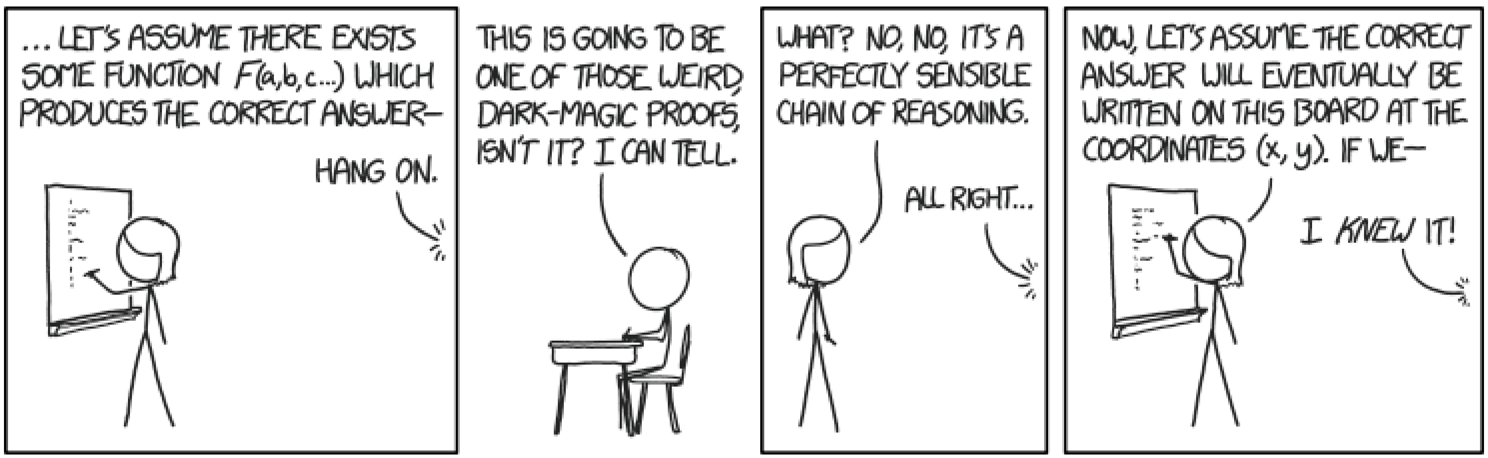
CSE 311: Foundations of Computing

Lecture 7: Propositional & Predicate Logic Proofs



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 $\dfrac{A\ ;\ A \rightarrow B}{\therefore\ B}$

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 $\dfrac{A \,;\, A \rightarrow B}{\therefore\ B}$

Last class: Propositional Inference Rules

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

Elim ∧
$$\frac{A \wedge B}{\therefore A,\ B}$$

Intro ∧
$$\frac{A\ ;\ B}{\therefore A \wedge B}$$

Elim ∨
$$\frac{A \vee B\ ;\ \neg A}{\therefore B}$$

Intro ∨
$$\frac{A}{\therefore A \vee B,\ B \vee A}$$

Modus Ponens
$$\frac{A\ ;\ A \rightarrow B}{\therefore B}$$

Direct Proof
$$\frac{A \Rightarrow B}{\therefore A \rightarrow B}$$

Proofs

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

How To Start:

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

$$\frac{A \; ; \; A \rightarrow B}{\therefore \; B}$$

$$\frac{A \wedge B}{\therefore \; A, B}$$

$$\frac{A \; ; \; B}{\therefore \; A \wedge B}$$

Proofs

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

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

9. r ??

$$\frac{A \;;\; A \rightarrow B}{\therefore\ B}$$

$$\frac{A \wedge B}{\therefore\ A,\ B}$$

$$\frac{A \;;\; B}{\therefore\ A \wedge B}$$

Proofs

Show that r follows from $p, p \to q$, and $(p \wedge q) \to r$

1.	p	Given
2.	$p \to q$	Given
3.	q	MP: 1, 2
4.	$p \wedge q$	Intro $\wedge$: 1, 3
5.	$(p \wedge q) \to r$	Given
6.	r	MP: 4, 5

Two visuals of the same proof. We will use the top one, but if the bottom one helps you think about it, that's great!

$$\cfrac{\cfrac{p \quad ; \quad \cfrac{p \quad ; \quad p \to q}{q}\,\text{MP}}{p \wedge q}\,\text{Intro}\ \wedge \quad ; \quad (p \wedge q) \to r}{r}\,\text{MP}$$

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
20.	$\neg r$	?

<u>First: Write down givens and goal</u>

<u>Idea: Work backwards!</u>

Proofs

Prove that $\neg r$ follows from $p \wedge s$, $q \rightarrow \neg r$, and $\neg s \vee q$.

1.	$p \wedge s$	Given
2.	$q \rightarrow \neg r$	Given
3.	$\neg s \vee q$	Given
20.	$\neg r$	MP: 2, ?

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.

Proofs

Prove that $\neg r$ follows from $p \wedge s$, $q \rightarrow \neg r$, and $\neg s \vee q$.

1.	$p \wedge s$	Given
2.	$q \rightarrow \neg r$	Given
3.	$\neg s \vee q$	Given
19.	q	?
20.	$\neg r$	MP: 2, 19

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 $\neg r$...

Proofs

Prove that $\neg r$ follows from $p \wedge s$, $q \rightarrow \neg r$, and $\neg s \vee q$.

1.	$p \wedge s$	Given
2.	$q \rightarrow \neg r$	Given
3.	$\neg s \vee q$	Given
19.	q	?
20.	$\neg r$	MP: 2, 19

This looks like or-elimination.

Elim ∨ $\dfrac{A \vee B \,;\, \neg A}{\therefore B}$

Proofs

Prove that $\neg r$ follows from $p \wedge s$, $q \rightarrow \neg r$, and $\neg s \vee q$.

1. $p \wedge s$ Given
2. $q \rightarrow \neg r$ Given
3. $\neg s \vee q$ 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 $\vee$ Elim: 3, 18
20. $\neg r$ MP: 2, 19

Proofs

Prove that $\neg r$ follows from $p \wedge s$, $q \rightarrow \neg r$, and $\neg s \vee q$.

1.	$p \wedge s$	Given
2.	$q \rightarrow \neg r$	Given
3.	$\neg s \vee q$	Given
17.	s	
18.	$\neg\neg s$	Double Negation: 17
19.	q	$\vee$ Elim: 3, 18
20.	$\neg r$	MP: 2, 19

1. $p \wedge s$ Given
2. $q \rightarrow \neg r$ Given
3. $\neg s \vee q$ Given
17. s
18. $\neg\neg s$ Double Negation: 17
19. q $\vee$ Elim: 3, 18
20. $\neg r$ MP: 2, 19

Proofs

Prove that $\neg r$ follows from $p \wedge s$, $q \rightarrow \neg r$, and $\neg s \vee q$.

1.	$p \wedge s$	Given
2.	$q \rightarrow \neg r$	Given
3.	$\neg s \vee q$	Given
17.	s	$\wedge$ Elim: 1
18.	$\neg\neg s$	Double Negation: 17
19.	q	$\vee$ Elim: 3, 18
20.	$\neg r$	MP: 2, 19

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

Proofs

Prove that $\neg r$ follows from $p \wedge s$, $q \rightarrow \neg r$, and $\neg s \vee q$.

1.	$p \wedge s$	Given
2.	$q \rightarrow \neg r$	Given
3.	$\neg s \vee q$	Given
4.	s	$\wedge$ Elim: 1
5.	$\neg\neg s$	Double Negation: 4
6.	q	$\vee$ 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. $(p \rightarrow r) \vee q \equiv (\neg p \vee r) \vee q$

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

  e.g. 1. $p \rightarrow r$ given

  2. $\cancel{(p \vee q) \rightarrow r}$ ~~intro $\vee$ 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 ∧
$$\frac{A \wedge B}{\therefore A,\ B}$$

Intro ∧
$$\frac{A\ ;\ B}{\therefore A \wedge B}$$

Elim ∨
$$\frac{A \vee B\ ;\ \neg A}{\therefore B}$$

Intro ∨
$$\frac{A}{\therefore A \vee B,\ B \vee A}$$

Modus Ponens
$$\frac{A\ ;\ A \rightarrow B}{\therefore B}$$

Direct Proof
$$\frac{A \Rightarrow B}{\therefore A \rightarrow B}$$

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:

p	*q*	A	B
T	T	T	T
T	F	T	T
F	T	F	
F	F	F	

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

A ®B

Last class: New Perspective

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

p	q	A	B	$A \rightarrow B$
T	T	T	T	T
T	F	T	T	T
F	T	F	T	T
F	F	F	F	T

When we zoom out, what have we proven?

$$(A \rightarrow B) \equiv \mathbf{T}$$

To Prove An Implication: $A \rightarrow B$

$$\frac{A \Rightarrow B}{\therefore A \rightarrow B}$$

- 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 $(p \wedge q) \rightarrow r$

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

This is a proof of $p \rightarrow r$

3.1. p Assumption
3.2.
3.3. r ??

If we know p is true… Then, we've shown r is true

3. $p \rightarrow r$ Direct Proof

Proofs using the direct proof rule

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

1. q Given
2. $(p \wedge q) \rightarrow r$ Given
    - 3.1. p Assumption
    - 3.2. $p \wedge q$ Intro $\wedge$: 1, 3.1
    - 3.3. r MP: 2, 3.2
3. $p \rightarrow r$ Direct Proof

Example

Prove: $(p \land q) \to (p \lor q)$

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: $(p \wedge q) \rightarrow (p \vee q)$

1.1.	$p \wedge q$	Assumption
1.9.	$p \vee q$	??
1.	$(p \wedge q) \rightarrow (p \vee q)$	Direct Proof

Example

Prove: $(p \wedge q) \rightarrow (p \vee q)$

1.1.	$p \wedge q$	Assumption
1.2.	p	Elim $\wedge$: 1.1
1.3.	$p \vee q$	Intro $\vee$: 1.2
1.	$(p \wedge q) \rightarrow (p \vee q)$	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: $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$

Example

Prove: $((p \to q) \wedge (q \to r)) \to (p \to r)$

1.1. $(p \to q) \wedge (q \to r)$ Assumption

1.? $p \to r$

1. $\big((p \to q) \wedge (q \to r)\big) \to (p \to r)$ Direct Proof

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.? $p \to r$

1. $\big((p \to q) \land (q \to r)\big) \to (p \to r)$ Direct Proof

Example

Prove: $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$

1.1. $(p \rightarrow q) \wedge (q \rightarrow r)$ Assumption

1.2. $p \rightarrow q$ $\wedge$ Elim: 1.1

1.3. $q \rightarrow r$ $\wedge$ Elim: 1.1

1.4.1. p Assumption

1.4.? r

1.4. $p \rightarrow r$ Direct Proof

1. $\big((p \rightarrow q) \wedge (q \rightarrow r)\big) \rightarrow (p \rightarrow r)$ Direct Proof

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
1.4.2.	q	MP: 1.2, 1.4.1
1.4.3.	r	MP: 1.3, 1.4.2
1.4.	$p \to r$	Direct Proof
1.	$\big((p \to q) \land (q \to r)\big) \to (p \to r)$	Direct Proof

Inference Rules for Quantifiers: First look

Intro ∃

$$\frac{P(c) \text{ for some } c}{\therefore \quad \exists x\, P(x)}$$

Elim ∀

$$\frac{\forall x\, P(x)}{\therefore \quad P(a)} \quad \textbf{(for any } a\textbf{)}$$

Elim ∃

$$\frac{\exists x\, P(x)}{\therefore\ P(c) \textbf{ for some } \textbf{\textit{special}}^{**}\ c}$$

Intro ∀

** 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!

My First Predicate Logic Proof

Domain of Discourse
Integers

$$\text{Intro } \exists \quad \frac{P(c) \text{ for some } c}{\therefore \quad \exists x\, P(x)}$$

$$\text{Elim } \forall \quad \frac{\forall x\, P(x)}{\therefore \quad P(a) \textbf{ for any } a}$$

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 seems good

My First Predicate Logic Proof

Domain of Discourse
Integers

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

Intro $\exists$: $\dfrac{P(c) \text{ for some } c}{\therefore\ \exists x\ P(x)}$

Elim $\forall$: $\dfrac{\forall x\ P(x)}{\therefore\ P(a) \text{ for any } a}$

1.1. $\forall x\, P(x)$ 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

Domain of Discourse
Integers

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

Intro ∃: $\dfrac{P(c) \text{ for some } c}{\therefore\ \exists x\ P(x)}$

Elim ∀: $\dfrac{\forall x\ P(x)}{\therefore\ P(a) \text{ for any } a}$

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

We need an ∃ we don't have so "intro ∃" rule makes sense

1.5. $\exists x\ P(x)$ Intro ∃: ?

That requires P(c) for some c.

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

My First Predicate Logic Proof

Domain of Discourse
Integers

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

Intro ∃: $\dfrac{P(c) \text{ for some } c}{\therefore\ \exists x\, P(x)}$

Elim ∀: $\dfrac{\forall x\, P(x)}{\therefore\ P(a) \text{ for any } a}$

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

1.2. $P(5)$ Elim ∀: 1.1

We need an ∃ we don't have
so "intro ∃" rule makes sense

1.5. $\exists x\, P(x)$ Intro ∃: ?

That requires P(c)
for some c.

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

My First Predicate Logic Proof

Domain of Discourse
Integers

Intro ∃ $\dfrac{P(c) \text{ for some } c}{\therefore \quad \exists x\, P(x)}$

Elim ∀ $\dfrac{\forall x\, P(x)}{\therefore\; P(a) \text{ for any } a}$

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

1.1.	$\forall x\, P(x)$	Assumption
1.2.	$P(5)$	Elim ∀: 1.1
1.5.	$\exists x\, P(x)$	Intro ∃: 1.2
1.	$\forall x\, P(x) \rightarrow \exists x\, P(x)$	Direct Proof

My First Predicate Logic Proof

Intro $\exists$
$$\frac{P(c) \text{ for some } c}{\therefore\ \exists x\, P(x)}$$

Elim $\forall$
$$\frac{\forall x\, P(x)}{\therefore\ P(a) \text{ for any } a}$$

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

1.1.	$\forall x\, P(x)$	Assumption
1.2.	$P(5)$	Elim $\forall$: 1.1
1.3.	$\exists x\, P(x)$	Intro $\exists$: 1.2
1.	$\forall x\, P(x) \to \exists x\, P(x)$	Direct Proof

<u>Working forwards as well as backwards</u>:
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:

Domain of Discourse
Integers

- Given the basic properties of arithmetic on integers, define:

Predicate Definitions
$\text{Even}(x) := \exists y\ (x = 2 \cdot y)$
$\text{Odd}(x) := \exists y\ (x = 2 \cdot y + 1)$

A Not so Odd Example

Domain of Discourse
Integers

Predicate Definitions
Even(x) := $\exists y\ (x = 2 \cdot y)$
Odd(x) := $\exists y\ (x = 2 \cdot y + 1)$

Prove "There is an even number"

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

A Not so Odd Example

Domain of Discourse
Integers

Predicate Definitions
$\text{Even}(x) := \exists y\ (x = 2 \cdot y)$
$\text{Odd}(x) := \exists y\ (x = 2 \cdot y + 1)$

Prove "There is an even number"

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

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

A Prime Example

Domain of Discourse

Integers

Predicate Definitions

Even(x) := $\exists$y (x = 2·y)

Odd(x) := $\exists$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 $\exists x\,(\mathrm{Even}(x) \wedge \mathrm{Prime}(x))$

A Prime Example

Domain of Discourse
Integers

Predicate Definitions
$\text{Even}(x) := \exists y\,(x = 2\cdot y)$
$\text{Odd}(x) := \exists y\,(x = 2\cdot y + 1)$
$\text{Prime}(x) :=$ “$x > 1$ and $x \neq a\cdot b$ for all integers a, b with $1<a<x$”

Prove “There is an even prime number”

Formally: prove $\exists x\,(\text{Even}(x) \wedge \text{Prime}(x))$

1.	$\mathbf{2 = 2\cdot 1}$	**Algebra**
2.	$\exists y\,(\mathbf{2} = \mathbf{2}\cdot y)$	**Intro ∃: 1**
3.	$\text{Even}(\mathbf{2})$	**Def of** Even**: 3**
4.	$\text{Prime}(\mathbf{2})$*	**Property of integers**
5.	$\text{Even}(\mathbf{2}) \wedge \text{Prime}(\mathbf{2})$	**Intro ∧: 2, 4**
6.	$\exists x\,(\text{Even}(x) \wedge \text{Prime}(x))$	**Intro ∃: 5**

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

Inference Rules for Quantifiers: First look

Intro ∃

$$\frac{P(c) \text{ for some } c}{\therefore \quad \exists x\, P(x)}$$

Elim ∀

$$\frac{\forall x\, P(x)}{\therefore \quad P(a) \quad \textbf{(for any } a)}$$

Elim ∃

$$\frac{\exists x\, P(x)}{\therefore P(c) \textbf{ for some } \textbf{\textit{special}}{**}\ c}$$

Intro ∀

$$\frac{\text{“}\textbf{Let } a \textbf{ be arbitrary}^{*}\text{”}\ldots P(a)}{\therefore \quad \forall x\, P(x)}$$

** 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

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

Intro $\forall$	Elim $\exists$
"Let a be arbitrary*"...P(a) / $\therefore\ \forall x\ P(x)$	$\exists x\ P(x)$ / $\therefore$ P(c) **for some *special*** c

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

Even and Odd

Intro $\forall$	"Let a be arbitrary*"...P(a) / $\therefore$ $\forall$x P(x)	Elim $\exists$	$\exists$x P(x) / $\therefore$ P(c) for some *special*** c

Prove: "The square of any even number is even."

Formal proof of: $\forall x\,(\mathrm{Even}(x) \rightarrow \mathrm{Even}(x^2))$

1. Let **a** be an arbitrary integer

2. $\mathrm{Even}(\mathbf{a}) \rightarrow \mathrm{Even}(\mathbf{a}^2)$?
3. $\forall x\,(\mathrm{Even}(x) \rightarrow \mathrm{Even}(x^2))$ Intro $\forall$: 1,2

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

Even and Odd

Intro $\forall$: $\dfrac{\text{"Let } a \text{ be arbitrary*"} \ldots P(a)}{\therefore\ \forall x\, P(x)}$	Elim $\exists$: $\dfrac{\exists x\, P(x)}{\therefore\ P(c) \text{ for some special** } c}$

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

    2.6 Even($\mathbf{a}^2$) ?

2. Even(**a**)$\rightarrow$Even($\mathbf{a}^2$) Direct proof
3. $\forall x\, (\text{Even}(x)\rightarrow\text{Even}(x^2))$ Intro $\forall$: 1,2

Even and Odd

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

Intro $\forall$: "Let a be arbitrary*"...P(a) ∴ $\forall x\ P(x)$	Elim $\exists$: $\exists x\ P(x)$ ∴ P(c) for some *special*** c

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
   - 2.2 $\exists y\ (\mathbf{a} = 2y)$ — Definition of Even
   - 2.5 $\exists y\ (\mathbf{a}^2 = 2y)$ — ?
   - 2.6 Even($\mathbf{a}^2$) — Definition of Even
2. Even(**a**)$\rightarrow$Even($\mathbf{a}^2$) — Direct Proof
3. $\forall x\ (\text{Even}(x)\rightarrow\text{Even}(x^2))$ — Intro $\forall$: 1,2

Even and Odd

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

Intro $\forall$	Elim $\exists$
"Let a be arbitrary*"...P(a) / $\therefore\ \forall x\, P(x)$	$\exists x\, P(x)$ / $\therefore$ P(c) **for some *special***** c

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
   - 2.2 $\exists y\,(\mathbf{a} = 2y)$ — Definition of Even
   - 2.5 $\exists y\,(\mathbf{a}^2 = 2y)$ — Intro $\exists$: ?
   - 2.6 Even($\mathbf{a}^2$) — Definition of Even
2. Even(**a**)$\rightarrow$Even($\mathbf{a}^2$) — Direct proof
3. $\forall x\,(\text{Even}(x)\rightarrow\text{Even}(x^2))$ — Intro $\forall$: 1,2

Need $\mathbf{a}^2 = 2\mathbf{c}$ for some **c**

Even and Odd

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

Intro ∀	Elim ∃
$\dfrac{\text{"Let a be arbitrary*"...P(a)}}{\therefore \ \forall x\ P(x)}$	$\dfrac{\exists x\ P(x)}{\therefore\ P(c) \textbf{ for some } \textbf{\textit{special}**}\ c}$

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
   - 2.2 ∃y (**a** = 2y) — Definition of Even
   - 2.3 **a** = 2**b** — Elim ∃: **b**
   - 2.5 ∃y (**a**^{2} = 2y) — Intro ∃: ?
   - 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

Need **a**^{2} = 2c for some **c**

Even and Odd

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

Intro $\forall$: $\dfrac{\text{"Let } a \text{ be arbitrary*"} \ldots P(a)}{\therefore \quad \forall x\, P(x)}$	Elim $\exists$: $\dfrac{\exists x\, P(x)}{\therefore P(c) \text{ for some } \textit{special}^{**}\ c}$

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
2.2	$\exists y\ (a = 2y)$	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	Even(a^2)	Definition of Even

Used $a^2 = 2c$ for $c=2b^2$

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

These rules need more caveats...

There are extra conditions on using these rules:

Intro $\forall$

$$\frac{\text{"Let } a \text{ be arbitrary*"} \ldots P(a)}{\therefore \quad \forall x\, P(x)}$$

* in the domain of P

Elim $\exists$

$$\frac{\exists x\, P(x)}{\therefore P(c) \text{ for some } \textit{special}^{**}\ c}$$

** 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**
5.	$\forall x\, (b \geq x)$	Intro $\forall$: **2,4**
6.	$\exists y \forall x\, (y \geq x)$	Intro $\exists$: **5**

These rules need more caveats…

There are extra conditions on using these rules:

Intro ∀: "Let a be arbitrary*"…P(a) ∴ $\forall x\, P(x)$

* in the domain of P

Elim ∃: $\exists x\, P(x)$ ∴ P(c) for some *special*** c

** c has to be a NEW name.

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

BAD "PROOF"

1. $\forall x\, \exists y\, (y \ge x)$ Given
2. **Let a be an arbitrary integer**
3. $\exists y\, (y \ge \mathbf{a})$ Elim ∀: **1**
4. $\mathbf{b} \ge \mathbf{a}$ Elim ∃: **b**
5. $\forall x\, (\mathbf{b} \ge x)$ Intro ∀: **2,4**
6. $\exists y \forall x\, (y \ge x)$ Intro ∃ : **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:

Intro $\forall$: "Let a be arbitrary*"…P(a)

$\therefore\ \forall x\ P(x)$

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

Elim $\exists$: $\exists x\ P(x)$

$\therefore$ 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. $\exists y\ (y \geq \mathbf{a})$ — Elim $\forall$: 1
4. $\mathbf{b} \geq \mathbf{a}$ — Elim $\exists$: **b** special depends on **a**
5. ~~$\forall x\ (\mathbf{b} \geq x)$ — 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

Intro $\exists$

$$\frac{P(c) \text{ for some } c}{\therefore \quad \exists x\, P(x)}$$

Elim $\forall$

$$\frac{\forall x\, P(x)}{\therefore \quad P(a) \textbf{ for any } a}$$

Elim $\exists$

$$\frac{\exists x\, P(x)}{\therefore\ P(c) \textbf{ for some } \textbf{\textit{special}}^{**}\ c}$$

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

Intro $\forall$

$$\frac{\text{“}\textbf{Let } a \textbf{ be arbitrary}^{*}\text{”} \ldots P(a)}{\therefore \quad \forall x\, P(x)}$$

* 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.