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: Inference Rules for Quantifiers

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

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

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

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

** 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!.
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  \( \exists x \) 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. \(2 = 2 \cdot 1\) \hspace{1cm} Algebra
2. ∃y (2 = 2 \cdot y) \hspace{1cm} Intro ∃: 1
3. Even(2) \hspace{1cm} Definition of Even: 2
4. ∃x Even(x) \hspace{1cm} 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) := “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 \( \exists x \ (\text{Even}(x) \land \text{Prime}(x)) \)
A Prime Example

**Predicate Definitions**

- **Integers**
- **Domain of Discourse**
- **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  
   \[ \text{Algebra} \]
2. ∃y (2 = 2⋅y)  
   \[ \text{Intro } ∃: 1 \]
3. Even(2)  
   \[ \text{Def of Even: 3} \]
4. Prime(2)*  
   \[ \text{Property of integers} \]
5. Even(2) ∧ Prime(2)  
   \[ \text{Intro } ∧: 2, 4 \]
6. ∃x (Even(x) ∧ Prime(x))  
   \[ \text{Intro } ∃: 5 \]

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

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

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

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

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

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

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

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

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

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

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

"Let a be arbitrary*" \ldots P(a)

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

** c is a NEW name.

* 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(x^2))

3. ∀x (Even(x)→Even(x^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. \( \text{Even}(a) \rightarrow \text{Even}(a^2) \)

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

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

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 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

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

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 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

   2.5 ∃y (a² = 2y) Intro ∃: Need a² = 2c for some c
   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)

1. Let a be an arbitrary integer

2. Even(a)

2.1 Assumption

2.2 Even(a) → Even(a^2)

2.5 ∃y (a^2 = 2y)

2.6 Even(a^2)

2. Even(a) → Even(a^2)

3. ∀x (Even(x) → Even(x^2))

3. ∀x (Even(x) → Even(x^2))

Intro ∀: 1,2

Need a^2 = 2c for some c

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(x^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
   2.3 $a = 2b$ Elim $\exists: b$
   2.4 $a^2 = 4b^2 = 2(2b^2)$ Algebra
   2.5 $\exists y \ (a^2 = 2y)$ Intro $\exists$
   2.6 $\text{Even}(a^2)$ Definition of Even

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
These rules need some caveats...

There are extra conditions on using these rules:

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

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

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

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

Without those rules, it is possible to infer claims that are false
Without the rules, one could infer false claims...

There are extra conditions on using these rules:

1. ∀x ∃y (y ≠ x)  

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

∴ ∀x P(x)  

3. ∃x P(x)  

∴ P(c) for some special** c  

* in the domain of P  

** c has to be a NEW name.

Over integer domain: ∀x ∃y (y ≠ x) is True but ∃y∀x (y ≠ x) is False

BAD “PROOF”

1. ∀x ∃y (y ≠ x)  

   Given

2. Let a be an arbitrary integer

3. ∃y (y ≠ a)  

   Elim ∀: 1

4. b ≠ a  

   Elim ∃: 3 (b new constant)

5. ∀x (b ≠ x)  

   Intro ∀: 2,4

6. ∃y∀x (y ≠ x)  

   Intro ∃: 5
With the extra conditions we can kill the bad proof...

There are extra conditions on using these rules:

Over integer domain: $\forall x \exists y (y \neq x)$ is True but $\exists y \forall x (y \neq x)$ is False

BAD “PROOF” KILLED

1. $\forall x \exists y (y \neq x)$ Given
2. Let $a$ be an arbitrary integer
3. $\exists y (y \neq a)$ Elim $\forall$: 1
4. $b \neq a$ Elim $\exists$: 3 ($b$ depends on $a$)
5. $\forall x (b \neq x)$ Intro $\forall$: 2, 4
6. $\exists y \forall x (y \neq x)$ 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

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

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

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

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

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

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

• In principle, formal proofs are the standard for what it means to be “proven” in mathematics
  – almost all math (and theory CS) done in Predicate Logic

• But they are tedious and impractical
  – e.g., applications of commutativity and associativity
  – Russell & Whitehead’s formal proof that $1+1 = 2$
    appears after more than 100 pages of build up
  – we allowed ourselves to cite “Arithmetic”, “Algebra”, etc.

• Similar situation exists in programming...
a := ADD(i, 1)
b := MOD(a, n)
c := ADD(arr, b)
d := LOAD(c)
e := ADD(arr, i)
STORE(e, d)

arr[i] = arr[(i+1) % n];
Programming vs Proofs

\[
\begin{align*}
 a & := \text{ADD}(i, 1) & \text{Given} \\
 b & := \text{MOD}(a, n) & \text{Given} \\
 c & := \text{ADD}(arr, b) & \text{Elim } \land: 1 \\
 d & := \text{LOAD}(c) & \text{Double Negation: 4} \\
 e & := \text{ADD}(arr, i) & \text{Elim } \lor: 3, 5 \\
 \text{STORE}(e, d) & & \text{Modus Ponens: 2, 6}
\end{align*}
\]

Assembly Language for Programs

Assembly Language for Proofs
what is the “Java” for proofs?

Given

\( \land \) Elim: 1

Double Negation: 4

\( \lor \) Elim: 3, 5

MP: 2, 6

Assembly Language for Proofs

High-level Language for Proofs
Proofs

Given

Given

∧ Elim: 1

Double Negation: 4

∨ Elim: 3, 5

MP: 2, 6

Assembly Language for Proofs

High-level Language for Proofs

English?
Proofs

Given
Given
\( \land \text{ Elim: 1} \)

Double Negation: 4
\( \lor \text{ Elim: 3, 5} \)

MP: 2, 6

Assembly Language for Proofs

High-level Language for Proofs

Math English
Proofs

• Formal proofs follow simple well-defined rules and should be easy for a machine to check
  – as assembly language is easy for a machine to execute

• English proofs correspond to those rules but are designed to be easier for humans to read
  – also easy to check with practice
    (almost all actual math and theory CS is done this way)
  – English proof is correct if the reader is convinced that
    they could translate it into a formal proof
    (the reader is the “compiler” for English proofs)
Formal Proof: 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 $\exists: b$ depends on $a$
   2.4 $a^2 = 4b^2 = 2(2b^2)$ Algebra
   2.5 $\exists y \ (a^2 = 2y)$ Intro $\exists$
   2.6 $\text{Even}(a^2)$ Definition of Even

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

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

Even($x$) $\equiv \exists y \ (x=2y)$
Odd($x$) $\equiv \exists y \ (x=2y+1)$
Domain: Integers
Prove “The square of every even integer is even.”

Let \( a \) be an arbitrary integer.

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

Suppose \( a \) is even.

2.1 \( \text{Even}(a) \) Assumption

2.2 \( \exists y \ (a = 2y) \) Definition

2.3 \( a = 2b \) Elim \( \exists: \) \( b \) depends on \( a \)

Then, by definition, \( a = 2b \) for some integer \( b \).

2.4 \( a^2 = 4b^2 = 2(2b^2) \) Algebra

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

2.5 \( \exists y \ (a^2 = 2y) \) Intro \( \exists \)

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

So \( a^2 \) is, by definition, even.

Since \( a \) was arbitrary, we have shown that the square of every even number is even.

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

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

Prove “The square of every even integer is even.”

**Proof:** Let \( a \) be an arbitrary integer.

Suppose \( a \) is even. Then, by definition, \( a = 2b \) for some integer \( b \). Squaring both sides, we get \( a^2 = 4b^2 = 2(2b^2) \). So \( a^2 \) is, by definition, is even.

Since \( a \) was arbitrary, we have shown that the square of every even number is even. ■
English Proof: Even and Odd

Prove “The square of every even integer is even.”

Proof: Let \( a \) be an arbitrary even integer.

Then, by definition, \( a = 2b \) for some integer \( b \). Squaring both sides, we get \( a^2 = 4b^2 = 2(2b^2) \). So \( a^2 \) is, by definition, is even.

Since \( a \) was arbitrary, we have shown that the square of every even number is even. □

\( \forall x \ (\text{Even}(x) \rightarrow \text{Even}(x^2)) \)
Prove "The sum of two odd numbers is even."

Formally, prove \( \forall x \forall y ((\text{Odd}(x) \land \text{Odd}(y)) \rightarrow \text{Even}(x+y)) \)
Prove “The sum of two odd numbers is even.”

Formally, prove  \( \forall x \forall y ((\text{Odd}(x) \land \text{Odd}(y)) \rightarrow \text{Even}(x+y)) \)

Let \( x \) and \( y \) be arbitrary integers.

1. Let \( x \) be an arbitrary integer
2. Let \( y \) be an arbitrary integer

Since \( x \) and \( y \) were arbitrary, the sum of two odd integers is even.

3. \( (\text{Odd}(x) \land \text{Odd}(y)) \rightarrow \text{Even}(x+y) \)
4. \( \forall y ((\text{Odd}(x) \land \text{Odd}(y)) \rightarrow \text{Even}(x+y)) \)  \( \) Intro \( \forall \)
5. \( \forall x \forall y ((\text{Odd}(x) \land \text{Odd}(y)) \rightarrow \text{Even}(x+y)) \)  \( \) Intro \( \forall \)
Prove “The sum of two odd numbers is even.”

Formally, prove $\forall x \forall y ((\text{Odd}(x) \land \text{Odd}(y)) \rightarrow \text{Even}(x+y))$

Let $x$ and $y$ be arbitrary integers.

Suppose that both are odd.

so $x+y$ is even.

Since $x$ and $y$ were arbitrary, the sum of two odd integers is even.
Even and Odd

Prove “The sum of two odd numbers is even.”

Formally, prove \( \forall x \forall y ((\text{Odd}(x) \land \text{Odd}(y)) \rightarrow \text{Even}(x+y)) \)

Let \( x \) and \( y \) be arbitrary integers. Suppose that both are odd.

So \( x+y \) is even.

Since \( x \) and \( y \) were arbitrary, the sum of two odd integers is even.
English Proof: Even and Odd

Prove “The sum of two odd numbers is even.”

Let x and y be arbitrary integers.

1. Let \( x \) be an arbitrary integer
2. Let \( y \) be an arbitrary integer

Suppose that both are odd.

3.1 \( \text{Odd}(x) \land \text{Odd}(y) \) Assumption
3.2 \( \text{Odd}(x) \) Elim \( \land \): 3.1
3.3 \( \text{Odd}(y) \) Elim \( \land \): 3.1

Then, we have \( x = 2a+1 \) for some integer \( a \) and \( y = 2b+1 \) for some integer \( b \).

3.4 \( \exists z \ (x = 2z+1) \) Def of Odd: 3.2
3.5 \( x = 2a+1 \) Elim \( \exists \): 3.4: \( a \) depend \( x \)
3.6 \( \exists z \ (y = 2z+1) \) Def of Odd: 3.3
3.7 \( y = 2b+1 \) Elim \( \exists \): 3.6: \( b \) depend \( y \)

so \( x+y \) is, by definition, even.

3.9 \( \exists z \ (x+y = 2z) \) Intro \( \exists \): ?
3.10 \( \text{Even}(x+y) \) Def of Even

Since \( x \) and \( y \) were arbitrary, the sum of two odd integers is even.

3. \( (\text{Odd}(x) \land \text{Odd}(y)) \to \text{Even}(x+y) \) DPR
4. \( \forall y \ ((\text{Odd}(x) \land \text{Odd}(y)) \to \text{Even}(x+y)) \) Intro \( \forall \)
5. \( \forall x \forall y \ ((\text{Odd}(x) \land \text{Odd}(y)) \to \text{Even}(x+y)) \) Intro \( \forall \)
English Proof: Even and Odd

Prove “The sum of two odd numbers is even.”

Let x and y be arbitrary integers.

1. Let x be an arbitrary integer
2. Let y be an arbitrary integer

Suppose that both are odd.

3.1 Odd(x) \land Odd(y)  \text{ Assumption}
3.2 Odd(x)  \text{ Elim } \land: 3.1
3.3 Odd(y)  \text{ Elim } \land: 3.1

Then, we have x = 2a+1 for some integer a and y = 2b+1 for some integer b.

3.4 \exists z \ (x = 2z+1)  \text{ Def of Odd: 3.2}
3.5 x = 2a+1  \text{ Elim } \exists: 3.4: a \text{ depend } x
3.6 \exists z \ (y = 2z+1)  \text{ Def of Odd: 3.3}
3.7 y = 2b+1  \text{ Elim } \exists: 3.6: b \text{ depend } y

Their sum is x+y = ... = 2(a+b+1)

3.8 x+y = 2(a+b+1)  \text{ Algebra: 3.5, 3.7}
3.9 \exists z \ (x+y = 2z)  \text{ Intro } \exists: 3.8
3.10 Even(x+y)  \text{ Def of Even}

Since x and y were arbitrary, the sum of two odd integers is even.

3. (Odd(x) \land Odd(y)) \rightarrow Even(x+y)  \text{ DPR}
4. \forall y ((Odd(x) \land Odd(y)) \rightarrow Even(x+y))  \text{ Intro } \forall
5. \forall x \forall y ((Odd(x) \land Odd(y)) \rightarrow Even(x+y))  \text{ Intro } \forall
Prove “The sum of two odd numbers is even.”

Proof: Let \( x \) and \( y \) be arbitrary integers.

Suppose that both are odd. Then, we have \( x = 2a+1 \) for some integer \( a \) and \( y = 2b+1 \) for some integer \( b \). Their sum is \( x+y = (2a+1) + (2b+1) = 2a+2b+2 = 2(a+b+1) \), so \( x+y \) is, by definition, even.

Since \( x \) and \( y \) were arbitrary, the sum of any two odd integers is even. \( \blacksquare \)
Even and Odd

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

Prove “The sum of two odd numbers is even.”

Proof: Let x and y be arbitrary odd integers.

Then, x = 2a+1 for some integer a and y = 2b+1 for some integer b. Their sum is x+y = (2a+1) + (2b+1) = 2a+2b+2 = 2(a+b+1), so x+y is, by definition, even. Since x and y were arbitrary, the sum of any two odd integers is even.

∀x ∀y ((Odd(x) ∧ Odd(y)) → Even(x+y))