...let's assume there exists some function $F(x_0, x_1, ...)$ 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: My First Proof!

Show that $r$ follows from $p$, $p \rightarrow q$, and $q \rightarrow r$

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

Modus Ponens \[ A ; A \rightarrow B \]
\[ \therefore B \]
Last class: Proofs can use equivalences too

Show that \( \neg p \) follows from \( p \rightarrow q \) and \( \neg q \)

1. \( p \rightarrow q \)  
   Given

2. \( \neg q \)  
   Given

3. \( \neg q \rightarrow \neg p \)  
   Contrapositive: 1

4. \( \neg p \)  
   MP: 2, 3

Modus Ponens  
\[ \begin{array}{c}
A ; A \rightarrow B \\
\therefore B
\end{array} \]
Last class: Propositional Inference Rules

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

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

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

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

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

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

\[
\text{Direct Proof} \quad \frac{A \Rightarrow B}{\therefore A \to B}
\]
Proofs

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

How To Start:
We have givens, find the ones that go together and use them. Now, treat new things as givens, and repeat.

\[ A ; A \rightarrow B \]
\[ \therefore B \]

\[ A \land B \]
\[ \therefore A, B \]

\[ A ; B \]
\[ \therefore A \land B \]
Proofs

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

1. \( p \) \hspace{1cm} Given
2. \( p \rightarrow q \) \hspace{1cm} Given
3. \( (p \land q) \rightarrow r \) \hspace{1cm} Given

\[
A \, A \rightarrow B \\
\therefore B
\]

\[
A \land B \\
\therefore A, B
\]

9. \( r \) \hspace{1cm} ??

\[
A \, B \\
\therefore A \land B
\]
Proofs

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

1. \( p \)  
   Given

2. \( p \rightarrow q \)  
   Given

3. \( q \)  
   MP: 1, 2

4. \( p \land q \)  
   Intro \( \land \): 1, 3

5. \( (p \land q) \rightarrow r \)  
   Given

6. \( r \)  
   MP: 4, 5
Prove that \( \neg r \) follows from \( p \land s \), \( q \to \neg r \), and \( \neg s \lor q \).

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>( p \land s )</td>
<td>Given</td>
</tr>
<tr>
<td>2.</td>
<td>( q \to \neg r )</td>
<td>Given</td>
</tr>
<tr>
<td>3.</td>
<td>( \neg s \lor q )</td>
<td>Given</td>
</tr>
</tbody>
</table>

**Idea: Work backwards!**

First: Write down givens and goal.
Prove that \( \neg r \) follows from \( p \land s \), \( q \rightarrow \neg r \), and \( \neg s \lor q \).

Proofs

1. \( p \land s \) Given

2. \( q \rightarrow \neg r \) Given

3. \( \neg s \lor q \) Given

Idea: Work backwards!

We want to eventually get \( \neg r \). How?

- We can use \( q \rightarrow \neg r \) to get there.
- The justification between 2 and 20 looks like “elim \( \rightarrow \)” which is MP.

20. \( \neg r \) MP: 2, ?
Prove that \( \neg r \) follows from \( p \land s \), \( q \rightarrow \neg r \), and \( \neg s \lor q \).

1. \( p \land s \)  Given
2. \( q \rightarrow \neg r \)  Given
3. \( \neg s \lor q \)  Given

Idea: Work backwards!

We want to eventually get \( \neg r \). How?
- Now, we have a new “hole”
- We need to prove \( q \)...
  - Notice that at this point, if we prove \( q \), we’ve proven \( \neg r \)...

19. \( q \)  ?
20. \( \neg r \)  MP: 2, 19
Prove that $\neg r$ follows from $p \land s$, $q \rightarrow \neg r$, and $\neg s \lor q$.

1. $p \land s$  Given
2. $q \rightarrow \neg r$  Given
3. $\neg s \lor q$  Given

\[ \text{This looks like or-elimination.} \]

19. $q$  ?
20. $\neg r$  MP: 2, 19

\[ \text{Elim } A \lor B ; \neg A \quad \therefore B \]
Prove that \( \neg r \) follows from \( p \land s \), \( q \rightarrow \neg r \), and \( \neg s \lor q \).

1. \( p \land s \) Given
2. \( q \rightarrow \neg r \) Given
3. \( \neg s \lor q \) Given

18. \( \neg \neg s \) \( \neg \neg s \) doesn’t show up in the givens but \( s \) does and we can use equivalences
19. \( q \lor \) Elim: 3, 18
20. \( \neg r \) MP: 2, 19
Prove that \(\neg r\) follows from \(p \land s\), \(q \rightarrow \neg r\), and \(\neg s \lor q\).

1. \(p \land s\)  Given
2. \(q \rightarrow \neg r\)  Given
3. \(\neg s \lor q\)  Given

17. \(s\)

18. \(\neg \neg s\)  Double Negation: 17

19. \(q\)  \lor Elim: 3, 18

20. \(\neg r\)  MP: 2, 19
Prove that \( \neg r \) follows from \( p \land s \), \( q \rightarrow \neg r \), and \( \neg s \lor q \).

Proofs

Given

1. \( p \land s \)
2. \( q \rightarrow \neg r \)
3. \( \neg s \lor q \)

17. \( s \) \hspace{1cm} \land \text{ Elim: 1}
18. \( \neg \neg s \) \hspace{1cm} \text{Double Negation: 17}
19. \( q \) \hspace{1cm} \lor \text{ Elim: 3, 18}
20. \( \neg r \) \hspace{1cm} \text{MP: 2, 19}

No holes left! We just need to clean up a bit.
Proofs

Prove that \( \neg r \) follows from \( p \land s \), \( q \rightarrow \neg r \), and \( \neg s \lor q \).

1. \( p \land s \) Given
2. \( q \rightarrow \neg r \) Given
3. \( \neg s \lor q \) Given
4. \( s \) \( \land \) Elim: 1
5. \( \neg \neg s \) Double Negation: 4
6. \( q \) \( \lor \) Elim: 3, 5
7. \( \neg r \) MP: 2, 6
Important: Applications of Inference Rules

• You can use **equivalences** to make substitutions of any sub-formula.

  e.g. \((p \rightarrow r) \lor q \equiv (\neg p \lor r) \lor q\)

• **Inference rules only** can be applied to whole formulas (not correct otherwise).

  e.g. 1. \(p \rightarrow r\)  given

      2. \((p \lor q) \rightarrow r\)  intro \(\lor\) from 1.

  Does not follow! e.g. \(p=F, q=T, r=F\)
Last class: Propositional Inference Rules

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

- **Elim \( \land \)**
  \[
  \begin{array}{c}
  A \land B \\
  \hline
  \therefore A, B
  \end{array}
  \]

- **Intro \( \land \)**
  \[
  \begin{array}{c}
  A \land B \\
  \hline
  \therefore A, B
  \end{array}
  \]

- **Elim \( \lor \)**
  \[
  \begin{array}{c}
  A \lor B ; \neg A \\
  \hline
  \therefore B
  \end{array}
  \]

- **Intro \( \lor \)**
  \[
  \begin{array}{c}
  A \\
  \hline
  \therefore A \lor B, B \lor A
  \end{array}
  \]

- **Modus Ponens**
  \[
  \begin{array}{c}
  A ; A \rightarrow B \\
  \hline
  \therefore B
  \end{array}
  \]

- **Direct Proof**
  \[
  \begin{array}{c}
  A \Rightarrow B \\
  \hline
  \therefore A \rightarrow B
  \end{array}
  \]

Not like other rules
Last class: New Perspective

Rather than comparing A and B as columns, zooming in on just the rows where A is true:

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$A$</th>
<th>$B$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td></td>
</tr>
</tbody>
</table>

Given that A is true, we see that B is also true.

$A \supseteq B$
Rather than comparing $A$ and $B$ as columns, zooming in on just the rows where $B$ is true:

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$A$</th>
<th>$B$</th>
<th>$A \rightarrow B$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

When we zoom out, what have we proven?

$$(A \rightarrow B) \equiv T$$
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
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. $r$ ??
3.3. $r$ ??

3. $p \rightarrow r$ Direct Proof

If we know $p$ is true...
Then, we’ve shown $r$ is true
Proofs using the direct proof rule

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

1. \( q \) \hspace{1cm} Given
2. \((p \land q) \rightarrow r\) \hspace{1cm} Given
   
   3.1. \( p \) \hspace{1cm} Assumption
   
   3.2. \( p \land q \) \hspace{1cm} Intro \( \land \): 1, 3.1
   
   3.3. \( r \) \hspace{1cm} MP: 2, 3.2

3. \( p \rightarrow r \) \hspace{1cm} Direct Proof
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: \((p \land q) \rightarrow (p \lor q)\)

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

1.9. \(p \lor q\) \hspace{1cm} ??

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

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

1.1. \(p \land q\) Assumption
1.2. \(p\) Elim \(\land\): 1.1
1.3. \(p \lor q\) Intro \(\lor\): 1.2

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

1.4.1. \(p\) Assumption

1.4.? \(r\)

1.4. \(p \rightarrow r\) Direct Proof

1. \(((p \rightarrow q) \land (q \rightarrow r)) \rightarrow (p \rightarrow r)\) Direct Proof
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
1.4.1. $p$ 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
1. $(p \rightarrow q) \land (q \rightarrow r) \rightarrow (p \rightarrow r)$ Direct Proof
Inference Rules for Quantifiers: First look

** 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!

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

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

\[ \exists x \ P(x) \]
\[ \therefore \ P(c) \quad \text{for some special** c} \]
My First Predicate Logic Proof

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

The main connective is implication so Direct Proof seems good

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

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

1.5. $\exists x \, P(x)$

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

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

1. $\forall x \ P(x)$ Assumption

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

1.5. $\exists x \ P(x)$ Intro $\exists$: $\square$ That requires $P(c)$ for some $c$.

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

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

1. $\forall x \, P(x)$ Assumption
2. $P(5)$ Elim $\forall$: 1.1

1.5. $\exists x \, P(x)$ Intro $\exists$: That requires $P(c)$ for some $c$.

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

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

1. $\forall x \ P(x)$ Assumption
2. $P(5)$ Elim $\forall$: 1.1

1.5. $\exists x \ P(x)$ Intro $\exists$: 1.2

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

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

1. \( \forall x \ P(x) \quad \) Assumption
2. \( P(5) \quad \) Elim \( \forall \): 1.1
3. \( \exists x \ P(x) \quad \) Intro \( \exists \): 1.2

Direct Proof

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:

<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\cdot y)</td>
</tr>
<tr>
<td>Odd(x) := ∃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\cdot y)</td>
</tr>
<tr>
<td></td>
<td>Odd(x) := ∃y (x = 2\cdot y + 1)</td>
</tr>
</tbody>
</table>

Prove “There is an even number”
Formally: prove ∃x Even(x)

1. 2 = 2 \cdot 1          Algebra
2. ∃y (2 = 2 \cdot 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></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))
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) := ∃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. $2 = 2 \cdot 1$  
   **Algebra**

2. $∃y (2 = 2 \cdot y)$  
   **Intro $∃$: 1**

3. Even(2)  
   **Def of Even: 3**

4. Prime(2)  
   **Property of integers**

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**

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

- **Intro \( \exists \)**

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

- **\( \exists \)**

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

**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!**

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

- **Elim \( \forall \)**

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

**“Let a be arbitrary*”...P(a)**

**in the domain of P**
Even and Odd

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

Prove: “The square of any even number is even.”
Formal proof of: ∀x (Even(x) → Even(x²))
Even and Odd

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

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

1. Let \( a \) be an arbitrary integer

2. \( Even(a) \rightarrow Even(a^2) \)
3. \( \forall x (Even(x) \rightarrow Even(x^2)) \)

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

   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
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. $\text{Even}(a) \rightarrow \text{Even}(a^2)$ Direct Proof
   
   2.5 $\exists y \ (a^2 = 2y)$
   2.6 $\text{Even}(a^2)$ Definition of Even

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

“Let a be arbitrary*”...P(a) | Elim ∃ | ∃x P(x)
---|---|---
| ∴ ∀x P(x) | ∴ P(c) for some special** c

Prove: “The square of any 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

   2.5 ∃y (a^2 = 2y) Intro ∃: (?) Need a^2 = 2c for some c
   2.6 Even(a^2) Definition of Even

2. Even(a)→Even(a^2) Direct proof
3. ∀x (Even(x)→Even(x^2)) Intro ∀: 1,2

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

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

Prove: “The square of any 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
   2.3 a = 2b Elim ∃: b

   2.5 ∃y (a² = 2y) Intro ∃: ?
   2.6 Even(a²) Definition of Even

2. Even(a)→Even(a²) Direct proof

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

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

“Let a be arbitrary**”...P(a)  ∴  ∀x P(x)  ∴  P(c) for some special**  c

Prove: “The square of any 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

2.3  a = 2b  Elim ∃: b

2.4  a² = 4b² = 2(2b²)  Algebra

2.5  ∃y (a² = 2y)  Intro ∃

2.6  Even(a²)  Definition of Even

2.  Even(a) → Even(a²)  Direct Proof

3.  ∀x (Even(x) → Even(x²))  Intro ∀: 1,2
These rules need more caveats...

There are extra conditions on using these rules:

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

- **Elim ∃** ∃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. \( \forall x \ \exists y \ (y \geq x) \) \hspace{1cm} Given
2. Let \( a \) be an arbitrary integer
3. \( \exists y \ (y \geq a) \) \hspace{1cm} Elim \( \forall \) : 1
4. \( b \geq a \) \hspace{1cm} Elim \( \exists \) : \( b \)
5. \( \forall x \ (b \geq x) \) \hspace{1cm} Intro \( \forall \) : 2,4
6. \( \exists y \forall x \ (y \geq x) \) \hspace{1cm} Intro \( \exists \) : 5
These rules need more caveats...

There are extra conditions on using these rules:

\[ \forall x \exists y \ (y \geq x) \] 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:

- “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. 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

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

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

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

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

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

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

* 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.