Adam Blank Spring 2017

CSE 311

Foundations of Computing I

Pre-Lecture Problem

Suppose that p, and $p \rightarrow (q \wedge r)$ are true. Is q true? Can you prove it with equivalences?

How I 311

(1) Try problem

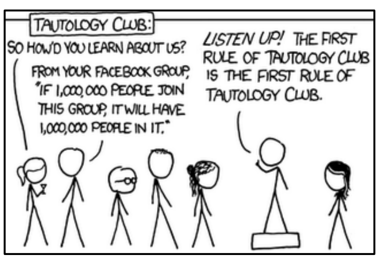
(2) Get stuck
30 min – 1 hr

(3) Break

(4) Try again!

CSE 311: Foundations of Computing

Lecture 7: Proofs

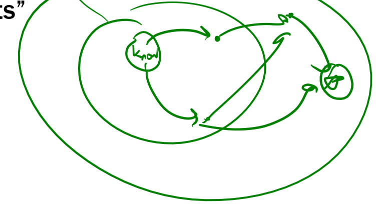


Applications of Logical Inference

- 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

Proofs

- Start with hypotheses and facts (**Axioms**)
- Use "rules" to generate more facts from existing facts (**Inference Rules**)
- Result is proved when it is included in the set of "proven facts"



Axioms

If I have nothing...

$$\frac{\text{Requirements:}}{\text{Conclusions: } \therefore C \quad D}$$

Then, I have also proven C

Then, I have also proven D

$p \rightarrow p \equiv$

$\neg p \vee p \equiv p \vee \neg p$

Example (Excluded Middle):

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

I have a proof of A $\vee \neg$A.

Inference Rules

If I have a proof of A and
I have a proof of B....

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

Conclusions: $\therefore C \qquad D$

Then, I have also proven C

Then, I have also proven D

Example (Modus Ponens):

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

If I have a proof of A and a proof of A → B, then I have a proof of B.

An inference rule: *Modus Ponens*

- If p and p → q are both true then q must be true
- Write this rule as

Modus Ponens
$$\frac{A \qquad A \rightarrow B}{\therefore \quad B}$$

- Given:
  - If it's Saturday, then you have a 311 lecture today.
  - It's Saturday.
- 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 → q — Given
3. q → r — Given
4. q — By MP: 1, 2
5. r — By MP: 3, 4

$$\frac{p \qquad p \rightarrow q}{\therefore \quad q}$$

r

My First Proof!

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

1.	p	Given
2.	p → q	Given
3.	q → r	Given
4.	q	MP: 1, 2
5.	r	MP: 3, 4

Proofs can use equivalences too

Show that ¬p follows from p → q and ¬q

1.	p → q	Given
2.	¬q	Given
3.	¬q → ¬p	Contrapositive: 1
4.	¬p	MP: 2, 3

More Inference Rules

Each connective has an "introduction rule" and an "elimination rule"

Consider "and". To know A ∧ B is true, what do we need to know...?

A	B	A ∧ B

$$\frac{A \qquad B}{\therefore \quad A \wedge B}$$

∧ Introduction
$$\frac{\qquad}{\therefore}$$

More Inference Rules

Each connective has an “introduction rule” and an “elimination rule”

Consider “and”. To know A ∧ B is true, what do we need to know…?

A	B	A ∧ B
T	T	T
T	F	F
T	T	F
T	F	F

The only case A ∧ B is true is when A and B are both true.

∧ Introduction

$$\dfrac{A \qquad B}{\therefore\ A \land B}$$

So, we can only prove A ∧ B if we already have a proof for A and we already have a proof for B.

More Inference Rules

Each connective has an “introduction rule” and an “elimination rule”

“Elimination” rules go the other way. If we know A ∧ B, then what do we know about A and B individually?

A	B	A ∧ B
T	T	T
T	F	F
T	T	F
T	F	F

When A ∧ B is true, then A is true and B is true.

∧ Elimination

$$\dfrac{A \land B}{\therefore\ A \qquad B}$$

So, if we can prove A ∧ B, then we can also prove A and we can also prove B.

Proofs

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

How To Start:

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

1. p Given
2. p → q Given
3. q MP: 1, 2
4. p ∧ q ∧ Intro: 1, 3
5. (p ∧ q) → r Given

100. r

Modus Ponens

$$\dfrac{A \qquad A \to B}{\therefore\ B}$$

∧ Introduction

$$\dfrac{A \qquad B}{\therefore\ A \land B}$$

∧ Elimination

$$\dfrac{A \land B}{\therefore\ A \qquad B}$$

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

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

$$\dfrac{\dfrac{p \qquad \dfrac{p \quad p \to q}{q}\,\text{MP}}{p \land q}\,\text{Intro}\ \land \qquad p \land q \to r}{r}\,\text{MP}$$

Simple Propositional Inference Rules

Elimination / **Introduction**

∧ — ∧ Elimination: $\dfrac{A \land B}{\therefore\ A \qquad B}$ — ∧ Introduction: $\dfrac{A \qquad B}{\therefore\ A \land B}$

∨ — ∨ Elimination: $\dfrac{A \lor B \qquad \neg A}{\therefore\ B}$ — ∨ Introduction: $\dfrac{A}{\therefore\ A \lor B \qquad B \lor A}$

¬q → ¬p

→ — Modus Ponens: $\dfrac{A \qquad A \to B}{\therefore\ B}$ — $\dfrac{p \Rightarrow q}{\therefore\ p \to q}$ Direct Proof Rule

Not like other rules

Important: Application of Inference Rules

- You can use equivalences to make substitutions of any sub-formula.
- Inference rules only can be applied to whole formulas (not correct otherwise).

e.g. 1. p → q Given

2. (p ∨ r) → q Intro ∨: 1

Important: Application of Inference Rules

- You can use equivalences to make substitutions of any sub-formula.
- Inference rules only can be applied to whole formulas (not correct otherwise).

e.g. 1. $p \to q$ Given

~~2. $(p \vee r) \to q$ Intro $\vee$: 1~~

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

Proofs

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

44.

45. $\neg r$

Idea: Work backwards!

Proofs

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

Idea: Work backwards!

We want to eventually get $\neg r$. How?
- We can use $q \to \neg r$ to get there.

45. $\neg r$

Proofs

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

Idea: Work backwards!

We want to eventually get $\neg r$. How?
- We can use $q \to \neg r$ to get there.
- The justification between 44 and 45 looks like "implication elim" which is MP.

44. $q \to \neg r$ Given

45. $\neg r$ MP: 44, ?

- So, we can justify line 45 now!

Proofs

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

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 $\neg r$...

43. q ?

44. $q \to \neg r$ Given

45. $\neg r$ MP: 44, 43

Proofs

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

Idea: Work backwards!

We want to eventually get q. How?
- Find a relevant given!

42. $\neg s \vee q$ Given

43. q ?

This looks like or-elimination.

44. $q \to \neg r$ Given

45. $\neg r$ MP: 44, 43

Proofs

Prove that ¬r follows from p ∧ s, Used! and Used!

41. $\neg\neg s$ It's more likely that $\neg\neg s$ shows up as s...
42. $\neg s \lor q$ Given
43. q ∨ Elim: 42, 41
44. $q \to \neg r$ Given
45. $\neg r$ MP: 44, 43

Proofs

Prove that ¬r follows from p ∧ s, Used! and Used!

39. $p \land s$ Given
40. s Use our last given!
41. $\neg\neg s$ Double Negation: 40
42. $\neg s \lor q$ Given
43. q ∨ Elim: 42, 41
44. $q \to \neg r$ Given
45. $\neg r$ MP: 44, 43

Remember, we're allowed to use equivalences!

Proofs

Prove that ¬r follows from Used! Used! and Used!

We don't have any holes in the proof left! We're done!

p ∧ s

s

39. $p \land s$ Given
40. s ∧ Elim: 39
41. $\neg\neg s$ Double Negation: 40
42. $\neg s \lor q$ Given
43. q ∨ Elim: 42, 41
44. $q \to \neg r$ Given
45. $\neg r$ MP: 44, 43

Proofs

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

Well, almost, let's renumber the steps:

1. $p \land s$ Given
2. s ∧ Elim: 1
3. $\neg\neg s$ Double Negation: 2
4. $\neg s \lor q$ Given
5. q ∨ Elim: 4, 3
6. $q \to \neg r$ Given
7. $\neg r$ MP: 6, 5

To Prove An Implication: $A \to B$

- We use the direct proof rule
- The "pre-requisite" for using the direct proof rule is that we **write a proof** that **Assuming** A, we can prove B.
- The direct proof rule:

  If you have such a proof then you can conclude that p → q is true

  Example: Prove p → (p ∨ q).

proof subroutine

1.1	p	Assumption
1.2	p ∨ q	Intro ∨: 1
1.	p → (p ∨ q)	Direct Proof Rule

Proofs using the direct proof rule

Show that p → r follows from q and (p ∧ q) → r

1.	q	Given
2.	(p ∧ q) → r	Given
3.1.	p	Assumption
3.2.	p ∧ q	Intro ∧: 1, 3.1
3.3.	r	MP: 2, 3.2
3.	p → r	Direct Proof Rule

This is a proof of $p \to r$

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

Example

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

There MUST be an application of the Direct Proof Rule to prove this implication.

Where do we start? We have no givens…

Example

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

Example

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

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

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
(1.2)	$p \rightarrow q$	$\wedge$ Elim: 1.1
(1.3)	$q \rightarrow r$	$\wedge$ 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 Rule
(1)	$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$	Direct Proof Rule

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.

Inference rules for quantifiers

∃ Introduction
P(c) for some c
∴ ∃x P(x)

∀ Introduction
∀x P(x)
∴ P(a) **for any** a

∀ Introduction
"**Let** a **be arbitrary***"...P(a)
∴ ∀x P(x)

* in the domain of P

∃ Elimination
∃x P(x)
∴ **P(c) for some *special*** ** **c**

** 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 variable!

Definitions: The Base of All Proofs

Domain of Discourse
Integers

- **Before proving anything about a topic, we need to provide definitions.**
- **A significant part of writing proofs is unrolling and re-rolling definitions.**

∃ Introduction
P(c) for some c
∴ ∃x P(x)

Predicate Definitions
Even(x) ≡ **∃**y (x = 2y)
Odd(x) ≡ **∃**y (x = 2y + 1)

- **Prove the statement** $\exists a\ (\text{Even}(a))$

Definitions: The Base of All Proofs

Domain of Discourse
Integers

- **Before proving anything about a topic, we need to provide definitions.**
- **A significant part of writing proofs is unrolling and re-rolling definitions.**

∃ Introduction
P(c) for some c
∴ ∃x P(x)

Predicate Definitions
Even(x) ≡ **∃**y (x = 2y)
Odd(x) ≡ **∃**y (x = 2y + 1)

- **Prove the statement** $\exists a\ (\text{Even}(a))$

1. $2 = 2 * 1$ — **Definition of Multiplication**
2. $\text{Even}(2)$ — **Definition of Even**
3. $\exists x\ \text{Even}(x)$ — **∃ Intro: 2**

Definitions: The Base of All Proofs

Domain of Discourse
Integers

Predicate Definitions
Even(x) ≡ **∃**y (x = 2y)
Odd(x) ≡ **∃**y (x = 2y + 1)

Prove the statement $\exists a\ (\text{Even}(a))$

1. $2 = 2 * 1$ — **Definition of Multiplication**
2. $\text{Even}(2)$ — **Definition of Even**
3. $\exists x\ \text{Even}(x)$ — **∃ Intro: 2**

Okay, you might say, but now we have "definition of multiplication"! Isn't that cheating?

Well, sort of, but we're going to trust that basic arithmetic operations work the way we'd expect. There's a fine line, and you can always ask if you're allowed to assume something (though the answer will usually be no…).

Definitions: The Base of All Proofs

Domain of Discourse
Integers >= 1

Predicate Definitions
Even(x) ≡ $\exists y(x = 2y)$
Odd(x) ≡ $\exists y(x = 2y + 1)$
Primeish(x) ≡ $\forall a \forall b\left(\left((a < b \wedge ab = x) \rightarrow (a = 1 \wedge b = x)\right)\right)$

Prove the statement $\exists a\ (\text{Primeish}(a))$

Proof Strategy:

- **2 is going to work.**
- **Try to prove all the individual facts we need.**
- **We do this from the inside out…**

1.	Let a be arbitrary	**Defining a**
2.	Let b be arbitrary	**Defining b**
3.	$a \leq 2 \vee a > 2$	**Excluded Middle**
4.	$b \leq 2 \vee b > 2$	**Excluded Middle**

Definitions: The Base of All Proofs

Domain of Discourse
Integers >= 1

Predicate Definitions
Primeish(x) ≡ $\forall a \forall b\left(\left((a < b \wedge ab = x) \rightarrow (a = 1 \wedge b = x)\right)\right)$

Prove the statement $\exists a\ (\text{Primeish}(a))$

1.	Let a be arbitrary	**Defining a**
2.	Let b be arbitrary	**Defining b**
3.	$a \leq 2 \vee a > 2$	**Excluded Middle**
4.	$b \leq 2 \vee b > 2$	**Excluded Middle**
5.	$(a \leq 2 \vee a > 2) \wedge (b \leq 2 \vee b > 2)$	**∧ Intro: 3, 4**
6.1.	$a < b \wedge ab = 2$	Assumption
6.2.	$a < b$	∧ Elim: 6.1
6.3.	$ab = 2$	∧ Elim: 6.1
6.4.	$a = 1 \wedge b = 2$	Simplifying 5 via 6.2 & 6.3
6.	$(a < b \wedge ab = 2) \rightarrow (a = 1 \wedge b = 2)$	**Direct Proof Rule**

Definitions: The Base of All Proofs

Domain of Discourse
Integers >= 1

Predicate Definitions
Primeish(x) ≡ $\forall a \forall b\left(\left((a < b \wedge ab = x) \rightarrow (a = 1 \wedge b = x)\right)\right)$

Prove the statement $\exists a\ (\text{Primeish}(a))$

1. Let a be arbitrary — **Defining a**
2. Let b be arbitrary — **Defining b**
3. $a \leq 2 \vee a > 2$ — **Excluded Middle**
4. $b \leq 2 \vee b > 2$ — **Excluded Middle**
5. $(a \leq 2 \vee a > 2) \wedge (b \leq 2 \vee b > 2)$ — **∧ Intro: 3, 4**
   - 6.1. $a < b \wedge ab = 2$ — Assumption
   - 6.2. $a < b$ — ∧ Elim: 6.1
   - 6.3. $ab = 2$ — ∧ Elim: 6.1
   - 6.4. $a = 1 \wedge b = 2$ — Simplifying 5 via 6.2 & 6.3
6. $(a < b \wedge ab = 2) \rightarrow (a = 1 \wedge b = 2)$ — **Direct Proof Rule**
7. $\forall b(a < b \wedge ab = 2) \rightarrow (a = 1 \wedge b = 2)$ — **∀ Intro: 6**

Definitions: The Base of All Proofs

Domain of Discourse
Integers >= 1

Predicate Definitions
Primeish(x) ≡ $\forall a \forall b\left(\left((a < b \wedge ab = x) \rightarrow (a = 1 \wedge b = x)\right)\right)$

Prove the statement $\exists a\ (\text{Primeish}(a))$

1. Let a be arbitrary — **Defining a**
2. Let b be arbitrary — **Defining b**
3. $a \leq 2 \vee a > 2$ — **Excluded Middle**
4. $b \leq 2 \vee b > 2$ — **Excluded Middle**
5. $(a \leq 2 \vee a > 2) \wedge (b \leq 2 \vee b > 2)$ — **∧ Intro: 3, 4**
   - 6.1. $a < b \wedge ab = 2$ — Assumption
   - 6.2. $a < b$ — ∧ Elim: 6.1
   - 6.3. $ab = 2$ — ∧ Elim: 6.1
   - 6.4. $a = 1 \wedge b = 2$ — Simplifying 5 via 6.2 & 6.3
6. $(a < b \wedge ab = 2) \rightarrow (a = 1 \wedge b = 2)$ — **Direct Proof Rule**
7. $\forall b(a < b \wedge ab = 2) \rightarrow (a = 1 \wedge b = 2)$ — **∀ Intro: 6**
8. $\text{Primeish}(2)$ — **∀ Intro: 7**

Definitions: The Base of All Proofs

Domain of Discourse
Integers >= 1

Predicate Definitions
Primeish(x) ≡ $\forall a \forall b\left(\left((a < b \wedge ab = x) \rightarrow (a = 1 \wedge b = x)\right)\right)$

Prove the statement $\exists a\ (\text{Primeish}(a))$

1. Let a be arbitrary — **Defining a**
2. Let b be arbitrary — **Defining b**
3. $a \leq 2 \vee a > 2$ — **Excluded Middle**
4. $b \leq 2 \vee b > 2$ — **Excluded Middle**
5. $(a \leq 2 \vee a > 2) \wedge (b \leq 2 \vee b > 2)$ — **∧ Intro: 3, 4**
   - 6.1. $a < b \wedge ab = 2$ — Assumption
   - 6.2. $a < b$ — ∧ Elim: 6.1
   - 6.3. $ab = 2$ — ∧ Elim: 6.1
   - 6.4. $a = 1 \wedge b = 2$ — Simplifying 5 via 6.2 & 6.3
6. $(a < b \wedge ab = 2) \rightarrow (a = 1 \wedge b = 2)$ — **Direct Proof Rule**
7. $\forall b(a < b \wedge ab = 2) \rightarrow (a = 1 \wedge b = 2)$ — **∀ Intro: 6**
8. $\text{Primeish}(2)$ — **∀ Intro: 7**
9. $\exists x\ \text{Primeish}(x)$ — **∃ Intro: 8**

BTW, this justification isn't really good enough...

Proofs using Quantifiers

"There exists an even primeish number"

First, we translate into predicate logic:

∃x Even(x) ∧ Primeish(x)

We've already proven $\text{Even}(2)$ **and** $\text{Primeish}(2)$**; so, we can use them as givens...**

1. $\text{Even}(2)$ — **Prev. Slide**
2. $\text{Primeish}(2)$ — **Prev. Slide**
3. $\text{Even}(2) \wedge \text{Primeish}(2)$ — **∧ Intro: 1, 2**
4. $\exists x\ (\text{Even}(x) \wedge \text{Primeish}(x))$ — **∃ Intro: 3**

Ugh...so much work

Predicate Definitions
Even(x) ≡ $\exists y(x = 2y)$
Primeish(x) ≡ $\forall a \forall b\left(\left((a < b \wedge ab = x) \rightarrow (a = 1 \wedge b = x)\right)\right)$

Note that 2 = 2*1 by definition of multiplication. It follows that there is a y such that 2 = 2y; so, two is even.

Consider two arbitrary non-negative integers a, b.

Suppose a < b and ab = 2. Note that when b > 2, the product is always greater than 2. Furthermore, a < b. So, the only solution to the equation is a = 1 and b = 2. So, a = 1 and b = 2.

Since a and b were arbitrary, it follows that 2 is primeish.

Since 2 is even and primeish, there exists a number that is even and primeish.

This is the same proof, but infinitely easier to read and write....