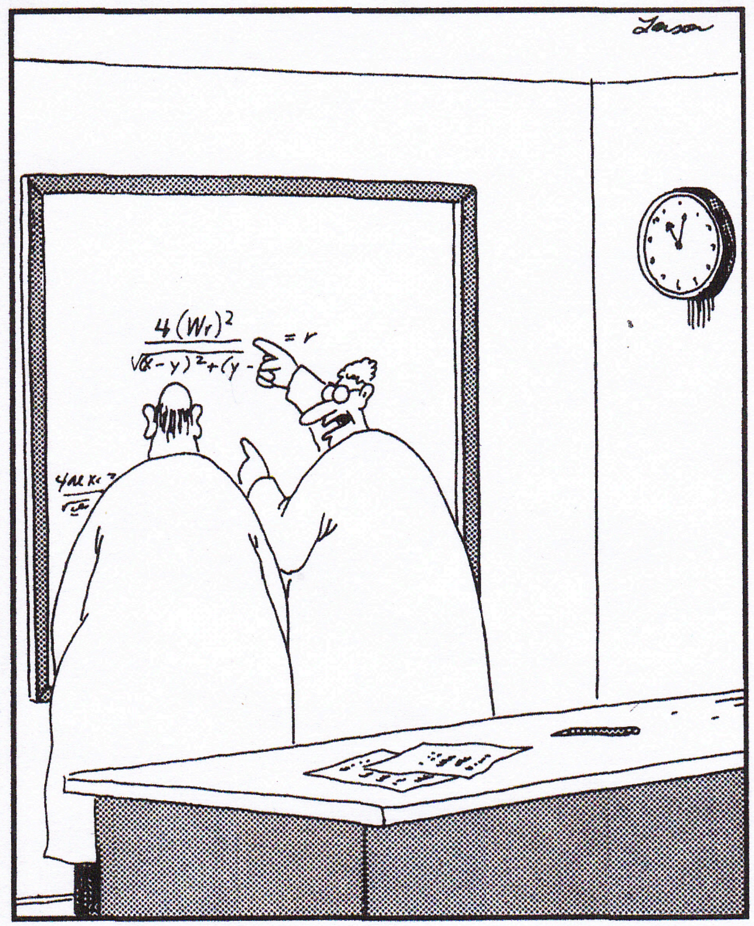
CSE 311: Foundations of Computing

Lecture 9: Proof Strategies & Set Theory



"Yes, yes, I *know* that, Sidney... *every*body knows *that!*... But look: Four wrongs *squared*, minus two wrongs to the fourth power, divided by this formula, *do* make a right."

Last class: English Proofs

- High-level language let us work more quickly
  - should not be necessary to spill out every detail
  - examples so far
    - skipping Intro ∧ and Elim ∧ (and hence, Commutativity and Associativity)
    - skipping Double Negation
    - 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. ∎

Proof Strategies: Proof by Contrapositive

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

	1.1. $\neg q$	Assumption
	...	
	1.3. $\neg p$	
1.	$\neg q \to \neg p$	Direct Proof Rule
2.	$p \to q$	Contrapositive: 1

Proof Strategies: Proof by Contrapositive

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

We will prove 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 Rule
2.	$p \rightarrow q$	Contrapositive: 1

Proof by Contradiction: One way to prove $\neg p$

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

1.1.	p	Assumption
...		
1.3.	F	
1.	$p \to$ F	Direct Proof rule
2.	$\neg p \vee$ 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.	$p \rightarrow$ F	Direct Proof rule
2.	$\neg p \vee$ F	Law of Implication: 1
3.	$\neg p$	Identity: 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: "No integer is both even and odd."

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

Proof: We work 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. ■

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)

Applications of Predicate Logic

- Remainder of the course will use predicate logic to prove important properties of interesting objects
  - start with math objects that are widely used in CS
  - eventually more CS-specific objects

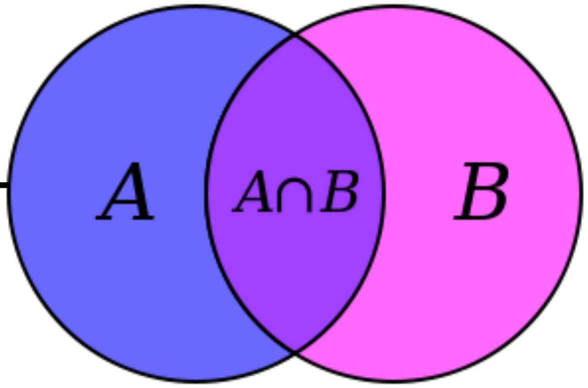
- Encode domain knowledge in predicate definitions
- Then apply predicate logic to infer useful results

Domain of Discourse
Integers

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

Set Theory

Set Theory



Sets are collections of objects called elements.

Write a ∈ B **to say that** a **is an element of set** B**,**
and a ∉ B **to say that it is not.**

Some simple examples
A = {1}
B = {1, 3, 2}
C = {☐, 1}
D = {{17}, 17}
E = {1, 2, 7, cat, dog, ∅, α}

Some Common Sets

$\mathbb{N}$ is the set of **Natural Numbers;** $\mathbb{N} = \{0, 1, 2, \ldots\}$

$\mathbb{Z}$ is the set of **Integers**; $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

$\mathbb{Q}$ is the set of **Rational Numbers**; e.g. ½, -17, 32/48

$\mathbb{R}$ is the set of **Real Numbers**; e.g. 1, -17, 32/48, $\pi, \sqrt{2}$

[n] is the set **{1, 2, …, n}** when **n** is a natural number

$\varnothing$ = **{}** is the **empty set**; the *only* set with no elements

Sets can be elements of other sets

For example

$A = \{\{1\},\{2\},\{1,2\},\varnothing\}$

$B = \{1,2\}$

Then $B \in A$.

Definitions

- A and B are *equal* if they have the same elements

$$A = B \equiv \forall x\,(x \in A \leftrightarrow x \in B)$$

- A is a *subset* of B if every element of A is also in B

$$A \subseteq B \equiv \forall x\,(x \in A \rightarrow x \in B)$$

- Notes:

$$(A = B) \equiv (A \subseteq B) \wedge (B \subseteq A)$$

$A \supseteq B$ means $B \subseteq A$

$A \subset B$ means $A \subseteq B$

Definition: Equality

A and B are *equal* if they have the same elements

$$A = B \equiv \forall x\,(x \in A \leftrightarrow x \in B)$$

A = {1, 2, 3}
B = {3, 4, 5}
C = {3, 4}
D = {4, 3, 3}
E = {3, 4, 3}
F = {4, {3}}

Which sets are equal to each other?

Definition: Subset

A is a *subset* of B if every element of A is also in B

$$A \subseteq B \equiv \forall x\, (x \in A \rightarrow x \in B)$$

A = {1, 2, 3}
B = {3, 4, 5}
C = {3, 4}

<u>QUESTIONS</u>

$\varnothing \subseteq A$?
$A \subseteq B$?
$C \subseteq B$?

Building Sets from Predicates

S = the set of all* x for which $P(x)$ is true

$$S = \{x : P(x)\}$$

S = the set of all x in A for which $P(x)$ is true

$$S = \{x \in A : P(x)\}$$

*in the domain of P, usually called the "universe" U

Set Operations

$$A \cup B = \{ x : (x \in A) \vee (x \in B) \}$$ **Union**

$$A \cap B = \{ x : (x \in A) \wedge (x \in B) \}$$ **Intersection**

$$A \setminus B = \{ x : (x \in A) \wedge (x \notin B) \}$$ **Set Difference**

A = {1, 2, 3}
B = {3, 5, 6}
C = {3, 4}

QUESTIONS

Using A, B, C and set operations, make…

[6] =

{3} =

{1,2} =

More Set Operations

$$A \oplus B = \{\, x : (x \in A) \oplus (x \in B)\}$$

Symmetric Difference

$$\bar{A} = A^C = \{\, x : x \notin A \,\}$$

(with respect to universe U)

Complement

A = {1, 2, 3}
B = {1, 2, 4, 6}
Universe:
U = {1, 2, 3, 4, 5, 6}

$A \oplus B$ = {3, 4, 6}
$\bar{A}$ = {4,5,6}

De Morgan's Laws

$$\overline{A \cup B} = \bar{A} \cap \bar{B}$$

$$\overline{A \cap B} = \bar{A} \cup \bar{B}$$