CSE 311: Foundations of Computing

Topic 3: Proofs

Logical Inference

- So far, we've considered:
  - how to understand and *express* things using propositional and predicate logic
  - how to *compute* using Propositional logic (circuits)
  - how to show that different ways of expressing or computing them are *equivalent* to each other

- Logic also has methods that let us *infer* implied properties from ones that we know
  - equivalence is a small part of this

New Perspective

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

p	*q*	A(*p*,*q*)	B(*p*,*q*)
T	T	T	
T	F	T	
F	T	F	
F	F	F	

New Perspective

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

p	*q*	A(*p*,*q*)	B(*p*,*q*)
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.

$$A \Rightarrow B$$

New Perspective

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

p	*q*	A(*p*,*q*)	B(*p*,*q*)
T	T	T	T
T	F	T	T
F	T	F	?
F	F	F	?

When we zoom out, what have we proven?

New Perspective

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

p	*q*	A(*p*,*q*)	B(*p*,*q*)	A → 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?

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

New Perspective

Equivalences

$A \equiv B$ and $(A \leftrightarrow B) \equiv T$ are the same

Inference

$A \Rightarrow B$ and $(A \rightarrow B) \equiv T$ are the same

Can do the inference by zooming in to the rows where A is true

– that is, we assume that A is true

Proofs

- Start with given facts (hypotheses)
- Use rules of inference to extend set of facts
- Result is proved when it is included in the set

An inference rule: *Modus Ponens*

- If A and $A \rightarrow B$ are both true, then B must be true
- Write this rule as $\dfrac{A \; ; \; A \rightarrow B}{\therefore \; B}$
- Given:
  - If it is Friday, then you have a 311 lecture today.
  - It is Friday.
- Therefore, by Modus Ponens:
  - You have a 311 lecture today.

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.		
5.		

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

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: 4, 3

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

Proofs can use equivalences too

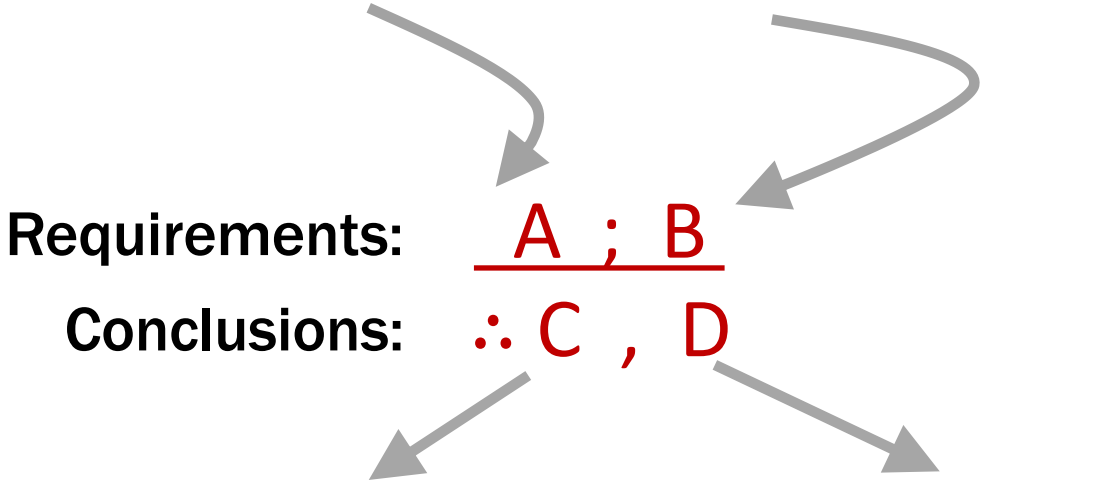
Show that ¬p follows from $p \rightarrow q$ and ¬q

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

Inference Rules

If A is true and B is true ....

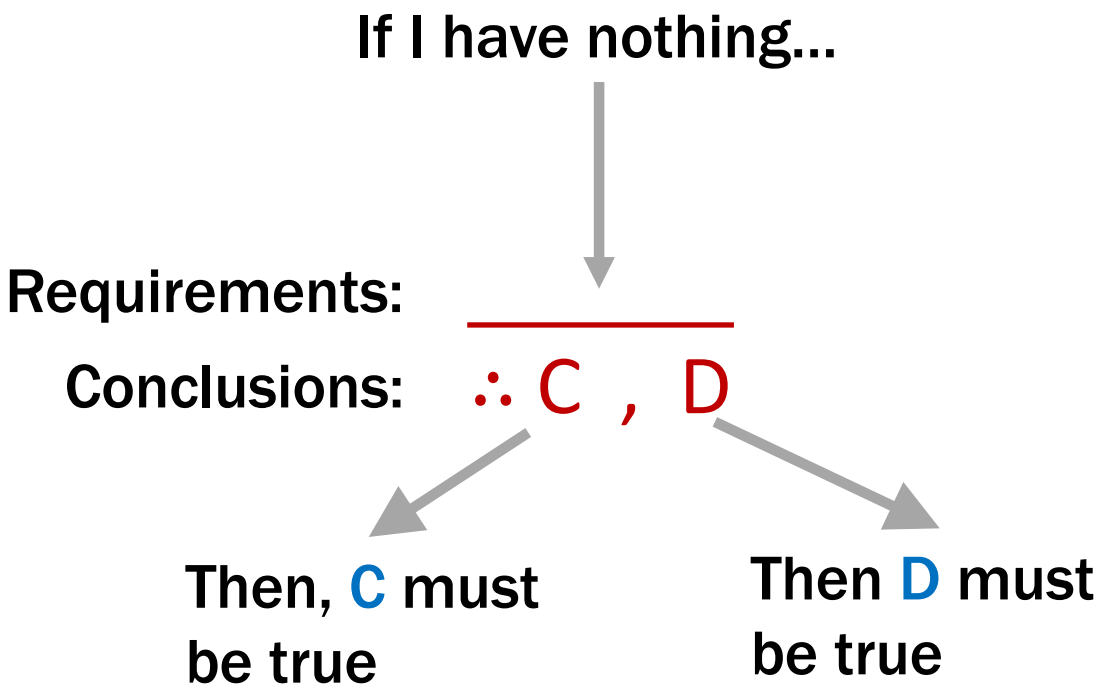


Example (Modus Ponens):

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

If I have A and $A \rightarrow B$ both true, Then B must be true.

Axioms: Special inference rules



Example (Excluded Middle):

$$\frac{}{\therefore\ A \vee \neg A}$$

$A \vee \neg A$ must be true.

Simple Propositional Inference Rules

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

Elim $\wedge$

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

Intro $\wedge$

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

Elim $\vee$

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

Intro $\vee$

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

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 $p, p \to q,$ and $p \wedge q \to r$

1.	p	Given
2.	$p \to q$	Given
3.	$p \wedge q \to r$	Given

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

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

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

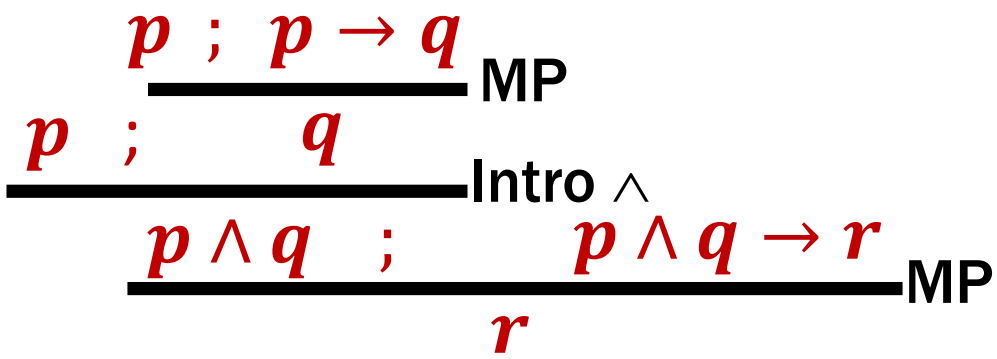
Proofs

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

Proofs

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



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 right one, but if the bottom one helps you think about it, that's great!

$$\dfrac{\dfrac{p \;;\; p \to q}{q}\text{MP} \qquad p \to q}{p \wedge q}\text{Intro } \wedge$$

$$\dfrac{p \wedge q \;;\; p \wedge q \to r}{r}\text{MP}$$

Proofs

Prove that ¬r follows from p ∧ s, q → ¬r, and ¬s ∨ q.

1. $p \wedge s$ Given
2. $q \rightarrow \neg r$ Given
3. $\neg s \vee q$ Given

First: Write down givens and goal

20. $\neg r$?

Idea: Work backwards!

Proofs

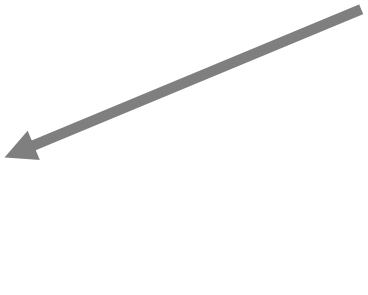
Prove that ¬r follows from p ∧ s, q → ¬r, and ¬s ∨ q.

1.	$p \wedge s$	Given
2.	$q \rightarrow \neg r$	Given
3.	$\neg s \vee q$	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 →" which is MP.



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

Proofs

Prove that ¬r follows from p ∧ s, q → ¬r, and ¬s ∨ q.

1.	$p \wedge s$	Given
2.	$q \rightarrow \neg r$	Given
3.	$\neg s \vee q$	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

Proofs

Prove that ¬r follows from p ∧ s, q → ¬r, and ¬s ∨ 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 ¬r follows from p ∧ s, q → ¬r, and ¬s ∨ q.

1.	$p \wedge s$	Given
2.	$q \rightarrow \neg r$	Given
3.	$\neg s \vee q$	Given

18.	$\neg\neg s$	
19.	q	∨ Elim: 3, 18
20.	$\neg r$	MP: 2, 19

$\neg\neg s$ doesn't show up in the givens but s does and we can use equivalences

Proofs

Prove that ¬r follows from p ∧ s, q → ¬r, and ¬s ∨ 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	Elim ∨: 3, 18
20.	$\neg r$	MP: 2, 19

Proofs

Prove that ¬r follows from p ∧ s, q → ¬r, and ¬s ∨ q.

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

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

Proofs

Prove that ¬r follows from p ∧ s, q → ¬r, and ¬s ∨ q.

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

  Does not follow! e.g . p=F, q=T, r=F

Recall: Propositional Inference Rules

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

Elim $\wedge$

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

Intro $\wedge$

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

Elim $\vee$

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

Intro $\vee$

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

Modus Ponens

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

Direct Proof

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

Recall: 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.

$$A \Rightarrow B$$

Recall: 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?

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

Recall: Propositional Inference Rules

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

Elim $\wedge$

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

Intro $\wedge$

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

Elim $\vee$

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

Intro $\vee$

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

Modus Ponens

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

Direct Proof

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

Not like other rules

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 "**Assuming** 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

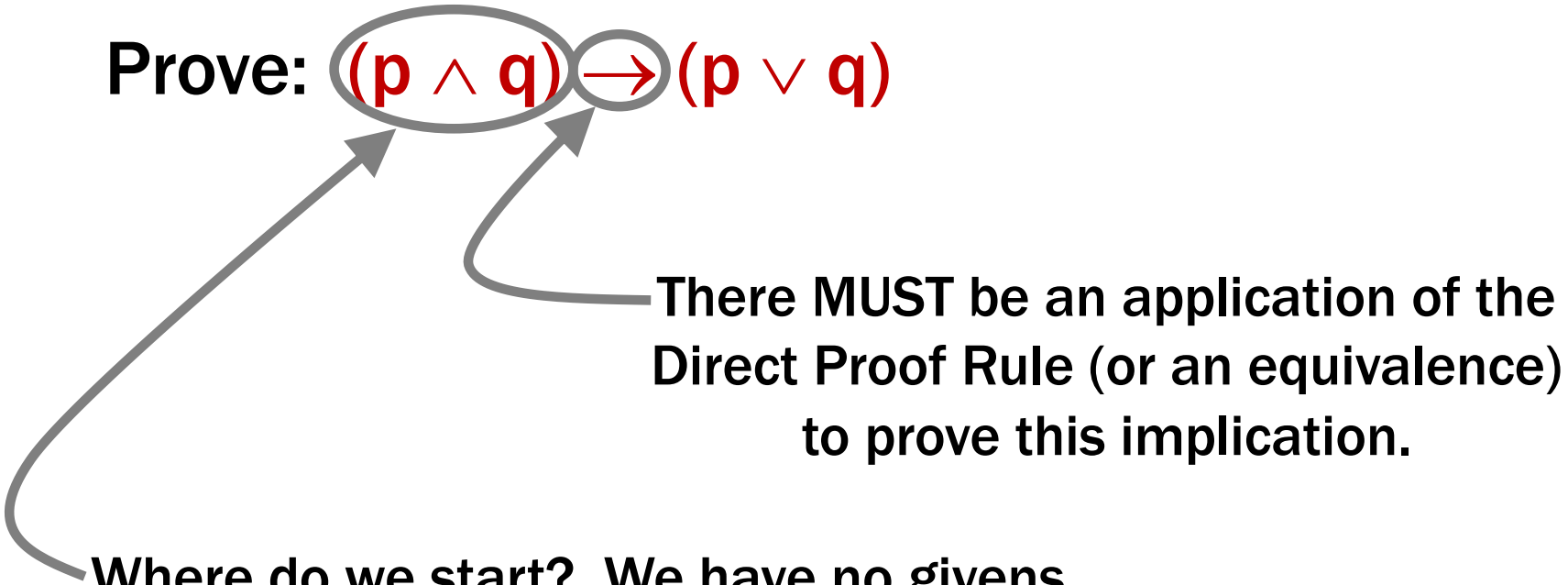
Proofs using the direct proof rule

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



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

Applications of Logical Inference

- **Software Engineering**
  - Express desired properties of program as set of logical constraints
  - Use inference rules to show that program implies that those constraints are satisfied
- **Artificial Intelligence**
  - Automated reasoning
- **Algorithm design and analysis**
  - e.g., Correctness, Loop invariants.
- **Logic Programming, e.g. Prolog**
  - Express desired outcome as set of constraints
  - Automatically apply logic inference to derive solution

Recall: Propositional Inference Rules

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

Elim $\wedge$

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

Intro $\wedge$

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

Elim $\vee$

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

Intro $\vee$

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

Modus Ponens

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

Direct Proof

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

Our General Proof Strategy

1. Use **introduction** rules to see how you would build **up** the formula you want to prove from pieces of what is given

2. Use **elimination** rules to break **down** the given formulas to get the pieces you need to do 1.

3. Write the proof beginning with what you figured out for 2 followed by 1.

Our General Proof Strategy

1. $p \to q$ Given
2. p Given

...

?. $(p \vee r) \wedge q$?

Use **elimination** rules to move **down**

Our General Proof Strategy

1. $p \to q$	Given
2. p	Given
3. q	MP: 2, 1
...	
?. $(p \vee r) \wedge q$	?

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Our General Proof Strategy

1. $p \to q$ Given
2. p Given
3. q MP: 2, 1

...

?. $p \vee r$

?. q

?. $(p \vee r) \wedge q$ Intro $\wedge$

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Our General Proof Strategy

1. $p \to q$ Given
2. p Given

...

?. $p \vee r$ Intro $\vee$??

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Exception: Intro $\vee$ (**must** wait until you know which one is true)

Our General Proof Strategy

1. $p \to q$	Given	
2. p	Given	
…		
?. r	?	
?. $p \vee r$	Intro $\vee$	

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Exception: Intro $\vee$
(**must** wait until you know which one is true)

Our General Proof Strategy

1. $p \wedge q$	Given
2. p	Elim $\wedge$: 1
3. q	Elim $\wedge$: 1
…	
?. $(p \vee r) \wedge q$	?

Could **wait** on Elim $\wedge$
(**but** there is no reason to)

Use **elimination** rules
to move **down**

Use **introduction** rules
to move **up**

Exception: Intro $\vee$
(**must** wait until you know
which one is true)

Example

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

Example

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

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

1.? $p \rightarrow r$

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

Example

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

1.1.	$(p \to q) \wedge (q \to r)$	Assumption
1.2.	$p \to q$	Elim ∧: 1.1
1.3.	$q \to r$	Elim ∧: 1.1

1.? $p \to r$

1. $\big((p \to q) \wedge (q \to r)\big) \to (p \to r)$ 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. $p \rightarrow q$ Elim ∧: 1.1

1.3. $q \rightarrow r$ 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: $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$

1.1.	$(p \rightarrow q) \wedge (q \rightarrow r)$	Assumption
1.2.	$p \rightarrow q$	Elim ∧: 1.1
1.3.	$q \rightarrow r$	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.	$\big((p \rightarrow q) \wedge (q \rightarrow r)\big) \rightarrow (p \rightarrow r)$	Direct Proof

Minimal Rules for Propositional Logic

Can get away with just these:

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

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

Excluded Middle

$$\frac{}{\therefore A \vee \neg A}$$

Note: **not** non-contradiction

Rules for Propositional Logic *with Tautology*

More rules makes proofs easier

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

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

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

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

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

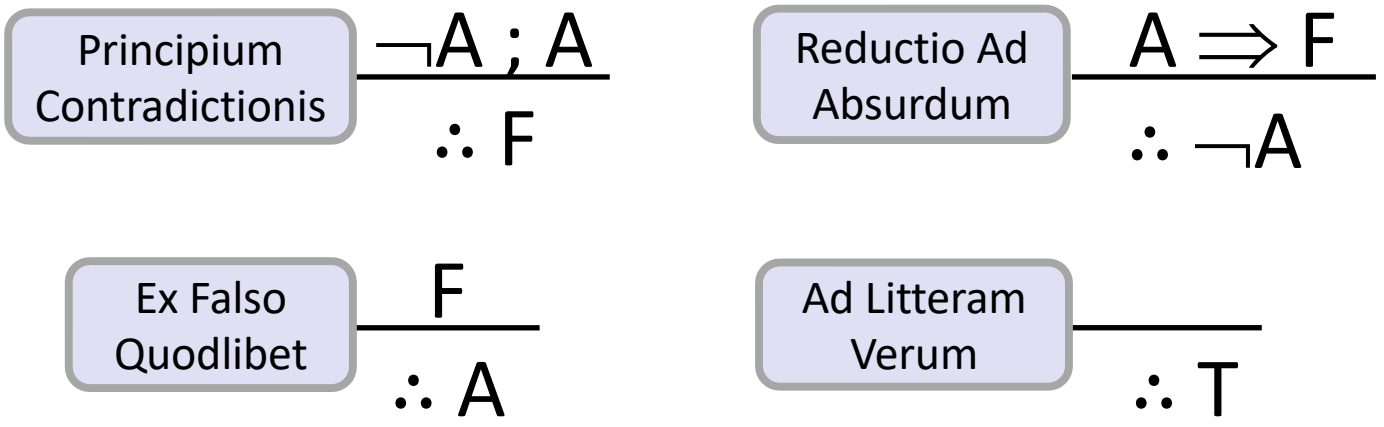
Direct Proof $\dfrac{A \Rightarrow B}{\therefore A \rightarrow B}$

Tautology $\dfrac{A \equiv T}{\therefore A}$

Equivalent $\dfrac{A \equiv B\ ;\ B}{\therefore A}$

More Rules for Propositional Logic

More rules makes proofs easier



useful for proving things
without the Tautology rule

Other Rules for Propositional Logic

Some rules can be written in different ways

- **e.g., two different elimination rules for "∨"**

Elim ∨

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

Cases

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

these rules are equally capable

Rules for Propositional Logic *w/o Tautology*

	Elimination	Introduction
$\wedge$	Elim $\wedge$	Intro $\wedge$
$\vee$	Cases	Intro $\vee$
$\rightarrow$	Modus Ponens	Direct Proof
$\neg$	Principium Contradictionis	Reductio Ad Absurdum
F / T	Ex Falso Quodlibet	Ad Litteram Verum

Administrivia

- Posted a video on our rules for Propositional Logic
  - motivation and walkthrough for the new rules
  - two example proofs using them
  - mentions some applications outside of 311

- Please watch that by Wednesday
  - less than 20 minutes
  - link is on the Topics page under the Topic 3 lecture

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 ∃

Intro ∀

My First Predicate Logic Proof

Domain of Discourse
Integers

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

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

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

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

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. $\exists x\ P(x)$?

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**

1.4. $P(5)$?

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

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

1.4. $P(5)$ Elim ∀: 1.1

1.5. $\exists x\ P(x)$ Intro ∃: 1.4

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
1.3. $\exists x\ P(x)$ Intro ∃: 1.2

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

This follows our usual strategy — eliminate forward, introduce backward — but it is weird...

How did we know to use 5? We didn't! We just guessed it.

Randomly guessing numbers is not good proof strategy!

Our General Proof Strategy

1. $\forall x\,((x > 9) \rightarrow P(x))$ Given

...

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

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Our General Proof Strategy

1.	$\forall x\,((x > 9) \rightarrow P(x))$	Given
...		
?.	$P(5)$	?
?.	$\exists x\,P(x)$	Intro ∃

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Our General Proof Strategy

1. $\forall x\,((x > 9) \rightarrow P(x))$ Given

...

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

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Exception: Intro ∨ / ∃
(**must** wait until you know which one is true)

Our General Proof Strategy

1. $\forall x\, P(x)$ Given
2. $P(100) \rightarrow Q(100)$ Given

...

?. $\exists x\, Q(x)$?

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Our General Proof Strategy

1.	$\forall x\, P(x)$	Given
2.	$P(100) \rightarrow Q(100)$	Given
3.	$P(1)$	Elim ∀: 1
…		
?.	$\exists x\, Q(x)$	?

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Our General Proof Strategy

1.	$\forall x\, P(x)$	Given
2.	$P(100) \rightarrow Q(100)$	Given
3.	$P(1)$	Elim ∀: 1
4.	$P(2)$	Elim ∀: 1
…		
?.	$\exists x\, Q(x)$	?

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Our General Proof Strategy

1.	$\forall x\, P(x)$	Given
2.	$P(100) \rightarrow Q(100)$	Given
3.	$P(1)$	Elim ∀: 1
4.	$P(2)$	Elim ∀: 1
5.	$P(3)$	Elim ∀: 1
…		
?.	$\exists x\, Q(x)$	?

Exception: Elim ∀
(**must** wait until you know which one *you need*)

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Our General Proof Strategy

1. $\forall x\, P(x)$ — Given

...

?. $\exists x\, P(x)$ — ?

Exception: Elim ∀
(**must** wait until you know which one *you need*)

Use **elimination** rules to move **down**

Use **introduction** rules to move **up**

Exception: Intro ∨ / ∃
(**must** wait until you know which one is true)

Domain Knowledge

- Intro ∃ and Elim ∀ are *creative* steps
  - need to know the right object to use

    make the wrong choice and the proof won't work
  - the other rules are *mechanical*

    you can apply them blindly without thinking too hard

- Requires your understanding (and intuition) of the objects in question
  - i.e., your "domain knowledge"

Predicate Logic Proofs with more content

- Want to be able to use domain knowledge so that proofs are about things we understand

- Example:

Domain of Discourse
Integers

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

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

A Not so Odd Example

Domain of Discourse
Integers

Predicate Definitions
Even(x) := ∃y (x = 2·y)
Odd(x) := ∃y (x = 2·y + 1)

Prove "There is an even number"

Formally: prove ∃x Even(x)

A Not so Odd Example

Domain of Discourse
Integers

Predicate Definitions
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.	**6 = 2·3**	**Algebra**
2.	∃y (**6 = 2**·y)	**Intro ∃: 1**
3.	Even(**6**)	**Definition of** Even
4.	∃x Even(x)	**Intro ∃: 3**

A Prime Example

Domain of Discourse
Integers

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

Prove "There is an even prime number"

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

A Prime Example

Domain of Discourse
Integers

Predicate Definitions
Even(x) := ∃y (x = 2·y)
Odd(x) := ∃y (x = 2·y + 1)
Prime(x) := "…"

Prove "There is an even prime number"

Formally: prove ∃x (Even(x) ∧ Prime(x))

1.	**2 = 2·1**	**Algebra**
2.	∃y (**2** = **2**·y)	**Intro ∃: 1**
3.	Even(**2**)	**Def of** Even**: 3**
4.	Prime(**2**)*	**Property of integers**
5.	Even(**2**) ∧ Prime(**2**)	**Intro ∧: 3, 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

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 ∃

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

Intro ∀

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

** 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

Note: bottom two rules are *complex* but mechanical
(you can apply them blindly)

Even and Odd

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

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) / ∴ ∀x P(x)	∃x P(x) / ∴ P(c) for some *special*** c

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

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

1. $\forall x\,(Even(x) \rightarrow Even(x^2))$?

Even and Odd

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

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) / ∴ ∀x P(x)	∃x P(x) / ∴ P(c) for some *special*** c

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

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

Let **a** be an arbitrary integer

1.1 $Even(\mathbf{a}) \rightarrow Even(\mathbf{a}^2)$?

1. $\forall x\,(Even(x) \rightarrow Even(x^2))$ Intro ∀

Even and Odd

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

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) / ∴ ∀x P(x)	∃x P(x) / ∴ P(c) for some *special*** c

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

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

Let a be an arbitrary integer

1.1.1 Even(**a**) Assumption

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

1.1 Even(**a**)→Even($\mathbf{a}^2$) Direct proof

1. $\forall x\,(Even(x) \rightarrow Even(x^2))$ Intro ∀

Even and Odd

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

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) / ∴ ∀x P(x)	∃x P(x) / ∴ P(c) for some *special*** c

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

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

Let a be an arbitrary integer

1.1.1 Even(**a**) — Assumption

1.1.2 ∃y (**a** = 2y) — Definition of Even: 1.1.1

1.1.6 Even($\mathbf{a}^2$) — ?

1.1 Even(**a**)→Even($\mathbf{a}^2$) — Direct proof

1. ∀x (Even(x)→Even(x^2)) — Intro ∀

Even and Odd

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

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) / ∴ ∀x P(x)	∃x P(x) / ∴ P(c) for some *special*** c

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

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

Let a be an arbitrary integer

1.1.1 Even(**a**) — Assumption

1.1.2 ∃y (**a** = 2y) — Definition of Even: 1.1.1

1.1.5 ∃y ($\mathbf{a}^2$ = 2y) — ?

1.1.6 Even($\mathbf{a}^2$) — Definition of Even

1.1 Even(**a**)→Even($\mathbf{a}^2$) — Direct proof

1. ∀x (Even(x)→Even(x^2)) — Intro ∀

Even and Odd

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

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) / ∴ ∀x P(x)	∃x P(x) / ∴ P(c) **for some *special*** c

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

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

Let a be an arbitrary integer

1.1.1 Even(**a**) — Assumption
1.1.2 ∃y (**a** = 2y) — Definition of Even: 1.1.1
1.1.3 **a** = 2**b** — Elim ∃: 1.1.2

Need $a^2 = 2c$ for some **c**

1.1.5 ∃y (a^2 = 2y) — ?
1.1.6 Even(a^2) — Definition of Even

1.1 Even(**a**)→Even(a^2) — Direct proof

1. ∀x (Even(x)→Even(x^2)) — Intro ∀

Even and Odd

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

Intro ∀: "Let a be arbitrary*"...P(a) / ∴ ∀x P(x)

Elim ∃: ∃x P(x) / ∴ P(c) for some *special*** c

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

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

Let a be an arbitrary integer

1.1.1	Even(**a**)	Assumption
1.1.2	∃y (**a** = 2y)	Definition of Even
1.1.3	**a** = 2**b**	Elim ∃
1.1.4	$\mathbf{a}^2 = 2(2\mathbf{b}^2)$	Algebra
1.1.5	∃y ($\mathbf{a}^2$ = 2y)	Intro ∃
1.1.6	Even($\mathbf{a}^2$)	Definition of Even
1.1	Even(**a**)→Even($\mathbf{a}^2$)	Direct proof
1.	∀x (Even(x)→Even(x^2))	Intro ∀

Used $\mathbf{a}^2 = 2\mathbf{c}$ for $\mathbf{c}=2\mathbf{b}^2$

Even and Odd

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

Intro ∀: "Let a be arbitrary*"...P(a) / ∴ ∀x P(x)

Elim ∃: ∃x P(x) / ∴ P(c) for some *special*** c

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

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

Let a be an arbitrary integer

1.1.1	Even(**a**)	Assumption
1.1.2	∃y (**a** = 2y)	Definition of Even: 1.1.1
1.1.3	**a** = 2**b**	Elim ∃: 1.1.2
1.1.4	$\mathbf{a}^2 = 2(2\mathbf{b}^2)$	Algebra: 1.1.3
1.1.5	∃y ($\mathbf{a}^2$ = 2y)	Intro ∃: 1.1.4
1.1.6	Even($\mathbf{a}^2$)	Definition of Even: 1.1.5
1.1	Even(**a**)→Even($\mathbf{a}^2$)	Direct proof
1.	$\forall x\,(Even(x) \rightarrow Even(x^2))$	Intro ∀

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

Rules for Propositional Logic *w/o Tautology*

	Elimination	Introduction
$\wedge$	Elim $\wedge$	Intro $\wedge$
$\vee$	Cases	Intro $\vee$
$\rightarrow$	Modus Ponens	Direct Proof
$\neg$	Principium Contradictionis	Reductio Ad Absurdum
F / T	Ex Falso Quodlibet	Ad Litteram Verum

Recall: Important Equivalences

- **Identity**
  - $p \wedge \mathrm{T} \equiv p$
  - $p \vee \mathrm{F} \equiv p$
- **Domination**
  - $p \vee \mathrm{T} \equiv \mathrm{T}$
  - $p \wedge \mathrm{F} \equiv \mathrm{F}$
- **Idempotent**
  - $p \vee p \equiv p$
  - $p \wedge p \equiv p$
- **Commutative**
  - $p \vee q \equiv q \vee p$
  - $p \wedge q \equiv q \wedge p$
- **Associative**
  - $(p \vee q) \vee r \equiv p \vee (q \vee r)$
  - $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
- **Distributive**
  - $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
  - $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
- **Absorption**
  - $p \vee (p \wedge q) \equiv p$
  - $p \wedge (p \vee q) \equiv p$
- **Negation**
  - $p \vee \neg p \equiv \mathrm{T}$
  - $p \wedge \neg p \equiv \mathrm{F}$

Recall: Proof by Cases

Some rules can be written in different ways

- **e.g., two different elimination rules for "∨"**

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

$$\text{Cases} \quad \frac{A \vee B \; ; \; A \rightarrow C \; ; \; B \rightarrow C}{\therefore C}$$

these rules are equally capable

Example: Absorption via Latin Rules

Show that P follows from $P \vee (P \wedge Q)$...

1. $P \vee (P \wedge Q)$ Given

Cases $\dfrac{A \vee B \; ; \; A \rightarrow C \; ; \; B \rightarrow C}{\therefore C}$

4. P ?

Example: Absorption via Latin Rules

Show that P follows from $P \vee (P \wedge Q)$...

1. $P \vee (P \wedge Q)$	Given
2. $P \rightarrow P$	?
3. $(P \wedge Q) \rightarrow P$	?
4. P	Cases: 1, 2, 3

Example: Absorption via Latin Rules

Show that P follows from $P \vee (P \wedge Q)$...

1. $P \vee (P \wedge Q)$ — Given

2. $P \rightarrow P$ — Direct Proof

   3.1. $P \wedge Q$ — Assumption

   3.?. P — ?

3. $(P \wedge Q) \rightarrow P$ — Direct Proof

Example: Absorption via Latin Rules

Show that P follows from $P \vee (P \wedge Q)$...

1. $P \vee (P \wedge Q)$	Given
2. $P \rightarrow P$	Direct Proof
3.1. $P \wedge Q$	Assumption
3.2. P	Elim $\wedge$: 3.1
3. $(P \wedge Q) \rightarrow P$	Direct Proof
4. P	Cases: 1, 2, 3

Example: Absorption via Latin Rules

Show that P follows from $P \vee (P \wedge Q)$...

1. $P \vee (P \wedge Q)$	Given
2.1. P	Assumption
2.?. P	?
2. $P \rightarrow P$	Direct Proof
3.1. $P \wedge Q$	Assumption
3.2. P	Elim $\wedge$: 3.1
3. $(P \wedge Q) \rightarrow P$	Direct Proof

Example: Absorption via Latin Rules

Show that P follows from $P \vee (P \wedge Q)$...

1. $P \vee (P \wedge Q)$	Given
2.1. P	Assumption
2. $P \rightarrow P$	Direct Proof
3.1. $P \wedge Q$	Assumption
3.2. P	Elim $\wedge$: 3.1
3. $(P \wedge Q) \rightarrow P$	Direct Proof
4. P	Cases: 1, 2, 3

Example: Distributivity via Latin Rules

Show $(P \wedge Q) \vee (P \wedge R)$ follows from $P \wedge (Q \vee R)$...

1. $P \wedge (Q \vee R)$ Given

6. $(P \wedge Q) \vee (P \wedge R)$?

Example: Distributivity via Latin Rules

Show $(P \wedge Q) \vee (P \wedge R)$ follows from $P \wedge (Q \vee R)$...

1. $P \wedge (Q \vee R)$	Given
2. P	Elim ∧: 1
3. $Q \vee R$	Elim ∧: 1

6. $(P \wedge Q) \vee (P \wedge R)$	?

Example: Distributivity via Latin Rules

Show $(P \wedge Q) \vee (P \wedge R)$ follows from $P \wedge (Q \vee R)$...

1. $P \wedge (Q \vee R)$	Given
2. P	Elim $\wedge$: 1
3. $Q \vee R$	Elim $\wedge$: 1
4. $Q \rightarrow (P \wedge Q) \vee (P \wedge R)$	?
5. $R \rightarrow (P \wedge Q) \vee (P \wedge R)$	?
6. $(P \wedge Q) \vee (P \wedge R)$	Cases: 3, 4, 5

Example: Distributivity via Latin Rules

Show $(P \wedge Q) \vee (P \wedge R)$ follows from $P \wedge (Q \vee R)$...

1. $P \wedge (Q \vee R)$	Given
2. P	Elim $\wedge$: 1
3. $Q \vee R$	Elim $\wedge$: 1
4.1. Q	Assumption
4.?. $(P \wedge Q) \vee (P \wedge R)$	?
4. $Q \rightarrow (P \wedge Q) \vee (P \wedge R)$	Direct Proof
5. $R \rightarrow (P \wedge Q) \vee (P \wedge R)$	?
6. $(P \wedge Q) \vee (P \wedge R)$	Cases: 3, 4, 5

Example: Distributivity via Latin Rules

Show $(P \wedge Q) \vee (P \wedge R)$ follows from $P \wedge (Q \vee R)$...

1. $P \wedge (Q \vee R)$	Given
2. P	Elim ∧: 1
3. $Q \vee R$	Elim ∧: 1
4.1. Q	Assumption
4.2. $P \wedge Q$	Intro ∧: 2, 4.1
4.3. $(P \wedge Q) \vee (P \wedge R)$	Intro ∨: 4.2
4. $Q \rightarrow (P \wedge Q) \vee (P \wedge R)$	Direct Proof
5. $R \rightarrow (P \wedge Q) \vee (P \wedge R)$	?
6. $(P \wedge Q) \vee (P \wedge R)$	Cases: 3, 4, 5

Example: Distributivity via Latin Rules

Show $(P \wedge Q) \vee (P \wedge R)$ follows from $P \wedge (Q \vee R)$...

1. $P \wedge (Q \vee R)$	Given
2. P	Elim $\wedge$: 1
3. $Q \vee R$	Elim $\wedge$: 1
4.1. Q	Assumption
4.2. $P \wedge Q$	Intro $\wedge$: 2, 4.1
4.3. $(P \wedge Q) \vee (P \wedge R)$	Intro $\vee$: 4.2
4. $Q \rightarrow (P \wedge Q) \vee (P \wedge R)$	Direct Proof
5.1. R	Assumption
5.3. $(P \wedge Q) \vee (P \wedge R)$	?
5. $R \rightarrow (P \wedge Q) \vee (P \wedge R)$	Direct Proof
6. $(P \wedge Q) \vee (P \wedge R)$	Cases: 3, 4, 5

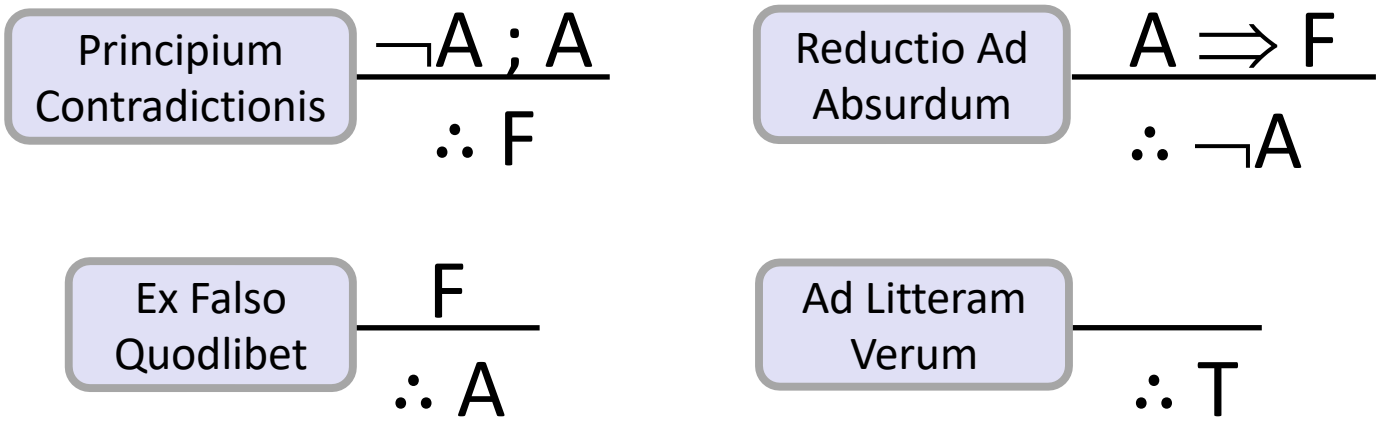
Example: Distributivity via Latin Rules

Show $(P \wedge Q) \vee (P \wedge R)$ follows from $P \wedge (Q \vee R)$...

1. $P \wedge (Q \vee R)$	Given
2. P	Elim ∧: 1
3. $Q \vee R$	Elim ∧: 1
4.1. Q	Assumption
4.2. $P \wedge Q$	Intro ∧: 2, 4.1
4.3. $(P \wedge Q) \vee (P \wedge R)$	Intro ∨: 4.2
4. $Q \rightarrow (P \wedge Q) \vee (P \wedge R)$	Direct Proof
5.1. R	Assumption
5.2. $P \wedge R$	Intro ∧: 2, 5.1
5.3. $(P \wedge Q) \vee (P \wedge R)$	Intro ∨: 5.2
5. $R \rightarrow (P \wedge Q) \vee (P \wedge R)$	Direct Proof
6. $(P \wedge Q) \vee (P \wedge R)$	Cases: 3, 4, 5

Recall: the Latin Rules

More rules makes proofs easier



useful for proving things
without the Tautology rule

Example: De Morgan's Law via Latin Rules

Show that $\neg(A \vee B)$ follows from $\neg A \wedge \neg B$...

1. $\neg \boldsymbol{A} \wedge \neg \boldsymbol{B}$ Given

4. $\neg(\boldsymbol{A} \vee \boldsymbol{B})$?

Example: De Morgan's Law via Latin Rules

Show that $\neg(A \vee B)$ follows from $\neg A \wedge \neg B$...

1.	$\neg A \wedge \neg B$	Given
2.	$\neg A$	Elim ∧: 1
3.	$\neg B$	Elim ∧: 1

Reductio Ad Absurdum

$$\frac{A \Rightarrow F}{\therefore \neg A}$$

4.	$\neg(A \vee B)$	Absurdum

Example: De Morgan's Law via Latin Rules

Show that $\neg(A \vee B)$ follows from $\neg A \wedge \neg B$...

1. $\neg A \wedge \neg B$ — Given
2. $\neg A$ — Elim ∧: 1
3. $\neg B$ — Elim ∧: 1
    4.1. $A \vee B$ — Assumption

    4.4. $\mathbf{F}$ — ?
4. $\neg(A \vee B)$ — Absurdum

Example: De Morgan's Law via Latin Rules

Show that $\neg(A \vee B)$ follows from $\neg A \wedge \neg B$...

1. $\neg A \wedge \neg B$	Given
2. $\neg A$	Elim $\wedge$: 1
3. $\neg B$	Elim $\wedge$: 1
4.1. $A \vee B$	Assumption
4.2. $A \rightarrow \mathrm{F}$	?
4.3. $B \rightarrow \mathrm{F}$	?
4.4. F	Cases: 4.1, 4.2, 4.3
4. $\neg(A \vee B)$	Absurdum

Example: De Morgan's Law via Latin Rules

Show that $\neg(A \vee B)$ follows from $\neg A \wedge \neg B$...

1. $\neg A \wedge \neg B$	Given
2. $\neg A$	Elim ∧: 1
3. $\neg B$	Elim ∧: 1
4.1. $A \vee B$	Assumption
4.2.1. A	Assumption
4.2.2. $\mathbf{F}$	?
4.2. $A \rightarrow \mathbf{F}$	Direct Proof
4.3. $B \rightarrow \mathbf{F}$	?
4.4. $\mathbf{F}$	Cases: 4.1, 4.2, 4.3
4. $\neg(A \vee B)$	Absurdum

Principium Contradictionis

$$\frac{\neg A \ ; \ A}{\therefore \ F}$$

Example: De Morgan's Law via Latin Rules

Show that $\neg(A \vee B)$ follows from $\neg A \wedge \neg B$...

1. $\neg A \wedge \neg B$	Given
2. $\neg A$	Elim $\wedge$: 1
3. $\neg B$	Elim $\wedge$: 1
4.1. $A \vee B$	Assumption
4.2.1. A	Assumption
4.2.2. $\mathbf{F}$	Contradiction: 4.2.1, 2
4.2. $A \rightarrow \mathbf{F}$	Direct Proof
4.3. $B \rightarrow \mathbf{F}$	?
4.4. $\mathbf{F}$	Cases: 4.1, 4.2, 4.3
4. $\neg(A \vee B)$	Absurdum

Example: De Morgan's Law via Latin Rules

Show that $\neg(A \vee B)$ follows from $\neg A \wedge \neg B$...

1. $\neg A \wedge \neg B$	Given
2. $\neg A$	Elim $\wedge$: 1
3. $\neg B$	Elim $\wedge$: 1
4.1. $A \vee B$	Assumption
4.2.1. A	Assumption
4.2.2. $\mathbf{F}$	Contradiction: 4.2.1, 2
4.2. $A \rightarrow \mathbf{F}$	Direct Proof
4.3.1. B	Assumption
4.3.2. $\mathbf{F}$	?
4.3. $B \rightarrow \mathbf{F}$	Direct Proof
4.4. $\mathbf{F}$	Cases: 4.1, 4.2, 4.3
4. $\neg(A \vee B)$	Absurdum

Example: De Morgan's Law via Latin Rules

Show that $\neg(A \vee B)$ follows from $\neg A \wedge \neg B$...

1. $\neg A \wedge \neg B$	Given
2. $\neg A$	Elim $\wedge$: 1
3. $\neg B$	Elim $\wedge$: 1
4.1. $A \vee B$	Assumption
4.2.1. A	Assumption
4.2.2. $\mathbf{F}$	Contradiction: 4.2.1, 2
4.2. $A \to \mathbf{F}$	Direct Proof
4.3.1. B	Assumption
4.3.2. $\mathbf{F}$	Contradiction: 4.3.1, 3
4.3. $B \to \mathbf{F}$	Direct Proof
4.4. $\mathbf{F}$	Cases: 4.1, 4.2, 4.3
4. $\neg(A \vee B)$	Absurdum

Recall: Important Equivalences

- **Identity**
  - $p \wedge \mathrm{T} \equiv p$
  - $p \vee \mathrm{F} \equiv p$
- **Domination**
  - $p \vee \mathrm{T} \equiv \mathrm{T}$
  - $p \wedge \mathrm{F} \equiv \mathrm{F}$
- **Idempotent**
  - $p \vee p \equiv p$
  - $p \wedge p \equiv p$
- **Commutative**
  - $p \vee q \equiv q \vee p$
  - $p \wedge q \equiv q \wedge p$
- **Associative**
  - $(p \vee q) \vee r \equiv p \vee (q \vee r)$
  - $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
- **Distributive**
  - $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
  - $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
- **Absorption**
  - $p \vee (p \wedge q) \equiv p$
  - $p \wedge (p \vee q) \equiv p$
- **Negation**
  - $\boxed{p \vee \neg p \equiv \mathrm{T}}$
  - $p \wedge \neg p \equiv \mathrm{F}$

Does not follow from Latin rules

Recall: Inference Rules for Quantifiers

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 ∃

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

Intro ∀

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

** 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

Recall; Proofs with Domain Knowledge

- Want to be able to use domain knowledge so that proofs are about things we understand

- Example:

Domain of Discourse
Integers

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

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

Odd Plus Odd

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

Intro ∀: "Let a be arbitrary*"...P(a) / ∴ ∀x P(x)

Elim ∃: ∃x P(x) / ∴ P(c) for some *special*** c

Prove: "The sum of two odd numbers is even."

Formal proof of: $\forall x\, \forall y\, (Odd(x) \wedge Odd(y) \rightarrow Even(x+y))$

1. $\forall x\, \forall y\, (Odd(\mathbf{x}) \wedge Odd(\mathbf{y}) \rightarrow Even(\mathbf{x+y}))$?

Even and Odd

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

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) / ∴ ∀x P(x)	∃x P(x) / ∴ P(c) for some *special*** c

Prove: "The sum of two odd numbers is even."

Formal proof of: ∀x ∀y (Odd(x) ∧ Odd(y) → Even(x+y))

Let a and b be an arbitrary integer

1.1 Odd(**a**) ∧ Odd(**b**) → Even(**a+b**) ?

1. ∀x ∀y (Odd(**x**) ∧ Odd(**y**) → Even(**x+y**)) Intro ∀

Even and Odd

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

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) / ∴ ∀x P(x)	∃x P(x) / ∴ P(c) for some *special*** c

Prove: "The sum of two odd numbers is even."

Formal proof of: ∀x ∀y (Odd(x) ∧ Odd(y) → Even(x+y))

Let a and b be an arbitrary integer

1.1.1 Odd(**a**) ∧ Odd(**b**) Assumption

1.1.? Even(**a** + **b**) ?

1.1 Odd(**a**) ∧ Odd(**b**) → Even(**a+b**) Direct proof

1. ∀x ∀y (Odd(**x**) ∧ Odd(**y**) → Even(**x+y**)) Intro ∀

Even and Odd

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

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) / ∴ ∀x P(x)	∃x P(x) / ∴ P(c) for some *special*** c

Let **a** and **b** be an arbitrary integer

1.1.1	Odd(**a**) ∧ Odd(**b**)	Assumption
1.1.2	Odd(**a**)	Elim ∧: 1.1.1
1.1.3	Odd(**b**)	Elim ∧: 1.1.1

1.1.?	Even(**a** + **b**)	?
1.1	Odd(**a**) ∧ Odd(**b**) → Even(**a+b**)	Direct proof
1.	∀x ∀y (Odd(**x**) ∧ Odd(**y**) → Even(**x+y**))	Intro ∀

Even and Odd

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

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) / ∴ ∀x P(x)	∃x P(x) / ∴ P(c) **for some *special*** c

Let a and b be an arbitrary integer

1.1.1	Odd(**a**) ∧ Odd(**b**)	Assumption
1.1.2	Odd(**a**)	Elim ∧: 1.1.1
1.1.3	Odd(**b**)	Elim ∧: 1.1.1
1.1.4	∃y (**a** = 2y+1)	Def of Odd: 1.1.2
1.1.5	∃y (**b** = 2y+1)	Def of Odd: 1.1.3

1.1.?	Even(**a** + **b**)	?
1.1	Odd(**a**) ∧ Odd(**b**) → Even(**a+b**)	Direct proof
1.	∀x ∀y (Odd(**x**) ∧ Odd(**y**) → Even(**x+y**))	Intro ∀

Even and Odd

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

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) / ∴ ∀x P(x)	∃x P(x) / ∴ P(c) for some *special*** c

Let **a** and **b** be an arbitrary integer

1.1.1	Odd(**a**) ∧ Odd(**b**)	Assumption
1.1.2	Odd(**a**)	Elim ∧: 1.1.1
1.1.3	Odd(**b**)	Elim ∧: 1.1.1
1.1.4	∃y (**a** = 2y+1)	Def of Odd: 1.1.2
1.1.5	∃y (**b** = 2y+1)	Def of Odd: 1.1.3
1.1.?	∃y (**a** + **b** = 2y)	?
1.1.?	Even(**a** + **b**)	Def of Even
1.1	Odd(**a**) ∧ Odd(**b**) → Even(**a+b**)	Direct proof
1.	∀x ∀y (Odd(**x**) ∧ Odd(**y**) → Even(**x+y**))	Intro ∀

Even and Odd

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

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) / ∴ ∀x P(x)	∃x P(x) / ∴ P(c) for some *special*** c

Let **a** and **b** be an arbitrary integer

1.1.1	Odd(**a**) ∧ Odd(**b**)	Assumption
1.1.2	Odd(**a**)	Elim ∧: 1.1.1
1.1.3	Odd(**b**)	Elim ∧: 1.1.1
1.1.4	∃y (**a** = 2y+1)	Def of Odd: 1.1.2
1.1.5	∃y (**b** = 2y+1)	Def of Odd: 1.1.3
1.1.6	**a** = 2**c** + 1	Elim ∃: 1.1.4
1.1.7	**b** = 2**d** + 1	Elim ∃: 1.1.5
1.1.?	∃y (**a** + **b** = 2y)	?
1.1.?	Even(**a** + **b**)	Def of Even
1.1	Odd(**a**) ∧ Odd(**b**) → Even(**a+b**)	Direct proof
1.	∀x ∀y (Odd(**x**) ∧ Odd(**y**) → Even(**x+y**))	Intro ∀

Even and Odd

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

Intro ∀	Elim ∃
"Let a be arbitrary*"...P(a) / ∴ ∀x P(x)	∃x P(x) / ∴ P(c) **for some *special*** c

Let a and b be an arbitrary integer

1.1.1	Odd(**a**) ∧ Odd(**b**)	Assumption
1.1.2	Odd(**a**)	Elim ∧: 1.1.1
1.1.3	Odd(**b**)	Elim ∧: 1.1.1
1.1.4	∃y (**a** = 2y+1)	Def of Odd: 1.1.2
1.1.5	∃y (**b** = 2y+1)	Def of Odd: 1.1.3
1.1.6	**a** = 2**c** + 1	Elim ∃: 1.1.4
1.1.7	**b** = 2**d** + 1	Elim ∃: 1.1.5
1.1.8	**a** + **b** = 2(**c** + **d** +1)	Algebra: 1.1.6–7
1.1.9	∃y (**a** + **b** = 2y)	Intro ∃: 1.1.8
1.1.10	Even(**a** + **b**)	Def of Even: 1.1.9
1.1	Odd(**a**) ∧ Odd(**b**) → Even(**a+b**)	Direct proof
1.	∀x ∀y (Odd(**x**) ∧ Odd(**y**) → Even(**x+y**))	Intro ∀

Formal Proofs

- Formal proofs follow simple well-defined rules
  - "assembly language" (like byte code) for proofs
  - easy for a machine to check

- Important to understand
  - mental "foundations" of Computer Science
  - has useful applications, e.g., Programming Languages

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 can be tedious and impractical…

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) := $\exists a\ \exists b\ (\text{Integer}(a) \wedge \text{Integer}(b) \wedge (x = a/b) \wedge (b \neq 0))$

Prove: "If x and y are rational, then xy is rational."

1. Rational(**x**) ∧ Rational(**y**) → Rational(**xy**) ?

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) := $\exists a\ \exists b\ (\text{Integer}(a) \wedge \text{Integer}(b) \wedge (x = a/b) \wedge (b \neq 0))$

Prove: "If x and y are rational, then xy is rational."

1.1. Rational(**x**) ∧ Rational(**y**) Assumption

1.?. Rational(**x** + **y**) Def of Rational

1. Rational(**x**) ∧ Rational(**y**) → Rational(**xy**) Direct Proof

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) := $\exists a\ \exists b\ (\text{Integer}(a) \wedge \text{Integer}(b) \wedge (x = a/b) \wedge (b \neq 0))$

Prove: "If x and y are rational, then xy is rational."

1.1. Rational(**x**) ∧ Rational(**y**) Assumption

Then, x = a/b for some integers a, b, where b≠0, and y = c/d for some integers c,d, where d≠0.

Multiplying, we get that xy = (a/b)(c/d) = (ac)/(bd).

Since b and d are both non-zero, so is bd.

Furthermore, ac and bd are integers.

By definition, then, xy is rational.

1.?. Rational(**x** + **y**) Def of Rational

1. Rational(**x**) ∧ Rational(**y**) → Rational(**xy**) Direct Proof

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions

Rational(x) := $\exists a\ \exists b\ (\text{Integer}(a) \wedge \text{Integer}(b) \wedge (x = a/b) \wedge (b \neq 0))$

Prove: "If x and y are rational, then xy is rational."

Suppose x and y are rational.

1.1 $\text{Rational}(x) \wedge \text{Rational}(y)$ **Assumption**

Then, x = a/b for some integers a, b, where b≠0 and y = c/d for some integers c,d, where d≠0.

1.4 $\exists p\ \exists q\ ((x = p/q) \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge (q \neq 0))$
Def Rational: 1.2

1.5 $(x = a/b) \wedge \text{Integer}(a) \wedge \text{Integer}(b) \wedge (b \neq 0)$
Elim ∃: 1.4

1.6 $\exists p\ \exists q\ \big((x = p/q) \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge (q \neq 0)\big)$
Def Rational: 1.3

1.7 $(y = c/d) \wedge \text{Integer}(c) \wedge \text{Integer}(d) \wedge (d \neq 0)$
Elim ∃: 1.4

...

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) := $\exists a\ \exists b\ (\text{Integer}(a) \wedge \text{Integer}(b) \wedge (x = a/b) \wedge (b \neq 0))$

Prove: "If x and y are rational, then xy is rational."

Suppose x and y are rational.

1.1 $\text{Rational}(x) \wedge \text{Rational}(y)$ **Assumption**

??

Then, x = a/b for some integers a, b, where b≠0 and y = c/d for some integers c,d, where d≠0.

1.4 $\exists p\ \exists q\ ((x = p/q) \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge (q \neq 0))$
Def Rational: 1.2

1.5 $(x = a/b) \wedge \text{Integer}(a) \wedge \text{Integer}(b) \wedge (b \neq 0)$
Elim ∃: 1.4

1.6 $\exists p\ \exists q\ \big((x = p/q) \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge (q \neq 0)\big)$
Def Rational: 1.3

1.7 $(y = c/d) \wedge \text{Integer}(c) \wedge \text{Integer}(d) \wedge (d \neq 0)$
Elim ∃: 1.4

...

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) := $\exists a\ \exists b\ (\text{Integer}(a) \wedge \text{Integer}(b) \wedge (x = a/b) \wedge (b \neq 0))$

Prove: "If x and y are rational, then xy is rational."

Suppose x and y are rational.

Then, x = a/b for some integers a, b, where b≠0 and y = c/d for some integers c,d, where d≠0.

...

1.1 $\text{Rational}(x) \wedge \text{Rational}(y)$ **Assumption**

1.2 $\text{Rational}(x)$ **Elim ∧: 1.1**

1.3 $\text{Rational}(y)$ **Elim ∧: 1.1**

1.4 $\exists p\ \exists q\ ((x = p/q) \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge (q \neq 0))$ **Def Rational: 1.2**

1.5 $(x = a/b) \wedge \text{Integer}(a) \wedge \text{Integer}(b) \wedge (b \neq 0)$ **Elim ∃: 1.4**

1.6 $\exists p\ \exists q\ \big((x = p/q) \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge (q \neq 0)\big)$ **Def Rational: 1.3**

1.7 $(y = c/d) \wedge \text{Integer}(c) \wedge \text{Integer}(d) \wedge (d \neq 0)$ **Elim ∃: 1.4**

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) := $\exists a\ \exists b\ (\text{Integer}(a) \wedge \text{Integer}(b) \wedge (x = a/b) \wedge (b \neq 0))$

Prove: "If x and y are rational, then xy is rational."

...

1.5 $(x = a/b) \wedge \text{Integer}(a) \wedge \text{Integer}(b) \wedge (b \neq 0)$

...

1.7 $(y = c/d) \wedge \text{Integer}(c) \wedge \text{Integer}(d) \wedge (d \neq 0)$

Multiplying, we get xy = (ac)/(bd).

1.10 $xy = (a/b)(c/d) = (ac/bd) = (ac)/(bd)$

Algebra

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) := $\exists a\ \exists b\ (\text{Integer}(a) \wedge \text{Integer}(b) \wedge (x = a/b) \wedge (b \neq 0))$

Prove: "If x and y are rational, then xy is rational."

...

1.5 $(x = a/b) \wedge \text{Integer}(a) \wedge \text{Integer}(b) \wedge (b \neq 0)$

...

1.7 $(y = c/d) \wedge \text{Integer}(c) \wedge \text{Integer}(d) \wedge (d \neq 0)$

??

Multiplying, we get xy = (ac)/(bd).

1.10 $xy = (a/b)(c/d) = (ac/bd) = (ac)/(bd)$

Algebra

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) := $\exists a\ \exists b\ (\text{Integer}(a) \wedge \text{Integer}(b) \wedge (x = a/b) \wedge (b \neq 0))$

Prove: "If x and y are rational, then xy is rational."

...

1.5 $(x = a/b) \wedge \text{Integer}(a) \wedge \text{Integer}(b) \wedge (b \neq 0)$

...

1.7 $(y = c/d) \wedge \text{Integer}(c) \wedge \text{Integer}(d) \wedge (d \neq 0)$

1.8 $x = a/b$ **Elim ∧: 1.5**

1.9 $y = c/d$ **Elim ∧: 1.7**

Multiplying, we get xy = (ac)/(bd).

1.10 $xy = (a/b)(c/d) = (ac/bd) = (ac)/(bd)$ **Algebra**

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) := $\exists a\ \exists b\ (\text{Integer}(a) \wedge \text{Integer}(b) \wedge (x = a/b) \wedge (b \neq 0))$

Prove: "If x and y are rational, then xy is rational."

...

1.5 $(x = a/b) \wedge \text{Integer}(a) \wedge \text{Integer}(b) \wedge (b \neq 0)$

...

1.7 $(y = c/d) \wedge \text{Integer}(c) \wedge \text{Integer}(d) \wedge (d \neq 0)$

...

	1.11 $b \neq 0$	**Elim ∧: 1.5***
	1.12 $d \neq 0$	**Elim ∧: 1.7**
Since b and d are non-zero, so is bd.	**1.13** $bd \neq 0$	**Prop of Integer Mult**

* Oops, I skipped steps here...

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) := $\exists a\ \exists b\ (\text{Integer}(a) \wedge \text{Integer}(b) \wedge (x = a/b) \wedge (b \neq 0))$

Prove: "If x and y are rational, then xy is rational."

...

1.5 $(x = a/b) \wedge (\text{Integer}(a) \wedge (\text{Integer}(b) \wedge (b \neq 0)))$

...

1.7 $(y = c/d) \wedge (\text{Integer}(c) \wedge (\text{Integer}(d) \wedge (d \neq 0)))$

...

1.11 $\text{Integer}(a) \wedge \big(\text{Integer}(b) \wedge (b \neq 0)\big)$ **Elim ∧: 1.5**

1.12 $\text{Integer}(b) \wedge (b \neq 0)$ **Elim ∧: 1.11**

1.13 $b \neq 0$ **Elim ∧: 1.12**

We left out the parentheses...

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) := $\exists a\ \exists b\ (\text{Integer}(a) \wedge \text{Integer}(b) \wedge (x = a/b) \wedge (b \neq 0))$

Prove: "If x and y are rational, then xy is rational."

…

1.5 $(x = a/b) \wedge \text{Integer}(a) \wedge \text{Integer}(b) \wedge (b \neq 0)$

…

1.7 $(y = c/d) \wedge \text{Integer}(c) \wedge \text{Integer}(d) \wedge (d \neq 0)$

…

1.13 $b \neq 0$ — **Elim ∧: 1.5**

…

1.16 $d \neq 0$ — **Elim ∧: 1.7**

Since b and d are non-zero, so is bd.

1.17 $bd \neq 0$ — **Prop of Integer Mult**

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) := $\exists a\ \exists b\ (\text{Integer}(a) \wedge \text{Integer}(b) \wedge (x = a/b) \wedge (b \neq 0))$

Prove: "If x and y are rational, then xy is rational."

...

1.5 $(x = a/b) \wedge \text{Integer}(a) \wedge \text{Integer}(b) \wedge (b \neq 0)$

...

1.7 $(y = c/d) \wedge \text{Integer}(c) \wedge \text{Integer}(d) \wedge (d \neq 0)$

...

1.19 $\text{Integer}(a)$ — **Elim ∧: 1.5***

...

1.22 $\text{Integer}(b)$ — **Elim ∧: 1.5***

...

1.24 $\text{Integer}(c)$ — **Elim ∧: 1.7***

...

1.27 $\text{Integer}(d)$ — **Elim ∧: 1.7***

1.28 $\text{Integer}(ac)$ — **Prop of Integer Mult**

1.29 $\text{Integer}(bd)$ — **Prop of Integer Mult**

Furthermore, ac and bd are integers.

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) := $\exists a\ \exists b\ (\text{Integer}(a) \wedge \text{Integer}(b) \wedge (x = a/b) \wedge (b \neq 0))$

Prove: "If x and y are rational, then xy is rational."

...

1.10 $xy = (a/b)(c/d) = (ac/bd) = (ac)/(bd)$

...

1.17 $bd \neq 0$ — **Prop of Integer Mult**

...

1.28 $\text{Integer}(ac)$ — **Prop of Integer Mult**

1.29 $\text{Integer}(bd)$ — **Prop of Integer Mult**

1.30 $\text{Integer}(bd) \wedge (bd \neq 0)$ — **Intro ∧: 1.29, 1.17**

1.31 $\text{Integer}(ac) \wedge \text{Integer}(bd) \wedge (bd \neq 0)$ — **Intro ∧: 1.28, 1.30**

1.32 $(xy = (a/b)/(c/d)) \wedge \text{Integer}(ac) \wedge \text{Integer}(bd) \wedge (bd \neq 0)$ — **Intro ∧: 1.10, 1.31**

1.33 $\exists p\ \exists q\ \left((xy = p/q) \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge (q \neq 0)\right)$ — **Intro ∃: 1.32**

1.34 $\text{Rational}(xy)$ — **Def of Rational: 1.3**

By definition, then, xy is rational.

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) := $\exists a\ \exists b\ (\text{Integer}(a) \wedge \text{Integer}(b) \wedge (x = a/b) \wedge (b \neq 0))$

Prove: "If x and y are rational, then xy is rational."

Suppose x and y are rational.	**1.1** $\text{Rational}(x) \wedge \text{Rational}(y)$	**Assumption**
	...	
	1.10 $xy = (a/b)(c/d) = (ac/bd) = (ac)/(bd)$	
	...	
	1.17 $bd \neq 0$	**Prop of Integer Mult**
	...	
Furthermore, ac and bd are integers.	**1.28** $\text{Integer}(ac)$	**Prop of Integer Mult**
	1.29 $\text{Integer}(bd)$	**Prop of Integer Mult**
	...	
By definition, then, xy is rational.	**1.34** $\text{Rational}(xy)$	**Def of Rational: 1.32**

And finally...

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) := $\exists a\ \exists b\ (\text{Integer}(a) \wedge \text{Integer}(b) \wedge (x = a/b) \wedge (b \neq 0))$

Prove: "If x and y are rational, then xy is rational."

Suppose x and y are rational.	**1.1** $\text{Rational}(x) \wedge \text{Rational}(y)$	**Assumption**
	...	
	1.10 $xy = (a/b)(c/d) = (ac/bd) = (ac)/(bd)$	
	...	
	1.17 $bd \neq 0$	**Prop of Integer Mult**
	...	
Furthermore, ac and bd are integers.	**1.28** $\text{Integer}(ac)$	**Prop of Integer Mult**
	1.29 $\text{Integer}(bd)$	**Prop of Integer Mult**
	...	
By definition, then, xy is rational.	**1.34** $\text{Rational}(xy)$	**Def of Rational: 1.32**

1. $\text{Rational}(x) \wedge \text{Rational}(y) \rightarrow \text{Rational}(xy)$

Direct Proof

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) := $\exists a\ \exists b\ (\text{Integer}(a) \wedge \text{Integer}(b) \wedge (x = a/b) \wedge (b \neq 0))$

Prove: "If x and y are rational, then xy is rational."

Proof: Suppose x and y are rational.

Then, x = a/b for some integers a, b, where b≠0, and y = c/d for some integers c,d, where d≠0.

Multiplying, we get that xy = (ac)/(bd). Since b and d are both non-zero, so is bd. Furthermore, ac and bd are integers. By definition, then, xy is rational. ■

vs more than 35 lines of formal proof

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 can be tedious and impractical
  - e.g., applications of commutativity and associativity
  - Russell & Whitehead's formal proof that 1+1 = 2 is *several hundred pages* long

    we allow ourselves to cite "Arithmetic", "Algebra", etc.

- *Historically*, rarely used for "real mathematics"...

English Proofs

- Vastly more common in CS and math

- High-level language that lets us work more quickly
  - not necessary to spell out *every* detail
  - reader checks that the writer is not skipping too much

    the reader is the "compiler" for English proofs

    they implement a community standard of correctness

- English proofs require understanding formal proofs
  - English proof follows the structure of a formal proof
  - we will learn English proofs by translating from formal

    eventually, we will write English directly

English Proofs

- Vastly more common in CS and math

- High-level language that lets us work more quickly
  - not necessary to spell out *every* detail
  - reader checks that the writer is not skipping too much

    the reader is the "compiler" for English proofs

    they implement a community standard of correctness

- Examples of what can be skipped (more to come):
  - Intro and Elim $\wedge$
  - explicitly stating existence claims (Elim $\exists$ immediately)
  - explicitly invoking Direct Proof (clear from context)