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.
Last class: Propositional Inference Rules

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

\[ \text{Elim} \land \quad A \land B \quad \therefore A, B \]

\[ \text{Intro} \land \quad A ; B \quad \therefore A \land B \]

\[ \text{Elim} \lor \quad A \lor B ; \neg A \quad \therefore B \]

\[ \text{Intro} \lor \quad A \quad \therefore A \lor B, B \lor A \]

\[ \text{Modus Ponens} \quad A ; A \rightarrow B \quad \therefore B \]

\[ \text{Direct Proof Rule} \quad A \Rightarrow B \quad \therefore A \rightarrow B \]

Not like other rules
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

1.4.1. \( p \) 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

### Intro $\exists$

- **Premise:** $P(c)$ for some $c$
- **Conclusion:** $\exists x \ P(x)$

### Elim $\forall$

- **Premise:** $\forall x \ P(x)$
- **Conclusion:** $P(a)$ for any $a$

### Intro $\forall$

- **Premise:** "Let $a$ be arbitrary*" ... $P(a)$
- **Conclusion:** $\forall x \ P(x)$

### Elim $\exists$

- **Premise:** $\exists x \ P(x)$
- **Conclusion:** $P(c)$ 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!
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

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

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

That requires \( P(c) \) for some \( c \).

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

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

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

\[\begin{align*}
1.1. \quad & \forall x \, P(x) \quad \text{Assumption} \\
1.2 \quad & P(a) \quad \text{Elim } \forall: 1.1
\end{align*}\]

We could have picked any name or domain expression here.

\[\begin{align*}
1.5. \quad & \exists x \, P(x) \quad \text{Intro } \exists: \text{?}
\end{align*}\]

That requires \( P(c) \) for some \( c \).

\[\begin{align*}
1. \quad & \forall x \, P(x) \rightarrow \exists x \, P(x) \quad \text{Direct Proof Rule}
\end{align*}\]
My First Predicate Logic Proof

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

No holes. Just need to clean up.

1. $\forall x P(x)$ Assumption
2. $P(a)$ Elim $\forall$: 1.1

5. $\exists x P(x)$ Intro $\exists$: 1.2
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. $P(a)$ Elim $\forall$: 1.1
3. $\exists x P(x)$ Intro $\exists$: 1.2

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 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:

<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) ≡ ∃y (x = 2⋅y)</td>
</tr>
<tr>
<td>Odd(x) ≡ ∃y (x = 2⋅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) ≡ ∃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)
A Not so Odd Example

Domain of Discourse | Predicate Definitions
--- | ---
Integers | 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

<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>
<tr>
<td></td>
<td>Prime(x) ≡ “x &gt; 1 and x≠a⋅b for all integers a, b with 1&lt;a&lt;x”</td>
</tr>
</tbody>
</table>

Prove “There is an even prime number”
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) ≡ ∃y (x = 2⋅y)</td>
</tr>
<tr>
<td></td>
<td>Odd(x) ≡ ∃y (x = 2⋅y + 1)</td>
</tr>
<tr>
<td></td>
<td>Prime(x) ≡ “x &gt; 1 and x≠a⋅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 ∃x (Even(x) ∧ 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

<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) ≡ ∃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

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

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

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

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

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

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

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

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

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

Elim \∃ \quad \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. Even(a)→Even(a^2)

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

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

---

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

Formal proof of: ∀x (Even(x) → Even(x²))

1. Let a be an arbitrary integer
   2.1 Even(a) Assumption

   2.6 Even(a²)

2. Even(a) → Even(a²) Direct proof rule

3. ∀x (Even(x) → Even(x²)) Intro ∀: 1,2

---

Even a be arbitrary*”...P(a)  
∀x P(x)  
∃x P(x) for some special** c
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

\[
\begin{align*}
2.5 & \quad \exists y \ (a^2 = 2y) \\
2.6 & \quad \text{Even}(a^2) \\
\end{align*}
\]

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

Exercises

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

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

1. Let \( a \) be an arbitrary integer
   2.1 \( \text{Odd}(a) \) Assumption
   2.2 \( \exists y \ (a = 2y + 1) \) Definition of Odd

\[
\begin{align*}
2.5 & \quad \exists y \ (a^2 = 2y + 1) \\
2.6 & \quad \text{Odd}(a^2) \\
\end{align*}
\]

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

“Let a be arbitrary*”...P(a)  ∴  ∀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(x²))

1. Let a be an arbitrary integer
   2.1  Even(a)  Assumption
   2.2  ∃y (a = 2y)  Definition of Even
       
       2.5  ∃y (a² = 2y)  Intro ∃ rule:  
       2.6  Even(a²)  Definition of Even
       
       2.  Even(a)→Even(a²)  Direct proof rule
       3.  ∀x (Even(x)→Even(x²))  Intro ∀: 1,2

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

Domain: Integers

* Intro ∀
** Elim ∃
*** c

Need a² = 2c for some c
Even and Odd

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

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

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

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 \( \text{Even}(a) \)  
       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: \( ? \)

   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 Even($a$) \hspace{1cm} Assumption
   - 2.2 $\exists y \ (a = 2y)$ \hspace{1cm} Definition of Even
   - 2.3 $a = 2b$ \hspace{1cm} Elim $\exists$: $b$ special depends on $a$
   - 2.4 $a^2 = 4b^2 = 2(2b^2)$ \hspace{1cm} Algebra
   - 2.5 $\exists y \ (a^2 = 2y)$ \hspace{1cm} Intro $\exists$ rule
   - 2.6 Even($a^2$) \hspace{1cm} Definition of Even

2. Even($a$)$\rightarrow$Even($a^2$) \hspace{1cm} Direct proof rule

3. $\forall x \ (\text{Even}(x) \rightarrow \text{Even}(x^2))$ \hspace{1cm} Intro $\forall$: 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)  
\[ \forall x \ P(x) \]  

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

* 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 \( \exists \): \( b \) 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:

\[
\text{Intro } \forall: \quad \text{Let a be arbitrary*}\ldots P(a)
\]

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

\[
\exists x P(x)
\]

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

* 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 \( \exists: b \) 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:

- "Let \( a \) be arbitrary*"... \( P(a) \)
  
  \[
  \therefore \quad \forall x \ P(x)
  \]

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

* 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. \( \forall x \exists y \ (y \geq x) \) 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

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

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

“Let } a \text{ be arbitrary}^{*} \ldots P(a) \quad \therefore \quad \forall x \ P(x) \]

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

---

* 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.
An English Proof

Prove “There is an even integer”

Proof:

1. $2 = 2 \cdot 1$  
   2. $\exists y \ (2 = 2 \cdot y)$  
      Intro $\exists$: 1  
   3. $\text{Even}(2)$  
      Defn of Even: 2  
   4. $\exists x \ \text{Even}(x)$  
      Intro $\exists$: 3

Therefore, there is an even integer $\blacksquare$
Prove “The square of every even integer is even.”

Proof: Let $a$ be an arbitrary even integer.

1. Let $a$ be an arbitrary integer. [Assumption]

2.1 $\text{Even}(a)$

Then, by definition, $a = 2b$ for some integer $b$ (depending on $a$).

2.2 $\exists y \ (a = 2y)$ [Definition]

2.3 $a = 2b$ [Definition]

$b$ special depends on $a$

2.4 $a^2 = 4b^2 = 2(2b^2)$ [Algebra]

Squaring both sides, we get $a^2 = 4b^2 = 2(2b^2)$.

2.5 $\exists y \ (a^2 = 2y)$ [Definition]

Since $2b^2$ is an integer, by definition, $a^2$ is even.

2.6 $\text{Even}(a^2)$ [Definition]

Since $a$ was arbitrary, it follows that the square of every even number is even. □
Even and Odd

 Predicate Definitions

<table>
<thead>
<tr>
<th>Even(x) $\equiv \exists y$ $(x = 2y)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Odd(x) $\equiv \exists y$ $(x = 2y + 1)$</td>
</tr>
</tbody>
</table>

 Domain of Discourse

 Integers

Prove “The square of every odd number is odd.”
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