Lecture 8: Predicate Logic Proofs

...let's assume there exists some function $F(a, b, c, ...)$ which produces the correct answer—hang on.

This is going to be one of those weird, dark-magic proofs, isn't it? I can tell.

What? No, no, it's a perfectly sensible chain of reasoning.

All right...

Now, let's assume the correct answer will eventually be written on this board at the coordinates $(x, y)$. If we—

I knew it!
Last class: Propositional Inference Rules

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

- **Elim \( \land \)**
  - \( A \land B \)
  - \( \therefore A, B \)

- **Intro \( \land \)**
  - \( A; B \)
  - \( \therefore A \land B \)

- **Elim \( \lor \)**
  - \( A \lor B; \neg A \)
  - \( \therefore B \)

- **Intro \( \lor \)**
  - \( A \)
  - \( \therefore A \lor B, B \lor A \)

- **Modus Ponens**
  - \( A; A \rightarrow B \)
  - \( \therefore B \)

- **Direct Proof Rule**
  - \( A \Rightarrow B \)
  - \( \therefore A \rightarrow B \)

Not like other rules
Last Class: 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 “\textbf{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
  \[
  \frac{A \Rightarrow B}{\therefore A \rightarrow B}
  \]
- 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 \( p \rightarrow (p \lor q) \).


\[\begin{align*}
\text{Indent proof subroutine} & \\
1.1. & p \quad \text{Assumption} \\
1.2. & p \lor q \quad \text{Intro } \lor: 1 \\
1. & p \rightarrow (p \lor q) \quad \text{Direct Proof Rule}
\end{align*}\]
Proofs using the direct proof rule

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

1. $q$  Given
2. $(p \land q) \rightarrow r$  Given

This is a proof of $p \rightarrow r$

3.1. $p$  Assumption
3.2. $p \land q$  Intro $\land$: 1, 3.1
3.3. $r$  MP: 2, 3.2

If we know $p$ is true...

Then, we've shown $r$ is true

3. $p \rightarrow r$  Direct Proof Rule
Example

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

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

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

1.1. \(p \land q\) Assumption

1.? \(p \lor q\)

1. \((p \land q) \rightarrow (p \lor q)\) Direct Proof Rule
Example

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

1.1. \(p \land q\) \hspace{1cm} \text{Assumption}

1.2. \(p\) \hspace{1cm} \text{Elim} \land \text{: 1.1}

1.? \(p \lor q\)

1. \((p \land q) \rightarrow (p \lor q)\) \hspace{1cm} \text{Direct Proof Rule}
Example

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

1.1. \( p \land q \) \hspace{1cm} Assumption
1.2. \( p \) \hspace{1cm} Elim \( \land \): 1.1
1.3. \( p \lor q \) \hspace{1cm} Intro \( \lor \): 1.2

1. \( (p \land q) \rightarrow (p \lor q) \) \hspace{1cm} 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.
Example

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

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

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

1.? \(p \rightarrow r\)

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

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

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

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

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

1.? \( p \rightarrow r \)

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

1.4. \(p \to r\) Direct Proof Rule

1. \(((p \to q) \land (q \to r)) \to (p \to r)\) Direct Proof Rule
Example

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

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

1.2. \(p \rightarrow q\) \hspace{1cm} \land \text{Elim: 1.1}

1.3. \(q \rightarrow r\) \hspace{1cm} \land \text{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. \(((p \rightarrow q) \land (q \rightarrow r)) \rightarrow (p \rightarrow r)\) Direct Proof Rule
Inference Rules for Quantifiers: First look

\[ P(c) \text{ for some } c \hspace{2cm} \forall x \ P(x) \]

\[ \therefore \exists x \ P(x) \hspace{2cm} \therefore P(a) \text{ (for any } a) \]

** Intro \( \exists \)**

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

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

** Elim \( \forall \)**

** Intro \( \forall \)**

** By special, we mean that } c \text{ is a name for a value where } P(c) \text{ is true. We can’t use anything else about that value, so } c \text{ has to be a NEW name!**}
My First Predicate Logic Proof

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

5. \((\forall x \ P(x)) \rightarrow (\exists x \ P(x))\)
My First Predicate Logic Proof

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

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

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. $\forall x P(x)$ Assumption

1.5. $\exists x P(x)$ Intro $\exists$: We need an $\exists$ we don’t have so “intro $\exists$” rule makes sense

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

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

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

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

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

$P(c)$ for some $c$ $\vdash \exists x \ P(x)$

$\forall x \ P(x)$ $\vdash P(a)$ for any $a$
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.

1.4. $P(a)$
1.5. $\exists x \ P(x)$  Intro $\exists$: 1.4

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.

1.4. $P(a)$ Elim $\forall$: 1.1
1.5. $\exists x \ P(x)$ Intro $\exists$: 1.4

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

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

• 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
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:

  Given the basic properties of arithmetic on integers, define:

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

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

Prove “There is an even prime number”
Formally: prove \( \exists x \ (\text{Even}(x) \land \text{Prime}(x)) \)
A Prime Example

### Domain of Discourse
Integers

### Predicate Definitions
- **Even(x)** := \( y \ (x = 2 \cdot y) \)
- **Odd(x)** := \( y \ (x = 2 \cdot y + 1) \)
- **Prime(x)** := “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. \( 2 = 2 \cdot 1 \) \quad Algebra
2. \( \exists y \ (2 = 2 \cdot y) \) \quad Intro \( \exists \): 1
3. **Even(2)** \quad Def of **Even**: 3
4. **Prime(2)** \quad Property of integers
5. **Even(2) \land Prime(2)** \quad Intro \( \land \): 2, 4
6. **\exists x \ (Even(x) \land Prime(x))** \quad Intro \( \exists \): 5

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

** Intro \( \exists \)

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

** Elim \( \forall \)

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

** Intro \( \forall \)

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

** Elim \( \exists \)

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

“Let a be arbitrary*”

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

** 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!

* in the domain of \( P \)
Even and Odd

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

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

Prove: “The square of any 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($x$) $\coloneqq \exists y \ (x=2y)$
Odd($x$) $\coloneqq \exists y \ (x=2y+1)$
Domain: Integers
Even and Odd

Prove: “The square of any 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. Even($a^2$)
   2. Even($a$)$\rightarrow$Even($a^2$) Direct proof rule
   3. $\forall x (\text{Even}(x)\rightarrow\text{Even}(x^2))$ Intro $\forall$: 1,2

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

Prove: “The square of any 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 \( \exists y \ (a^2 = 2y) \)
   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
Prove: “The square of any 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: 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

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

1. Let \( a \) be an arbitrary integer
   
   \hspace{1cm} 2.1 Even(\( a \)) \hspace{1.6cm} \text{Assumption}
   
   \hspace{1cm} 2.2 \exists y \ (a = 2y) \hspace{1cm} \text{Definition of Even}
   
   \hspace{1cm} 2.3 a = 2b \hspace{1.4cm} \text{Elim \( \exists \): \( b \)}
   
   \hspace{1cm} 2.5 \exists y \ (a^2 = 2y) \hspace{1.3cm} \text{Intro \( \exists \) rule: ?}
   
   \hspace{1cm} 2.6 \text{Even}(a^2) \hspace{1.6cm} \text{Definition of Even}

2. \text{Even}(a) \rightarrow \text{Even}(a^2) \hspace{1.5cm} \text{Direct proof rule}

3. \( \forall x \ (\text{Even}(x) \rightarrow \text{Even}(x^2)) \) \hspace{1.5cm} \text{Intro \( \forall \): 1,2}

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

Prove: “The square of any 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 $\exists$: $b$
   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
These rules need more caveats...

There are extra conditions on using these rules:

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

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

  * 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. \[ \exists y \ (y \geq a) \] Elim ∀: 1
4. \[ b \geq a \] Elim ∃: b
5. \[ \forall x \ (b \geq x) \] Intro ∀: 2,4
6. \[ \exists y \forall x \ (y \geq x) \] Intro ∃: 5
These rules need more caveats...

There are extra conditions on using these rules:

“Let a be arbitrary*”...P(a)

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

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

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

* 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. \( \exists y \ (y \geq a) \) Elim \( \forall\): 1
4. \( b \geq a \) Elim \( \exists\): b
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!
These rules need more caveats...

There are extra conditions on using these rules:

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

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

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

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

\[ \text{Intro } \exists \]

**P(c) for some c**
\[ \therefore \exists x \ P(x) \]

**Elim \(\forall\)**

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

\[ \text{Intro } \exists \]

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

**Elim \(\exists\)**

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

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

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

**“Let a be arbitrary”**...
- * in the domain of P. No other name in P depends on a
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.