

1.4.1. \(q\) Assumption
1.4.2. \(r\) \quad \text{MP: 1.2, 1.4.1}

1.4.3.

1.4. \(q \rightarrow s\) \quad \text{Direct Proof Rule}

1. \(( (q \rightarrow r) \land (r \rightarrow s)) \rightarrow (q \rightarrow s)\) \quad \text{Direct Proof Rule}
Example

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

1.1. \((q \rightarrow r) \land (r \rightarrow s)\) Assumption
1.2. \(q \rightarrow r\) \land Elim: 1.1
1.3. \(r \rightarrow s\) \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. \(q \rightarrow s\) Direct Proof Rule
1. \(((q \rightarrow r) \land (r \rightarrow s)) \rightarrow (q \rightarrow s)\) 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

* in the domain of P

** 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

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

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

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

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

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

We need an \( \exists \) we don’t have so “intro \( \exists \)” rule makes sense

\[ \text{Intro } \exists \quad \begin{array}{c} P(c) \text{ for some } c \\ \therefore \exists x P(x) \end{array} \]

\[ \text{Elim } \forall \quad \begin{array}{c} \forall x P(x) \\ \therefore P(a) \text{ for any } a \end{array} \]
My First Predicate Logic Proof

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

1. \( \forall x \ P(x) \rightarrow \exists x \ P(x) \)  \hspace{1cm} \text{Direct Proof Rule}

1.1. \( \forall x \ P(x) \)  \hspace{1cm} \text{Assumption}

1.5. \( \exists x \ P(x) \)  \hspace{1cm} \text{Intro } \exists : ?

We need an \( \exists \) we don’t have so “intro } \exists” rule makes sense

That requires \( P(c) \) for some \( c \).
My First Predicate Logic Proof

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

1. \( \forall x \, P(x) \) Assumption
   1.1. \( \forall x \, P(x) \)
   1.2. Let \( a \) be an object.
   1.3. \( P(a) \) Elim \( \forall \): 1.1

   We could have picked any name or domain expression here.

   1.5. \( \exists x \, P(x) \) Intro \( \exists \): ?

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

\[ \begin{align*}
\forall x \, P(x) & \quad \text{P(c) for some c} \\
\forall x \, P(x) & \quad \therefore \exists x \, P(x) \\
\forall x \, P(x) & \quad \therefore P(a) \text{ for any } a
\end{align*} \]
My First Predicate Logic Proof

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

1. $\forall x P(x)$ Assumption
2. Let $a$ be an object.
3. $P(a)$ Elim $\forall$: 1.1

5. $\exists x P(x)$ Intro $\exists$: 1.3

1. $\forall x P(x) \rightarrow \exists x P(x)$ Direct Proof Rule
My First Predicate Logic Proof

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 \( \forall \): 1.1
1.4. \( \exists x \, P(x) \) Intro \( \exists \): 1.3

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

\textbf{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.
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:

<table>
<thead>
<tr>
<th>Domain of Discourse</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integers</td>
</tr>
</tbody>
</table>

Given the basic properties of arithmetic on integers, define:

<table>
<thead>
<tr>
<th>Predicate Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Even(x) ( \equiv \exists y \ (x = 2 \cdot y) )</td>
</tr>
<tr>
<td>Odd(x) ( \equiv \exists y \ (x = 2 \cdot y + 1) )</td>
</tr>
</tbody>
</table>
A Not so Odd Example

<table>
<thead>
<tr>
<th>Domain of Discourse</th>
<th>Predicate Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integers</td>
<td>Even(x) $\equiv \exists y \ (x = 2 \cdot y)$</td>
</tr>
<tr>
<td></td>
<td>Odd(x) $\equiv \exists y \ (x = 2 \cdot y + 1)$</td>
</tr>
</tbody>
</table>

Prove “There is an even number”

Formally: prove $\exists x \text{ Even}(x)$
A Not so Odd Example

<table>
<thead>
<tr>
<th>Domain of Discourse</th>
<th>Predicate Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integers</td>
<td>Even(x) ≡ ∃y (x = 2·y)</td>
</tr>
<tr>
<td></td>
<td>Odd(x) ≡ ∃y (x = 2·y + 1)</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Domain of Discourse</th>
<th>Predicate Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integers</td>
<td>Even(x) $\equiv \exists y \ (x = 2 \cdot y)$</td>
</tr>
<tr>
<td></td>
<td>Odd(x) $\equiv \exists y \ (x = 2 \cdot y + 1)$</td>
</tr>
<tr>
<td></td>
<td>Prime(x) $\equiv \ &quot;x &gt; 1 \text{ and } x \neq a \cdot b \text{ for all integers } a, b \text{ with } 1 &lt; a &lt; x&quot;$</td>
</tr>
</tbody>
</table>

Prove “There is an even prime number”
A Prime Example

Predicate Definitions

<table>
<thead>
<tr>
<th>Domain of Discourse</th>
<th>Predicate Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integers</td>
<td>Even(x) ( \equiv \exists y \ (x = 2 \cdot y) )</td>
</tr>
<tr>
<td></td>
<td>Odd(x) ( \equiv \exists y \ (x = 2 \cdot y + 1) )</td>
</tr>
<tr>
<td></td>
<td>Prime(x) ( \equiv ) “x &gt; 1 and x \neq a \cdot b ) for all integers a, b with 1 &lt; a &lt; x”</td>
</tr>
</tbody>
</table>

Prove “There is an even prime number”

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

1. \( 2 = 2 \cdot 1 \) \hspace{1cm} \text{Arithmetic}
2. \( \text{Prime}(2) \) \hspace{1cm} \text{Property of integers}

* Later we will further break down “Prime” using quantifiers to prove statements like this
A Prime Example

<table>
<thead>
<tr>
<th>Domain of Discourse</th>
<th>Predicate Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integers</td>
<td></td>
</tr>
</tbody>
</table>

Even\( (x) \equiv \exists y \ (x = 2 \cdot y) \)
Odd\( (x) \equiv \exists y \ (x = 2 \cdot y + 1) \)
Prime\( (x) \equiv \text{“} x > 1 \) 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. \( 2 = 2 \cdot 1 \)\hspace{1cm} Arithmetic
2. Prime\( (2) \)\hspace{1cm} Property of integers
3. \( \exists y \ (2 = 2 \cdot y) \)\hspace{1cm} Intro \( \exists: 1 \)
4. Even\( (2) \)\hspace{1cm} Defn of Even: 3
5. Even\( (2) \land \text{Prime}(2) \)\hspace{1cm} Intro \( \land: 2, 4 \)
6. \( \exists x \ (\text{Even}(x) \land \text{Prime}(x)) \)\hspace{1cm} Intro \( \exists: 5 \)

* Later we will further break down “Prime” using quantifiers to prove statements like this
Inference Rules for Quantifiers: First look

**Intro ∃**

\[ P(c) \text{ for some } c \]

\[ \therefore \exists x \ P(x) \]

\[ \text{Intro } \forall \]

\[ \text{“Let } a \text{ be arbitrary*”... } P(a) \]

\[ \therefore \forall x \ P(x) \]

\[ \text{Elim } \forall \]

\[ \forall x \ P(x) \]

\[ \therefore P(a) \text{ for any } a \]

\[ \text{Intro } \exists \]

\[ \exists x \ P(x) \]

\[ \therefore P(c) \text{ for some } \text{special** } c \]

**Intro ∀**

**Elim ∃**

**Intro ∃**

\[ \text{“Let a be arbitrary*”... } P(a) \]

\[ \therefore \forall x \ P(x) \]

\[ \text{Elim } \exists \]

\[ \exists x \ P(x) \]

\[ \therefore P(c) \text{ for some special** } c \]

---

* in the domain of P

** 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

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

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

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

Intro \( \forall \): 1, 2
Even and Odd

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(a^2)

2. Even(a) \(\rightarrow\) Even(a^2) Direct proof rule

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

\( \vdots \) P(c) for some special** c

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

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 \( \text{Even}(a) \) Assumption
   2.2 \( \exists y \ (a = 2y) \) Definition of Even

   \[ 2.5 \exists y \ (a^2 = 2y) \]
   2.6 \( \text{Even}(a^2) \) Definition of Even

2. \( \text{Even}(a) \to \text{Even}(a^2) \) Direct proof rule

3. \( \forall x \ (\text{Even}(x) \to \text{Even}(x^2)) \) Intro \( \forall \): 1,2
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 \( \text{Even}(a) \)  Assumption
   2.2 \( \exists y \ (a = 2y) \)  Definition of Even

   2.5 \( \exists y \ (a^2 = 2y) \)  Intro \( \exists \) rule:  \( \varnothing \)  Need \( a^2 = 2c \) for some \( c \)
   2.6 \( \text{Even}(a^2) \)  Definition of Even

2. \( \text{Even}(a) \rightarrow \text{Even}(a^2) \)  Direct proof rule

3. \( \forall x \ (\text{Even}(x) \rightarrow \text{Even}(x^2)) \)  Intro \( \forall \): 1,2
Even and Odd

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 $\text{Even}(a)$ Assumption
   2.2 $\exists y \ (a = 2y)$ Definition of Even
   2.3 $a = 2b$ Elim $\exists$: $b$ special depends on $a$

   2.5 $\exists y \ (a^2 = 2y)$ Intro $\exists$ rule: $a^2 = 2c$ for some $c$
   2.6 $\text{Even}(a^2)$ Definition of Even

2. $\text{Even}(a) \rightarrow \text{Even}(a^2)$ Direct proof rule

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

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

2. \( \text{Even}(a) \rightarrow \text{Even}(a^2) \) 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:

1. Intro \( \forall \) “Let \( a \) be arbitrary*”...\( P(a) \) 
   \[ \therefore \] \( \forall x \ P(x) \) 

   * in the domain of \( P \)

2. Elim \( \exists \) \( \exists x \ P(x) \) 
   \[ \therefore P(c) \text{ for some } \text{special** } c \] 

   ** \( c \) 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
Why did we need to say that $b$ depends on $a$?

There are extra conditions on using these rules:

- 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*"...\( \forall x \ P(x) \)
  - * in the domain of \( P \). No other name in \( P \) depends on \( a \)

- **Elim \( \exists \)**: \( \exists x \ P(x) \)
  - ...\( \forall x \ P(x) \)
  - ...\( P(c) \) 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

\[ \begin{align*}
\text{Intro } \exists & \quad P(c) \text{ for some } c \\
\therefore & \quad \exists x \ P(x) 
\end{align*} \]

\[ \begin{align*}
\text{Elim } \forall & \quad \forall x \ P(x) \\
\therefore & \quad P(a) \text{ for any } a 
\end{align*} \]

\[ \begin{align*}
\text{Intro } \forall & \quad \text{“Let } a \text{ be arbitrary*”...} P(a) \\
\therefore & \quad \forall x \ P(x) 
\end{align*} \]

\[ \begin{align*}
\text{Elim } \exists & \quad \exists x \ P(x) \\
\therefore & \quad P(c) \text{ for some } \text{special** } c 
\end{align*} \]

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

** 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.