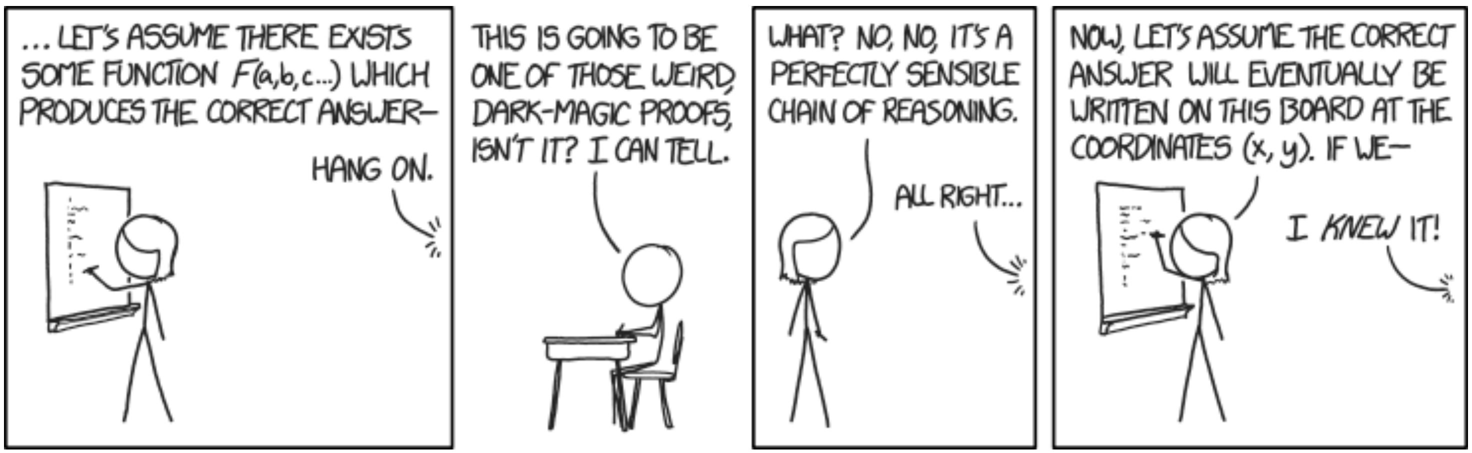
# CSE 311: Foundations of Computing

## Lecture 8:  Predicate Logic Proofs



# Last class: Propositional Inference Rules

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

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

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

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

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

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

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

# Proofs

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

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

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

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

# Proofs

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

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

9. $r$ ??

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

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

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

# Proofs

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

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

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

# Proofs

Prove that $\neg r$ follows from $p \land s$, $q \to \neg r$, and $\neg s \lor q$.

| | | |
|---|---|---|
| 1. | $p \land s$ | Given |
| 2. | $q \to \neg r$ | Given |
| 3. | $\neg s \lor q$ | Given |
| 20. | $\neg r$ | ? |

**First: Write down givens and goal**

**Idea: Work backwards!**

# Proofs

Prove that $\neg r$ follows from $p \land s$, $q \to \neg r$, and $\neg s \lor q$.

| | | |
|---|---|---|
| 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 $\to$" which is MP.

# Proofs

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

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

**Idea: Work backwards!**

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

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

# Proofs

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

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

This looks like or-elimination.

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

# Proofs

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

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

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

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

# Proofs

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

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

# Proofs

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

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

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

# Proofs

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

| | | |
|---|---|---|
| 1. | $p \wedge s$ | Given |
| 2. | $q \rightarrow \neg r$ | Given |
| 3. | $\neg s \vee q$ | Given |
| 4. | $s$ | $\wedge$ Elim: 1 |
| 5. | $\neg\neg s$ | Double Negation: 4 |
| 6. | $q$ | $\vee$ Elim: 3, 5 |
| 7. | $\neg r$ | MP: 2, 6 |

# Important: Applications of Inference Rules

- You can use equivalences to make substitutions of any sub-formula.

  e.g. $(p \rightarrow r) \vee q \equiv (\neg p \vee r) \vee q$

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

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

  ~~2. $(p \vee q) \rightarrow r$ intro $\vee$ from 1.~~

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

# Last class: Propositional Inference Rules

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

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

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

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

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

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

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

Not like other rules

## Last class: New Perspective

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

| *p* | *q* | **A** | **B** |
|---|---|---|---|
| T | T | T | T |
| T | F | T | T |
| F | T | F | |
| F | F | F | |

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

$$A \Rightarrow B$$

## Last class: New Perspective

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

| $p$ | $q$ | **A** | **B** | **A → B** |
|---|---|---|---|---|
| T | T | T | T | T |
| T | F | T | T | T |
| F | T | F | T | T |
| F | F | F | F | T |

When we zoom out, what have we proven?

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

# To Prove An Implication: $A \rightarrow B$

$$\frac{A \Longrightarrow B}{\therefore A \longrightarrow B}$$

- We use the direct proof rule
- The "pre-requisite" $A \Longrightarrow B$ for the direct proof rule is **a proof** that "**Given** A, we can prove B."
- The direct proof rule:

  If you have such a proof then you can conclude that $A \longrightarrow B$ 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: $(p \land q) \rightarrow (p \lor q)$

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

Where do we start? We have no givens...

# Example

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

1.1. $p \wedge q$ Assumption

1.9. $p \vee q$ ??

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

# Example

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

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

# One General Proof Strategy

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

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

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

## Example

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

# Example

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

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. | $p \rightarrow q$ | $\wedge$ Elim: 1.1 |
| 1.3. | $q \rightarrow r$ | $\wedge$ Elim: 1.1 |
| 1.? | $p \rightarrow r$ | |

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

# Example

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

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

1.2. $p \to q$ $\land$ Elim: 1.1

1.3. $q \to r$ $\land$ Elim: 1.1

1.4.1. $p$ Assumption

1.4.? $r$

1.4. $p \to r$ Direct Proof

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

# Example

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

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

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

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

1.4.1. $p$ Assumption

1.4.2. $q$ 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

# 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 ∃

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

Intro ∀

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

# My First Predicate Logic Proof

| Domain of Discourse |
| --- |
| Integers |

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

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

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

**5.** $(\forall x\, P(x)) \rightarrow (\exists x\, P(x))$ ?

The main connective is implication so Direct Proof seems good

# My First Predicate Logic Proof

| Domain of Discourse |
|---|
| Integers |

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

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. $\forall x\, P(x) \to \exists x\, P(x)$ 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**

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

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

**That requires P(c) for some c.**

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

# My First Predicate Logic Proof

| Domain of Discourse |
|---|
| Integers |

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

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

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

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

1.4. $P(5)$ ?

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

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

# My First Predicate Logic Proof

| Domain of Discourse |
| --- |
| Integers |

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

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

## 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 |

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

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

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

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

<u>Working forwards as well as backwards</u>:
In applying "Intro $\exists$" rule we didn't know what expression we might be able to prove P(c) for, so we worked forwards to figure out what might work.

# Predicate Logic Proofs

- Can use
  - Predicate logic inference rules

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

    even on subformulas
  - Propositional logic inference rules

    whole formulas only
  - Propositional logic equivalences

    even on subformulas

# Predicate Logic Proofs with more content

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

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

- Example:

| Domain of Discourse |
| --- |
| Integers |

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

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