CSE 311: Foundations of Computing

Topic 4: Proofs

... LET'S ASSUME THERE EXISTS SOME FUNCTION F(a,b,c...) WHICH PRODUCES THE CORRECT ANSWER–
HANG ON.
THIS IS GOING TO BE ONE OF THOSE WEIRD, DARK-MAGIC PROOFS, ISN'T IT? I CAN TELL.
WHAT? NO, NO, IT'S A PERFECTLY SENSIBLE CHAIN OF REASONING.
ALL RIGHT...
NOW, LET'S ASSUME THE CORRECT ANSWER WILL EVENTUALLY BE WRITTEN ON THIS BOARD AT THE COORDINATES (x, y). IF WE–
I KNEW IT!

Logical Inference

- So far, we've considered:
  - how to understand and *express* things using propositional and predicate logic
  - how to *compute* using Boolean (propositional) logic
  - 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)	$\mathrm{A} \rightarrow \mathrm{B}$
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?

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

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

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

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

My First Proof!

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

1.	p	Given
2.	$p \to q$	Given
3.	$q \to r$	Given
4.		
5.		

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

My First Proof!

Show that r follows from p, p → q, and q → r

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

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

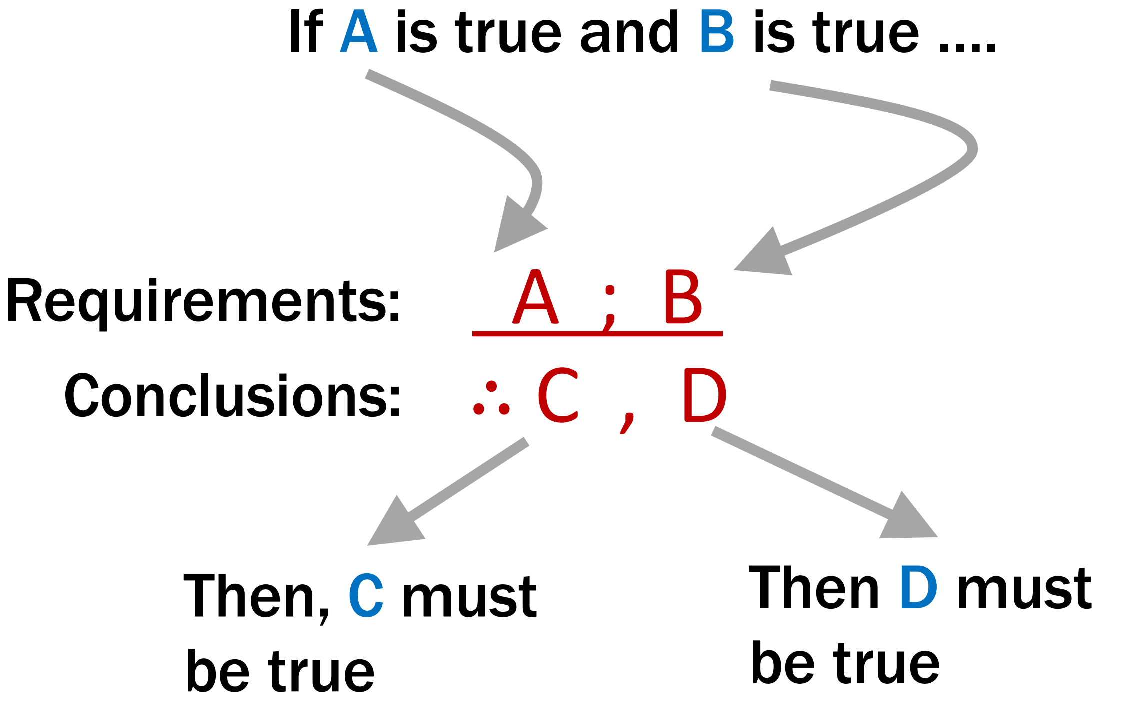
Proofs can use equivalences too

Show that $\neg p$ follows from $p \to q$ and $\neg q$

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

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

Inference Rules



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

Requirements: $\underline{\;A\;;\;B\;}$

Conclusions: $\therefore\ C\ ,\ D$

Then, C must be true

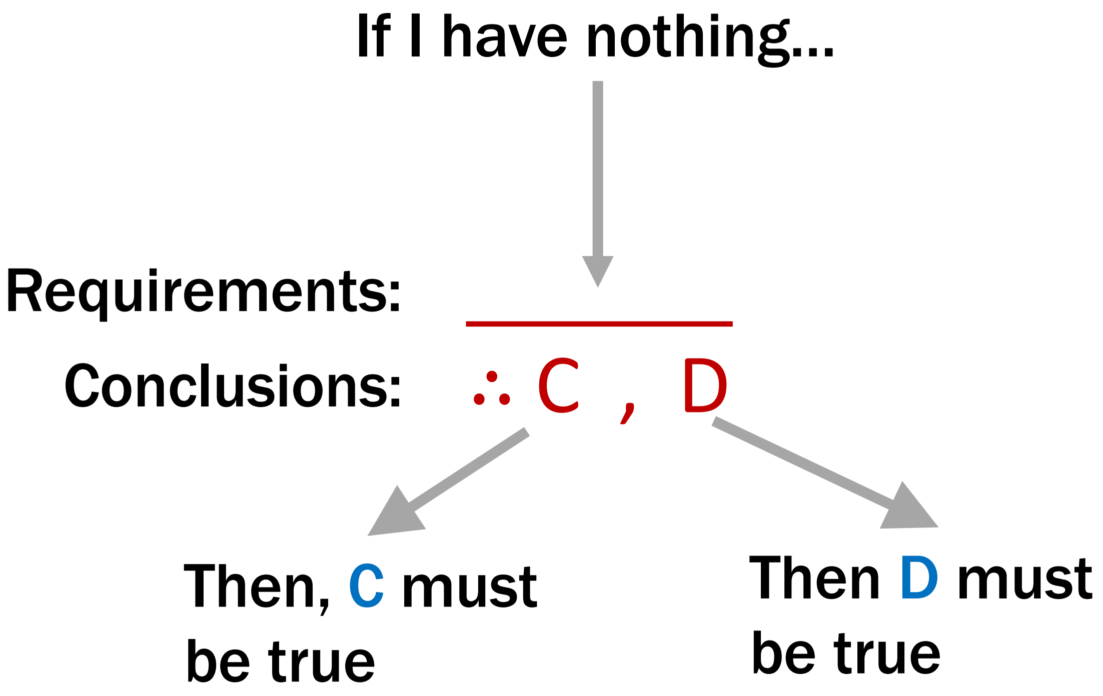
Then D must be true

Example (Modus Ponens):

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

If I have A and A → B both true,
Then B must be true.

Axioms: Special inference rules



If I have nothing…

Requirements: $\overline{}$

Conclusions: $\therefore C \ , \ D$

Then, C must be true

Then D must be true

Example (Excluded Middle):

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

A ∨¬A must be true.

Simple 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 $p \wedge q \rightarrow r$

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!

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

$$\dfrac{\dfrac{p \;\; ; \;\; \dfrac{p \; ; \; p \rightarrow q}{q}\,\text{MP}}{p \wedge q}\,\text{Intro} \wedge \quad ; \quad p \wedge q \rightarrow r}{r}\,\text{MP}$$

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
20.	$\neg r$	?

First: Write down givens and goal

Idea: Work backwards!

Proofs

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

1.	$p \land s$	Given
2.	$q \to \neg r$	Given
3.	$\neg s \lor q$	Given
20.	$\neg r$	MP: 2, ?

Idea: Work backwards!

We want to eventually get $\neg r$. How?

- We can use $q \to \neg r$ to get there.
- The justification between 2 and 20 looks like "elim →" 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 ¬r follows from p ∧ s, q → ¬r, and ¬s ∨ q.

1. $p \land s$ Given

2. $q \to \neg r$ Given

3. $\neg s \lor q$ Given

This looks like or-elimination.

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

19. q ?

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

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
18.	$\neg\neg s$	?
19.	q	$\lor$ 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 $\neg r$ 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

Proofs

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

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

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

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

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

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	$A \to B$
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?

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

Recall: 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

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

1. q Given

2. $(p \wedge q) \to r$ Given

This is a proof of $p \to r$

- 3.1. p Assumption
- 3.2.
- 3.3. r ??

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

3. $p \to r$ 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: $(p \wedge q) \rightarrow (p \vee q)$

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

1.1.	$p \land q$	Assumption
1.2.	p	Elim $\land$: 1.1
1.3.	$p \lor q$	Intro $\lor$: 1.2
1.	$(p \land q) \rightarrow (p \lor q)$	Direct Proof

One General Proof Strategy

1. Look at the rules for introducing connectives to see how you would build up the formula you want to prove from pieces of what is given

2. Use the rules for eliminating connectives to break down the given formulas so that you get the pieces you need to do 1.

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

Example

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

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

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.? $p \rightarrow r$

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.? r

1.4. $p \rightarrow r$ Direct Proof

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

Example

Prove: $((\mathrm{p} \rightarrow \mathrm{q}) \wedge (\mathrm{q} \rightarrow \mathrm{r})) \rightarrow (\mathrm{p} \rightarrow \mathrm{r})$

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

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

not non-contradiction

More Rules for Propositional Logic

More rules makes proofs easier

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

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

Tautology

$$\frac{A \equiv T}{\therefore A}$$

includes Excluded Middle as a special case but gives you *every* tautology

More Rules for Propositional Logic

More rules makes proofs easier

Principium Contradictionis

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

Reductio Ad Absurdum

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

Ex Falso Quodlibet

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

Ad Litteram Verum

$$\frac{\quad}{\therefore\ T}$$

useful for proving things
without the Tautology rule

remember that Tautology takes 2^n time!
(for CS reasons, Tautology is different)

More Rules for Propositional Logic

More rules makes proofs easier

Elim ∧

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

Intro ∧

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

Elim ∨

$$\frac{A \lor B \,;\, \neg A}{\therefore B}$$

Intro ∨

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

Modus Ponens

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

Direct Proof

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

Tautology

$$\frac{A \equiv T}{\therefore A}$$

Equivalent

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

Alternative Rules

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

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

Equivalent seems more general (take B = T)

How do we use Equivalent to do the work of Tautology?

1. A **Equivalent** $(A \equiv T)$ **?**

Alternative Rules

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

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

Equivalent seems more general (take B = T)

How do we use Equivalent to do the work of Tautology?

1.	**T**	**Ad Litteram Verum**
2.	A	**Equivalent** (A ≡ T) **1**

Alternative Rules

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

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

Actually, Equivalent is not more general!

How do we use Tautology to do the work of Equivalent?

$A \equiv B$ **holds iff** $(A \longleftrightarrow B) \equiv T$ **holds**

Other Rules for Propositional Logic

Some rules can be written in different ways

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

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

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

will see in **HW3** that these rules are equally capable

Rules for Propositional Logic w/o Tautology

	Elimination	Introduction
∧	Elim ∧	Intro ∧
∨	Cases	Intro ∨
→	Modus Ponens	Direct Proof
¬	Principium Contradictionis	Reductio Ad Absurdum
F	Ex Falso Quodlibet	
T		Ad Litteram Verum

why no introduction rule for F?

Rules for Propositional Logic

	Elimination	Introduction
∧	Elim ∧	Intro ∧
∨	Cases	Intro ∨
→	Modus Ponens	Direct Proof
¬	Principium Contradictionis	Reductio Ad Absurdum
F / T	Ex Falso Quodlibet	Ad Litteram Verum

- **These exact rules also show up in CS!** See HW3 EC!
  - **as typing rules for a functional programming language**
  - **"Curry-Howard" isomorphism says Proofs = Programs**

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 must be a NEW name!

My First Predicate Logic Proof

Domain of Discourse
Integers

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

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

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

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

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

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

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

Intro ∃: P(c) for some c
∴ ∃x P(x)

Elim ∀: ∀x P(x)
∴ P(a) for any a

Prove ∀x P(x) → ∃x P(x)

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

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

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

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

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

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

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

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

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

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

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

Working forwards as well as backwards:
In applying “Intro ∃” 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
$\mathrm{Even}(x) := \exists y\,(x = 2 \cdot y)$
$\mathrm{Odd}(x) := \exists y\,(x = 2 \cdot y + 1)$

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

$\text{Even}(x) := \exists y\, (x = 2 \cdot y)$

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

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** ∃**: 1**
3.	$\text{Even}(\mathbf{2})$	**Definition of** Even**: 2**
4.	$\exists x\, \text{Even}(x)$	**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) := "x > 1 and x≠a·b for
all integers a, b with 1<a<x"

Prove "There is an even prime number"

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

A Prime Example

Domain of Discourse

Integers

Predicate Definitions

$\text{Even}(x) := \exists y\ (x = 2\cdot y)$

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

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

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

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

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

Intro ∀ "Let a be arbitrary*"...$P(a)$
$\therefore\ \forall x\, P(x)$

Elim ∃ $\exists x\, P(x)$
$\therefore\ P(c)$ **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 and Odd

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

Intro ∀

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

Elim ∃

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

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

Even and Odd

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

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

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

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

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

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

Formal proof of: ∀x (Even(x) → Even(x^2))

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

   2.1 Even(**a**) Assumption

   2.6 Even(**a**^{2}) ?

2. Even(**a**)→Even(**a**^{2}) Direct proof
3. ∀x (Even(x)→Even(x^2)) Intro ∀: 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)
$\therefore\ \forall x\, P(x)$

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

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

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

Elim ∃ $\dfrac{\exists x\, P(x)}{\therefore P(c) \text{ for some special** } c}$

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

    2.2 ∃y (**a** = 2y) Definition of Even

    2.5 $\exists y\, (\mathbf{a}^2 = 2y)$ Intro ∃: ?

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

2. $\text{Even}(\mathbf{a}) \rightarrow \text{Even}(\mathbf{a}^2)$ Direct proof
3. $\forall x\, (\text{Even}(x) \rightarrow \text{Even}(x^2))$ Intro ∀: 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 ∀ $$\frac{\text{“Let } a \text{ be arbitrary*”}\ldots P(a)}{\therefore \quad \forall x\, P(x)}$$

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 ∃: b

2.5 $\exists y\,(a^2 = 2y)$ Intro ∃:
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 ∀: 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
2.2	$\exists y\,(a = 2y)$	Definition of Even
2.3	$a = 2b$	Elim ∃: **b**
2.5	$\exists y\,(a^2 = 2y)$	Intro ∃: ?
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 ∀: 1,2

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

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

Even and Odd

Intro ∀ $\dfrac{\text{“Let } a \text{ be arbitrary*”}\ldots P(a)}{\therefore\ \forall x\, P(x)}$

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

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

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

1.	Let **a** be an arbitrary integer	
2.1	Even(**a**)	Assumption
2.2	$\exists y\, (\mathbf{a} = 2y)$	Definition of Even
2.3	$\mathbf{a} = 2\mathbf{b}$	Elim ∃: **b**
2.4	$\mathbf{a}^2 = 4\mathbf{b}^2 = 2(2\mathbf{b}^2)$	Algebra
2.5	$\exists y\, (\mathbf{a}^2 = 2y)$	Intro ∃
2.6	$\mathrm{Even}(\mathbf{a}^2)$	Definition of Even
2.	$\mathrm{Even}(\mathbf{a}) \rightarrow \mathrm{Even}(\mathbf{a}^2)$	Direct Proof
3.	$\forall x\, (\mathrm{Even}(x) \rightarrow \mathrm{Even}(x^2))$	Intro ∀: 1,2

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

Inference Rules for Quantifiers: Full version

Intro ∃

P(c) for some c

∴ ∃x P(x)

Elim ∀

∀x P(x)

∴ P(a) **for any** a

Elim ∃

∃x P(x)

∴ P(c) **for some *special*** ** c

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

Intro ∀

“**Let** a **be arbitrary***”...P(a)

∴ ∀x P(x)

* 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 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 allowed ourselves to cite "Arithmetic", "Algebra", etc.

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

Formal vs English Proofs

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

- English proofs are easier for humans to read
  - "high level language" (like Java) for proofs
  - also easy to check with practice

    (almost all actual math and theory CS is done this way)
  - English proof is correct if the reader believes they could translate it into a formal proof

    (the reader is the "compiler" for English proofs)

Formal vs English Proofs

- Current math practice is changing
  - computer tools for writing formal proofs are improving
  - more mathematicians are writing them (e.g., Terry Tao)

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

    eventually, we will write English directly

Recall: Even and Odd

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

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

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

1.	Let $\mathbf{a}$ be an arbitrary integer	
2.1	Even($\mathbf{a}$)	Assumption
2.2	$\exists y\ (\mathbf{a} = 2y)$	Definition of Even
2.3	$\mathbf{a} = 2\mathbf{b}$	Elim $\exists$
2.4	$\mathbf{a}^2 = 4\mathbf{b}^2 = 2(2\mathbf{b}^2)$	Algebra
2.5	$\exists y\ (\mathbf{a}^2 = 2y)$	Intro $\exists$
2.6	Even($\mathbf{a}^2$)	Definition of Even
2.	Even($\mathbf{a}$)$\rightarrow$Even($\mathbf{a}^2$)	Direct Proof
3.	$\forall x\ (\text{Even}(x)\rightarrow\text{Even}(x^2))$	Intro $\forall$

English Proof: Even and Odd

$\text{Even}(x) \equiv \exists y\ (x=2y)$
$\text{Odd}(x) \equiv \exists y\ (x=2y+1)$
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	$\text{Even}(\mathbf{a})$	Assumption
Then, by definition, $\mathbf{a} = 2\mathbf{b}$ for some integer **b**.	2.2	$\exists y\ (\mathbf{a} = 2y)$	Definition
	2.3	$\mathbf{a} = 2\mathbf{b}$	Elim $\exists$
Squaring both sides, we get $\mathbf{a}^2 = 4\mathbf{b}^2 = 2(2\mathbf{b}^2)$.	2.4	$\mathbf{a}^2 = 4\mathbf{b}^2 = 2(2\mathbf{b}^2)$	Algebra
So $\mathbf{a}^2$ is, by definition, even.	2.5	$\exists y\ (\mathbf{a}^2 = 2y)$	Intro $\exists$
	2.6	$\text{Even}(\mathbf{a}^2)$	Definition
Since **a** was arbitrary, we have shown that the square of every even number is even.	2.	$\text{Even}(\mathbf{a}) \rightarrow \text{Even}(\mathbf{a}^2)$	Direct Proof
	3.	$\forall x\ (\text{Even}(x) \rightarrow \text{Even}(x^2))$	Intro $\forall$

English Proof: Even and Odd

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."

Proof: Let **a** be an arbitrary integer.

Suppose **a** is even. Then, by definition, **a** = 2**b** 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

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

Prove "The square of every even integer is even."

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

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

Since **a** was arbitrary, we have shown that the square of every even number is even. ■

$$\forall x\ (\mathrm{Even}(x) \rightarrow \mathrm{Even}(x^2))$$

Even and Odd

Predicate Definitions

Even(x) ≡ $\exists y\ (x = 2y)$

Odd(x) ≡ $\exists y\ (x = 2y + 1)$

Domain of Discourse

Integers

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

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

Even and Odd

Predicate Definitions

Even(x) ≡ $\exists y\ (x = 2y)$

Odd(x) ≡ $\exists y\ (x = 2y + 1)$

Domain of Discourse

Integers

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

Formally, prove ∀x ∀y ((Odd(x) ∧ Odd(y))→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 any odd integers is even.

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

Even and Odd

Predicate Definitions

Even(x) $\equiv \exists y\ (x = 2y)$

Odd(x) $\equiv \exists y\ (x = 2y + 1)$

Domain of Discourse

Integers

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

Formally, prove ∀x ∀y ((Odd(x) ∧ Odd(y))→Even(x+y))

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**) ∧ Odd(**y**) Assumption
so x+y is even.	**3.9** Even(**x+y**)
Since x and y were arbitrary, the sum of any odd integers is even.	**3.** (Odd(**x**) ∧ Odd(**y**)) → Even(**x+y**) DPR **4.** ∀x ∀y ((Odd(**x**) ∧ Odd(**y**)) → Even(x+y)) Intro ∀

Even and Odd

Predicate Definitions

Even(x) ≡ $\exists y\ (x = 2y)$

Odd(x) ≡ $\exists y\ (x = 2y + 1)$

Domain of Discourse

Integers

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

Formally, prove ∀x ∀y ((Odd(x) ∧ Odd(y))→Even(x+y))

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**) ∧ Odd(**y**) Assumption **3.2** Odd(**x**) Elim ∧: 2.1 **3.3** Odd(**y**) Elim ∧: 2.1
so x+y is even.	**3.9** Even(**x+y**)
Since x and y were arbitrary, the sum of any odd integers is even.	**3.** (Odd(**x**) ∧ Odd(**y**)) → Even(**x+y**) DPR **4.** ∀x ∀y ((Odd(**x**) ∧ Odd(**y**)) → Even(x+y)) Intro ∀

English Proof: Even and Odd

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

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	$\text{Odd}(\mathbf{x}) \wedge \text{Odd}(\mathbf{y})$	Assumption
3.2	$\text{Odd}(\mathbf{x})$	Elim ∧: 2.1
3.3	$\text{Odd}(\mathbf{y})$	Elim ∧: 2.1

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

3.4	$\exists \mathbf{z}\ (\mathbf{x} = 2\mathbf{z}+1)$	Def of Odd: 2.2
3.5	$\mathbf{x} = 2\mathbf{a}+1$	Elim ∃: 2.4
3.6	$\exists \mathbf{z}\ (\mathbf{y} = 2\mathbf{z}+1)$	Def of Odd: 2.3
3.7	$\mathbf{y} = 2\mathbf{b}+1$	Elim ∃: 2.5

so x+y is, by definition, even.

3.9	$\exists z\ (\mathbf{x+y} = 2z)$	Intro ∃: 2.4
3.10	$\text{Even}(\mathbf{x+y})$	Def of Even

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

3.	$(\text{Odd}(\mathbf{x}) \wedge \text{Odd}(\mathbf{y})) \rightarrow \text{Even}(\mathbf{x+y})$	DPR
4.	$\forall x\ \forall y\ ((\text{Odd}(\mathbf{x}) \wedge \text{Odd}(\mathbf{y})) \rightarrow \text{Even}(\mathbf{x+y}))$	Intro ∀

English Proof: Even and Odd

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

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**	
	3.1	$\text{Odd}(\mathbf{x}) \land \text{Odd}(\mathbf{y})$	Assumption
Suppose that both are odd.	3.2	$\text{Odd}(\mathbf{x})$	Elim ∧: 2.1
	3.3	$\text{Odd}(\mathbf{y})$	Elim ∧: 2.1
Then, we have x = 2a+1 for some integer a and y = 2b+1 for some integer b.	3.4	$\exists \mathbf{z}\ (\mathbf{x} = 2\mathbf{z}+1)$	Def of Odd: 2.2
	3.5	$\mathbf{x} = 2\mathbf{a}+1$	Elim ∃: 2.4
	3.6	$\exists \mathbf{z}\ (\mathbf{y} = 2\mathbf{z}+1)$	Def of Odd: 2.3
	3.7	$\mathbf{y} = 2\mathbf{b}+1$	Elim ∃: 2.5
Their sum is x+y = ... = 2(a+b+1)	3.8	$\mathbf{x+y} = 2(\mathbf{a}+\mathbf{b}+\mathbf{1})$	Algebra
	3.9	$\exists z\ (\mathbf{x+y} = 2z)$	Intro ∃: 2.4
so x+y is, by definition, even.	3.10	$\text{Even}(\mathbf{x+y})$	Def of Even
Since x and y were arbitrary, the sum of any odd integers is even.	3.	$(\text{Odd}(\mathbf{x}) \land \text{Odd}(\mathbf{y})) \rightarrow \text{Even}(\mathbf{x+y})$	DPR
	4.	$\forall x\ \forall y\ ((\text{Odd}(\mathbf{x}) \land \text{Odd}(\mathbf{y})) \rightarrow \text{Even}(\mathbf{x+y}))$	Intro ∀

Even and Odd

Predicate Definitions

Even(x) ≡ $\exists y\ (x = 2y)$

Odd(x) ≡ $\exists y\ (x = 2y + 1)$

Domain of Discourse

Integers

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. ■

Even and Odd

Predicate Definitions

Even(x) ≡ $\exists y\ (x = 2y)$

Odd(x) ≡ $\exists y\ (x = 2y + 1)$

Domain of Discourse

Integers

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.

■

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

Rational Numbers

Domain of Discourse
Real Numbers

- A real number x is *rational* iff there exist integers a and b with $b \neq 0$ such that $x=a/b$.

Rational(x) := ∃a ∃b (((Integer(a) ∧ Integer(b)) ∧ (x=a/b)) ∧ b≠0)

Rationality

Domain of Discourse
Real Numbers

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

Prove: "The product of two rationals is rational."

Formally, prove $\forall x\ \forall y\ ((\text{Rational}(x) \land \text{Rational}(y)) \to \text{Rational}(xy))$

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: "The product of two rationals is rational."

Proof: Let x and y be arbitrary rationals.

Since x and y were arbitrary, we have shown that the product of any two rationals 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: "The product of two rationals is rational."

Proof: Let x and y be arbitrary rationals.

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

By definition, then, xy is rational.

Since x and y were arbitrary, we have shown that the product of any two rationals is rational. ■

Rationality

Domain of Discourse
Real Numbers

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

Prove: "The product of two rationals is rational."

Proof: Let x and y be arbitrary rationals.

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.

Since x and y were arbitrary, we have shown that the product of any two rationals is rational. ■

Rationality

Domain of Discourse

Real Numbers

Predicate Definitions

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

Prove: "The product of two rationals is rational."

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

Recall that unquantified variables (not constants) are implicitly for-all quantified.

$\forall x\ \forall y\ ((\text{Rational}(x) \land \text{Rational}(y)) \rightarrow \text{Rational}(xy))$

Rationality

Domain of Discourse
Real Numbers

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

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

Proof: ~~Let x and y be arbitrary rationals.~~
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 = (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.

~~Since x and y were arbitrary, we have shown that the product of any two rationals is rational.~~ ■

Rationality

Domain of Discourse

Real Numbers

Predicate Definitions

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

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

Suppose x and y are rational.

1.1 $\text{Rational}(x) \land \text{Rational}(y)$ **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 $\exists p\, \exists q\, ((x = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0))$

Def Rational: 1.2

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

Elim ∃: 1.4

1.6 $\exists p\, \exists q\, \big((x = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0)\big)$

Def Rational: 1.3

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

Elim ∃: 1.4

Rationality

Domain of Discourse

Real Numbers

Predicate Definitions

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

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

Suppose x and y are rational.

1.1 $\text{Rational}(x) \land \text{Rational}(y)$ **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 $\exists p\ \exists q\ ((x = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0))$

Def Rational: 1.2

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

Elim ∃: 1.4

1.6 $\exists p\ \exists q\ ((x = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0))$

Def Rational: 1.3

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

Elim ∃: 1.4

…

Rationality

Domain of Discourse
Real Numbers

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

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

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

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

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

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

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

1.7 $(y = c/d) \land \text{Integer}(c) \land \text{Integer}(d) \land (d \neq 0)$
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) := $\exists a\ \exists b\ (\text{Integer}(a) \land \text{Integer}(b) \land (x = a/b) \land (b \neq 0))$

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

...

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

...

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

??

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

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

...

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

...

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

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

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

…

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

…

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

…

1.11 $\text{Integer}(a) \land \left(\text{Integer}(b) \land (b \neq 0)\right)$

Elim ∧: 1.5

1.12 $\text{Integer}(b) \land (b \neq 0)$ **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) := $\exists a\ \exists b\ (\text{Integer}(a) \land \text{Integer}(b) \land (x = a/b) \land (b \neq 0))$

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

…

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

…

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

…

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

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

...	
1.5 $(x = a/b) \land \text{Integer}(a) \land \text{Integer}(b) \land (b \neq 0)$	
...	
1.7 $(y = c/d) \land \text{Integer}(c) \land \text{Integer}(d) \land (d \neq 0)$	
...	
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) := $\exists a\ \exists b\ (\text{Integer}(a) \land \text{Integer}(b) \land (x = a/b) \land (b \neq 0))$

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

1.31 $\text{Integer}(ac) \land \text{Integer}(bd) \land (bd \neq 0)$

Intro ∧: 1.28, 1.30

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

1.33 $\exists p\ \exists q\ \left((xy = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0)\right)$

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) := $\exists a\ \exists b\ (\mathrm{Integer}(a) \land \mathrm{Integer}(b) \land (x = a/b) \land (b \neq 0))$

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

Suppose x and y are rational.	**1.1**	$\mathrm{Rational}(x) \land \mathrm{Rational}(y)$	**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**	$\mathrm{Integer}(ac)$	**Prop of Integer Mult**
	1.29	$\mathrm{Integer}(bd)$	**Prop of Integer Mult**
	...		
By definition, then, xy is rational.	**1.34**	$\mathrm{Rational}(xy)$	**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) := $\exists a\ \exists b\ (\text{Integer}(a) \land \text{Integer}(b) \land (x = a/b) \land (b \neq 0))$

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

English Proofs

- High-level language let us work more quickly
  - should not be necessary to spill out every detail
  - <u>reader</u> checks that the writer is not skipping too much
  - examples so far

    skipping Intro ∧ and Elim ∧

    not stating existence claims (immediately apply Elim ∃ to name the object)

    not stating that the implication has been proven ("Suppose X... Thus, Y." says it already)
  - (list will grow over time)

- English proof is correct if the <u>reader</u> believes they could translate it into a formal proof
  - the reader is the "compiler" for English proofs

Proof Strategies

Proof Strategies: Counterexamples

To prove $\neg\forall x\ P(x)$, prove $\exists\neg P(x)$:

- Equivalent by De Morgan's Law
- All we need to do that is find an x where $P(x)$ is **false**
- This example is called a ***counterexample*** to $\forall x\ P(x)$.

e.g. Prove "Not every prime number is odd"

Proof: 2 is a prime that is not odd — a counterexample to the claim that every prime number is odd. ■

An English proof does not need to cite De Morgan's law.

Proof Strategies: Proof by Contrapositive

If we assume ¬q and derive ¬p, then we have proven ¬q → ¬p, which is equivalent to proving p → q.

1.1. $\neg q$ Assumption

...

1.3. $\neg p$

1. $\neg q \rightarrow \neg p$ Direct Proof

2. $p \rightarrow q$ Contrapositive: 1

Proof Strategies: Proof by Contrapositive

If we assume $\neg$q and derive $\neg$p, then we have proven $\neg$q → $\neg$p, which is equivalent to proving p → q.

We will proved the contrapositive.

Suppose $\neg q$.

…

Thus, $\neg p$.

1.1.	$\neg q$	Assumption
…		
1.3.	$\neg p$	
1.	$\neg q \rightarrow \neg p$	Direct Proof
2.	$p \rightarrow q$	Contrapositive: 1

Proof by Contradiction: One way to prove ¬p

If we assume p and derive F (a contradiction), then we have proven ¬p.

1.1. p Assumption

...

1.3. F

1. $p \rightarrow \mathrm{F}$ Direct Proof
2. $\neg p \vee \mathrm{F}$ Law of Implication: 1
3. $\neg p$ Identity: 2

Proof Strategies: Proof by Contradiction

If we assume p and derive F (a contradiction), then we have proven $\neg$p.

We will argue by contradiction.

Suppose p.

...

This is a contradiction.

1.1.	p	Assumption
...		
1.3.	F	
1.	$p \rightarrow \mathrm{F}$	Direct Proof
2.	$\neg p \vee \mathrm{F}$	Law of Implication: 1
3.	$\neg p$	Identity: 2

Often, we will infer $\neg$R, where R is a prior fact.
Putting these together, we have $\mathrm{R} \wedge \neg \mathrm{R} \equiv \mathrm{F}$

Even and Odd

Predicate Definitions

Even(x) ≡ $\exists y\ (x = 2y)$

Odd(x) ≡ $\exists y\ (x = 2y + 1)$

Domain of Discourse

Rationals

Prove: "No integer is both even and odd."

Formally, prove $\neg \exists x\ (\mathrm{Even}(x) \land \mathrm{Odd}(x))$

Proof: We will argue by contradiction.

Even and Odd

Predicate Definitions

Even(x) ≡ $\exists y\ (x = 2y)$

Odd(x) ≡ $\exists y\ (x = 2y + 1)$

Domain of Discourse

Rationals

Prove: "No integer is both even and odd."

Formally, prove $\neg \exists x\ (\text{Even}(x) \wedge \text{Odd}(x))$

Proof: We will argue by contradiction.

Suppose that x is an integer that is both even and odd.

This is a contradiction. ■

Even and Odd

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

Domain of Discourse
Rationals

Prove: "No integer is both even and odd."

Formally, prove $\neg\,\exists x\ (\mathrm{Even}(x) \wedge \mathrm{Odd}(x))$

Proof: We will argue by contradiction.

Suppose that x is an integer that is both even and odd. Then, x=2a for some integer a, and x=2b+1 for some integer b.

This is a contradiction. ■

Even and Odd

Predicate Definitions

Even(x) ≡ $\exists y\ (x = 2y)$

Odd(x) ≡ $\exists y\ (x = 2y + 1)$

Domain of Discourse

Rationals

Prove: "No integer is both even and odd."

Formally, prove ¬ ∃x (Even(x)∧Odd(x))

Proof: We will argue by contradiction.

Suppose that x is an integer that is both even and odd. Then, x=2a for some integer a, and x=2b+1 for some integer b. This means 2a=x=2b+1 and hence 2a-2b=1 and so a-b=½. But a-b is an integer while ½ is not, so they cannot be equal. This is a contradiction. ■

Formally, we've shown Integer(½) ∧ ¬Integer(½) ≡ F.

Strategies

- Simple proof strategies already do a lot
  - counter examples
  - proof by contrapositive
  - proof by contradiction

- Later we will cover a specific strategy that applies to loops and recursion (mathematical induction)