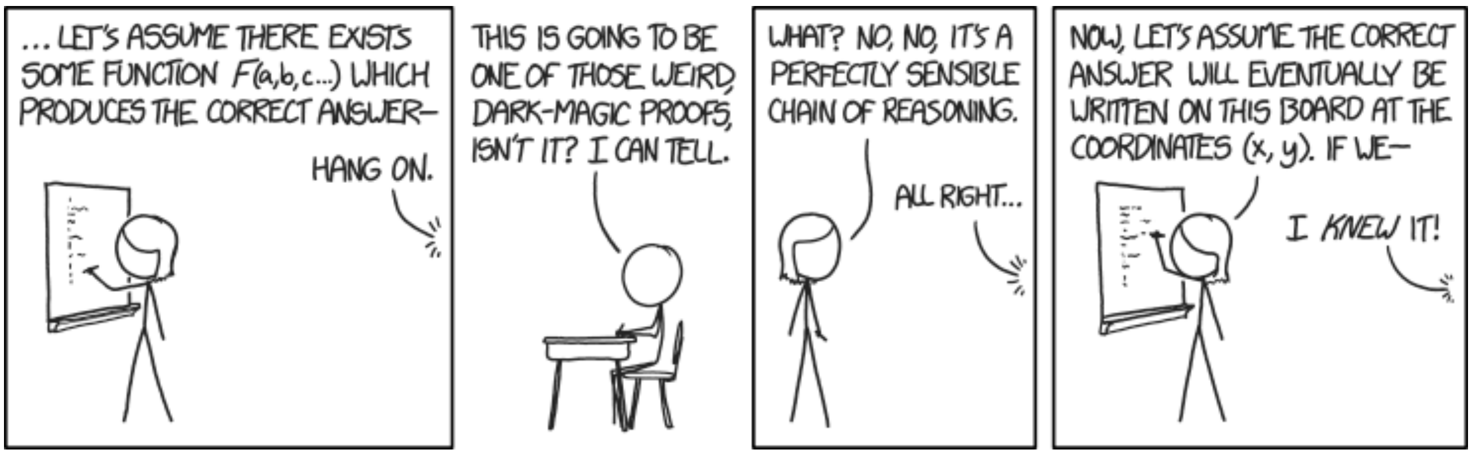
CSE 311: Foundations of Computing

Topic 3: Proofs



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

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 $\rightarrow$ 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?

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

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

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

- 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 → q, and q → 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 → q, and q → 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 → q and ¬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: $\underline{\quad A \;;\; B \quad}$

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

Then, C must be true

Then D must be 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

If I have nothing...

Requirements:

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

Then, C must be true

Then D must be true

Example (Excluded Middle):

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

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

Simple Propositional Inference Rules

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

Elim ∧

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

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

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

Proofs

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

How To Start:

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

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

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

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

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

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

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

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

Proofs

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

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

Proofs

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

$$\dfrac{p \;;\; p \rightarrow q}{q}\ \text{MP}$$

$$\dfrac{p \;;\; q}{p \wedge q}\ \text{Intro } \wedge$$

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

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

$p \; ; \; p \rightarrow q$
______ MP
$p \; ; \; q$
______ Intro $\wedge$
$p \wedge q \; ; \; p \wedge q \rightarrow r$
______ MP
r

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

20. $\neg r$?

First: Write down givens and goal

Idea: Work backwards!

Proofs

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

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

Idea: Work backwards!

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

- We can use $q \rightarrow \neg r$ to get there.
- The justification between 2 and 20 looks like "elim →" which is MP.

Proofs

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

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

Idea: Work backwards!

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

- Now, we have a new "hole"
- We need to prove q...
  - Notice that at this point, if we prove q, we've proven $\neg r$...

Proofs

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

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

This looks like or-elimination.

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

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

Proofs

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

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

Proofs

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

1.	$p \wedge s$	Given
2.	$q \rightarrow \neg r$	Given
3.	$\neg s \vee q$	Given
17.	s	Elim ∧: 1
18.	$\neg\neg s$	Equivalent: 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	Elim $\wedge$: 1
5.	$\neg\neg s$	Equivalent: 4
6.	q	Elim $\vee$: 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 → 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 ∧
$$\frac{A \wedge B}{\therefore A,\ B}$$

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

There MUST be an application of the Direct Proof Rule (or an equivalence) to prove this implication.

Where do we start? We have no givens…

Example

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

1.1.	$p \land q$	Assumption
1.9.	$p \lor q$	??
1.	$(p \land q) \to (p \lor q)$	Direct Proof

Example

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

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

One General Proof Strategy

1. p Given

...

?. r ?

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

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

One 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.

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: $((p \to q) \land (q \to r)) \to (p \to r)$

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

1.2. $p \to q$ Elim ∧: 1.1

1.3. $q \to r$ Elim ∧: 1.1

1.4.1. p Assumption

1.4.? r

1.4. $p \to r$ Direct Proof

1. $((p \to q) \land (q \to r)) \to (p \to r)$ 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

  1.4.2. q MP: 1.2, 1.4.1

  1.4.3. r MP: 1.3, 1.4.2

1.4. $p \rightarrow r$ Direct Proof

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

Basic Rules for Propositional Logic

Most basic rules are 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

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

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

Rules for Propositional Logic *with Tautology*

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

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

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

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

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 ∨

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

Cases

$$\frac{A \lor B \,;\, A \to C \,;\, B \to C}{\therefore C}$$

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

Inference Rules for Quantifiers: First look

Intro ∃

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

Elim ∀

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

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

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

Intro ∃: P(c) for some c ∴ ∃x P(x)

Elim ∀: ∀x P(x) ∴ P(a) **for any** a

5. $\forall x\ P(x) \to \exists x\ P(x)$?

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

Intro ∃: P(c) for some c ∴ ∃x P(x)

Elim ∀: ∀x P(x) ∴ P(a) **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. $\forall x\ P(x) \to \exists x\ P(x)$ **Direct Proof**

My First Predicate Logic Proof

Domain of Discourse
Integers

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

Intro ∃: P(c) for some c ∴ ∃x P(x)

Elim ∀: ∀x P(x) ∴ P(a) 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 had to guess it. That is not something we should do blindly / automatically.

<u>Lesson</u>: Elim ∀ and Intro ∃ are not rules we can apply *mechanically*

Predicate Logic Proofs

- Can use
  - Predicate logic inference rules

    whole formulas only
  - Predicate logic equivalences (De Morgan's)

    even on subformulas
  - Propositional logic inference rules

    whole formulas only
  - Propositional logic equivalences

    even on subformulas

Predicate Logic Proofs with more content

- In propositional logic we could just write down other propositional logic statements as "givens"

- Here, we also want to be able to use domain knowledge so proofs are about something specific

- Example:

Domain of Discourse
Integers

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

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

A Not so Odd Example

Domain of Discourse
Integers

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

Prove "There is an even number"

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

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

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

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

1.	$2 = 2 \cdot 1$	**Algebra**
2.	$\exists y\ (2 = 2 \cdot y)$	**Intro $\exists$: 1**
3.	Even(**2**)	**Def of** Even**: 3**
4.	Prime(**2**)*	**Property of integers**
5.	Even(**2**) $\wedge$ 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 ∃

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

Intro ∀

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

∴ ∀x P(x)

** By special, we mean that c is a name for a value where P(c) is true. We can't use anything else about that value, so c has to be a NEW name!

* in the domain of P

Even and Odd

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

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

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

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

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

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

Let a be an arbitrary integer

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

1. $\forall x\,(\mathrm{Even}(x) \rightarrow \mathrm{Even}(x^2))$ 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: $\forall x\,(\text{Even}(x) \rightarrow \text{Even}(x^2))$

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

Let a be an arbitrary integer

1.1.1 Even(**a**) Assumption

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

1.1.5 ∃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 ∀	"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: $\forall x\,(\text{Even}(x) \rightarrow \text{Even}(x^2))$

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 ∃ (**b**)
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 ∀

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

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

Let a be an arbitrary integer

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

Even and Odd

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

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

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

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

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

Let **a** be an arbitrary integer

- **1.1.1** Even(**a**) — Assumption
- **1.1.2** $\exists y\, (a = 2y)$ — Definition of Even: 1.1.1
- **1.1.3** $a = 2b$ — Elim ∃ (**b**): 1.1.2
- **1.1.4** $a^2 = 2(2b^2)$ — Algebra: 1.1.3
- **1.1.5** $\exists y\, (a^2 = 2y)$ — Intro ∃: 1.1.4
- **1.1.6** Even(a^2) — Definition of Even: 1.1.5

1.1 $\text{Even}(a) \rightarrow \text{Even}(a^2)$ — Direct proof

1. $\forall x\, (\text{Even}(x) \rightarrow \text{Even}(x^2))$ — Intro ∀

Formal Proofs

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

- 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

English Proofs

- 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

- Vastly more common in computer science

- English proof is correct if the reader believes they could translate it into a formal proof
  - the reader is the "compiler" for English proofs
  - different readers can have different standards!

English Proofs

- 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

- Vastly more common in computer science

- 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

Recall: Even and Odd

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

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

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

Let a be an arbitrary integer

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

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."

English	Formal	Rule
Let a be an arbitrary integer.	Let a be an arbitrary integer	
Suppose a is even.	1.1.1 Even(a)	Assumption
Then, by definition, $a = 2b$ for some integer b.	1.1.2 $\exists y\ (a = 2y)$	Definition
	1.1.3 $a = 2b$	Elim $\exists$
Squaring both sides, we get $a^2 = 4b^2 = 2(2b^2)$.	1.1.4 $a^2 = 2(2b^2)$	Algebra
So a^2 is, by definition, even.	1.1.5 $\exists y\ (a^2 = 2y)$	Intro $\exists$
	1.1.6 Even(a^2)	Definition
Since a was arbitrary, we have shown that the square of every even number is even.	1.1. Even(a)$\rightarrow$Even(a^2)	Direct Proof
	1. $\forall x$ (Even(x)$\rightarrow$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) ≡ $\exists y\ (x=2y)$
Odd(x) ≡ $\exists y\ (x=2y+1)$
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 $a^2 = 4b^2 = 2(2b^2)$. So a^2 is, by definition, is even.

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

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

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

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.

Let x and y be arbitrary integers.

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

1.1. (Odd(**x**) ∧ Odd(**y**)) → Even(**x+y**)

1. ∀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 $\forall$x $\forall$y ((Odd(x) $\wedge$ Odd(y))$\rightarrow$Even(x+y))

Let x and y be arbitrary integers.	**Let x and y be arbitrary integers**
Suppose that both are odd.	**1.1.1** Odd(**x**) $\wedge$ Odd(**y**) Assumption
so x+y is even.	**1.1.9** Even(**x+y**)
Since x and y were arbitrary, the sum of any odd integers is even.	**1.1.** (Odd(**x**) $\wedge$ Odd(**y**)) $\rightarrow$ Even(**x+y**) Direct.. **1.** $\forall$x $\forall$y ((Odd(**x**) $\wedge$ Odd(**y**)) $\rightarrow$ Even(x+y)) Intro $\forall$

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

Let x and y be arbitrary integers.

Suppose that both are odd.

so x+y is even.

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

Let x and y be arbitrary integers

1.1.1	Odd(**x**) ∧ Odd(**y**)	Assumption
1.1.2	Odd(**x**)	Elim ∧
1.1.3	Odd(**y**)	Elim ∧
1.1.9	Even(**x+y**)	
1.1.	(Odd(**x**) ∧ Odd(**y**)) → Even(**x+y**)	Direct..
1.	∀x ∀y ((Odd(**x**) ∧ Odd(**y**)) → Even(x+y))	Intro ∀

English Proof: Even and Odd

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

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

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.

so x+y is, by definition, even.

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

Let x and y be arbitrary integers.

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

English Proof: Even and Odd

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

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

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 = … = 2(a+b+1)

so x+y is, by definition, even.

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

Let x and y be arbitrary integers.

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

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.

■

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