CSE 311: Foundations of Computing

Lecture 11: Proof strategies & Set Theory

Recap: Natural language proofs

English proofs:

- More high-level, flexible
- Reader needs to be convinced this corresponds to formal logic proof

Proof strategies:

- Proof by counterexample
- Proof of the contrapositive
- Proof by contradiction

Another proof by Contradiction

<u>Definition:</u> An integer y is a strict multiple of x, if $y = a \cdot x$ for some integer a with $a \geq 2$.

Predicate Definitions
SMul (x,y) $\equiv \exists a\ (a \geq 2 \land y = ax)$

Domain of Discourse
Positive Integers

Example: $SMul(7,21) = T$, $SMul(7,22) = F$, $SMul(5,5) = F$

Another proof by Contradiction

Definition: An integer y is a strict multiple of x, if $y = a \cdot x$ for some integer a with $a \geq 2$.

Predicate Definitions
SMul (x,y) $\equiv \exists a\ (a \geq 2 \land y = ax)$

Domain of Discourse
Positive Integers

Example: $SMul(7,21) = T$, $SMul(7,22) = F$, $SMul(5,5) = F$

Prove: For all positive integers x there is a positive integer y that is a strict multiple of x and for all positive integer z it is not true that z is a multiple of x and y is a multiple of z.

Another proof by Contradiction

Definition: An integer y is a strict multiple of x, if $y = a \cdot x$ for some integer a with $a \geq 2$.

Predicate Definitions
SMul (x,y) $\equiv \exists a\ (a \geq 2 \land y = ax)$

Domain of Discourse
Positive Integers

Example: $SMul(7,21) = T$, $SMul(7,22) = F$, $SMul(5,5) = F$

Prove: For all positive integers x there is a positive integer y that is a strict multiple of x and for all positive integer z it is not true that z is a multiple of x and y is a multiple of z.

$$\forall x\ \exists y\ (SMul(x,y) \land \forall z\ \neg\big(SMul(x,z) \land SMul(z,y)\big))$$

Another proof by Contradiction

$\forall x\ \exists y\ (SMul(x,y) \wedge \forall z\ \neg\big(SMul(x,z) \wedge SMul(z,y)\big))$

<u>Prove:</u> For all positive integers x there is a positive integer y that is a strict multiple of x and for all positive integer z it is not true that z is a multiple of x and y is a multiple of z.

<u>Proof:</u>

Another proof by Contradiction

$$\forall x\ \exists y\ (SMul(x,y) \land \forall z\ \neg\big(SMul(x,z) \land SMul(z,y)\big))$$

<u>Prove:</u> For all positive integers x there is a positive integer y that is a strict multiple of x and for all positive integer z it is not true that z is a multiple of x and y is a multiple of z.

<u>Proof:</u>

Let x be an arbitrary positive integer.

Another proof by Contradiction

$$\forall x\ \exists y\ (SMul(x,y) \land \forall z\ \neg\big(SMul(x,z) \land SMul(z,y)\big))$$

<u>Prove:</u> For all positive integers x there is a positive integer y that is a strict multiple of x and for all positive integer z it is not true that z is a multiple of x and y is a multiple of z.

<u>Proof:</u>
Let x be an arbitrary positive integer.
Choose $y = 2x$ which is a strict multiple of x.

Another proof by Contradiction

$\forall x\, \exists y\, (SMul(x,y) \wedge \forall z\, \neg\big(SMul(x,z) \wedge SMul(z,y)\big))$

Prove: For all positive integers x there is a positive integer y that is a strict multiple of x and for all positive integer z it is not true that z is a multiple of x and y is a multiple of z.

Proof:
Let x be an arbitrary positive integer.
Choose $y = 2x$ which is a strict multiple of x.
Let z be an arbitrary positive integer.

Another proof by Contradiction

$\forall x\, \exists y\, (SMul(x, y) \wedge \forall z\, \neg(SMul(x, z) \wedge SMul(z, y)))$

<u>Prove:</u> For all positive integers x there is a positive integer y that is a strict multiple of x and for all positive integer z it is not true that z is a multiple of x and y is a multiple of z.

<u>Proof:</u>
Let x be an arbitrary positive integer.
Choose $y = 2x$ which is a strict multiple of x.
Let z be an arbitrary positive integer.
Assume for the sake of contradiction that z is a strict multiple of x and y is a strict multiple of z.

1.1 A Assume

1.n F

1. $A \rightarrow F$ DPR
2. $\neg A \vee F$ LoI
3. $\neg A$

Another proof by Contradiction

$$\forall x\ \exists y\ (SMul(x,y) \land \forall z\ \neg(SMul(x,z) \land SMul(z,y)))$$

Prove: For all positive integers x there is a positive integer y that is a strict multiple of x and for all positive integer z it is not true that z is a multiple of x and y is a multiple of z.

Proof:
Let x be an arbitrary positive integer.
Choose $y = 2x$ which is a strict multiple of x.
Let z be an arbitrary positive integer.
Assume for the sake of contradiction that z is a strict multiple of x and y is a strict multiple of z.
Hence $z = ax$ and $y = bz$ for some integers a, b with $a \geq 2$ and $b \geq 2$.

Another proof by Contradiction

$$\forall x\ \exists y\ (SMul(x,y) \land \forall z\ \neg\big(SMul(x,z) \land SMul(z,y)\big))$$

Prove: For all positive integers x there is a positive integer y that is a strict multiple of x and for all positive integer z it is not true that z is a multiple of x and y is a multiple of z.

Proof:
Let x be an arbitrary positive integer.
Choose $y = 2x$ which is a strict multiple of x.
Let z be an arbitrary positive integer.
Assume for the sake of contradiction that z is a strict multiple of x and y is a strict multiple of z.
Hence $z = ax$ and $y = bz$ for some integers a, b with $a \geq 2$ and $b \geq 2$.
Then $2x = y = bz = abx$.

Another proof by Contradiction

$$\forall x\ \exists y\ (SMul(x,y) \land \forall z\ \neg\big(SMul(x,z) \land SMul(z,y)\big))$$

<u>Prove:</u> For all positive integers x there is a positive integer y that is a strict multiple of x and for all positive integer z it is not true that z is a multiple of x and y is a multiple of z.

<u>Proof:</u>
Let x be an arbitrary positive integer.
Choose $y = 2x$ which is a strict multiple of x.
Let z be an arbitrary positive integer.
Assume for the sake of contradiction that z is a strict multiple of x and y is a strict multiple of z.
Hence $z = ax$ and $y = bz$ for some integers a, b with $a \geq 2$ and $b \geq 2$.
Then $2x = y = bz = abx$. Dividing by $x \neq 0$ gives $2 = ab \geq 4$.
That 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)

Lecture 11 Activity

You will be assigned to breakout rooms. Please:

- Introduce yourself
- Choose someone to share their screen, showing this PDF
- Prove the statement:

There are no integers x and y for which 2x+6y=1

$\neg \exists x \exists y\ 2x+6y=1$

Provide an English proof by contradiction.

AFSOC that there are integers x and y such that $2x+6y=1$. Dividing both sides by 2, we get $x+3y=1/2$. Since $x+3y$ is an integer but $1/2$ isn't, this is a contradiction. $\square$

Fill out the poll everywhere for Activity Credit!
Go to pollev.com/philipmg and login with your UW identity

Applications of Predicate Logic

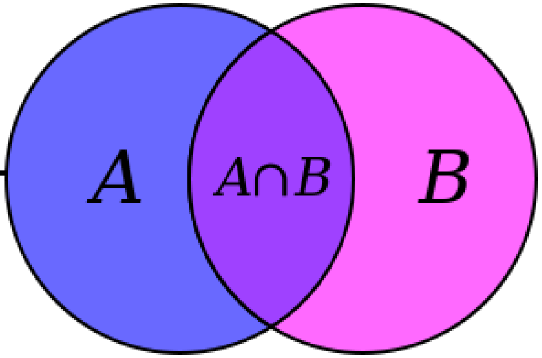
- Remainder of the course will use predicate logic to prove <u>important</u> properties of <u>interesting</u> objects
  - start with math objects that are widely used in CS
  - eventually more CS-specific objects

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

Domain of Discourse
Integers

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

Set Theory



Sets are collections of objects called **elements.**

Write $a \in B$ to say that a is an element of set B, and $a \notin B$ to say that it is not.

Some simple examples

$A = \{1\}$

$B = \{1, 3, 2\}$

$C = \{\square, 1\}$

$D = \{\{17\}, 17\}$

$E = \{1, 2, 7, \text{cat}, \text{dog}, \varnothing, \alpha\}$

Some Common Sets

$\mathbb{N}$ is the set of **Natural Numbers;** $\mathbb{N}$ = {0, 1, 2, …}
$\mathbb{Z}$ is the set of **Integers**; $\mathbb{Z}$ = {…, -2, -1, 0, 1, 2, …}
$\mathbb{Q}$ 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, π, $\sqrt{2}$
[n] is the set **{1, 2, …, n}** when **n** is a natural number
{} = ∅ 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

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

- Note: $(\boldsymbol{A} = \boldsymbol{B}) \equiv (\boldsymbol{A} \subseteq \boldsymbol{B}) \wedge (\boldsymbol{B} \subseteq \boldsymbol{A})$

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}

<u>QUESTIONS</u>

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

$$\overline{A} = \{\, x : x \notin A \,\}$$

(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}
$\overline{A}$ = {4,5,6}

It's propositional logic again

- Definition for $\cup$ based on $\vee$

- Definition for $\cap$ based on $\wedge$

- Complement works like $\neg$

De Morgan's Laws

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

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

De Morgan's Laws

Prove that $(A \cup B)^C = A^C \cap B^C$

Formally, prove $\forall x\ (x \in (A \cup B)^C \leftrightarrow x \in A^C \cap B^C)$

Proof: Let x be an arbitrary object.

Suppose $x \in (A \cup B)^C$. Then, by definition of complement, we have $\neg(x \in A \cup B)$. The latter is equivalent to $\neg(x \in A \vee x \in B)$, which is equivalent to $\neg(x \in A) \wedge \neg(x \in B)$ by De Morgan's law. We then have $x \in A^C$ and $x \in B^C$, by the definition of complement, so we have $x \in A^C \cap B^C$ by the definition of intersection.

Proof technique:
To show C = D show
$x \in C \rightarrow x \in D$ and
$x \in D \rightarrow x \in C$

De Morgan's Laws

Prove that $(A \cup B)^C = A^C \cap B^C$

Formally, prove $\forall \mathrm{x}\ (x \in (A \cup B)^C \leftrightarrow x \in A^C \cap B^C)$

Proof: Let x be an arbitrary object.

Suppose $x \in (A \cup B)^C$.... Then, $x \in A^C \cap B^C$.

Suppose $x \in A^C \cap B^C$. Then, by definition of intersection, we have $x \in A^C$ and $x \in B^C$. That is, we have $\neg(x \in A) \wedge \neg(x \in B)$, which is equivalent to $\neg(x \in A \vee x \in B)$ by De Morgan's law. The last is equivalent to $\neg(x \in A \cup B)$, by the definition of union, so we have shown $x \in (A \cup B)^C$, by the definition of complement. ■

De Morgan's Laws

Prove that $(A \cup B)^C = A^C \cap B^C$

Formally, prove $\forall \mathrm{x}\ (x \in (A \cup B)^C \leftrightarrow x \in A^C \cap B^C)$

Proof: Let x be an arbitrary object.

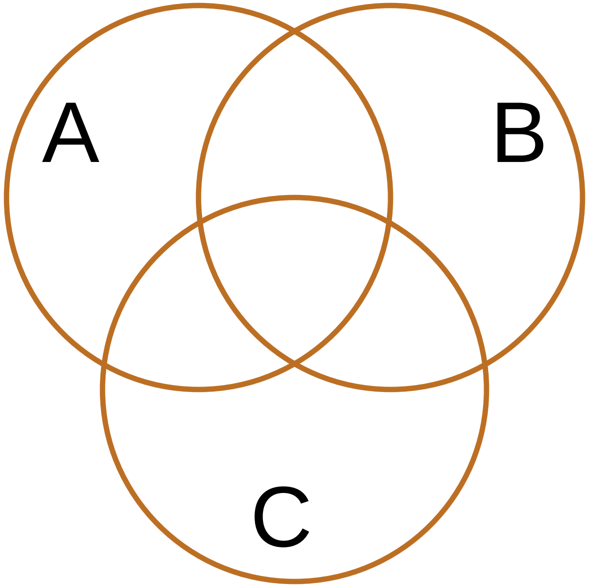
The stated bi-condition holds since:

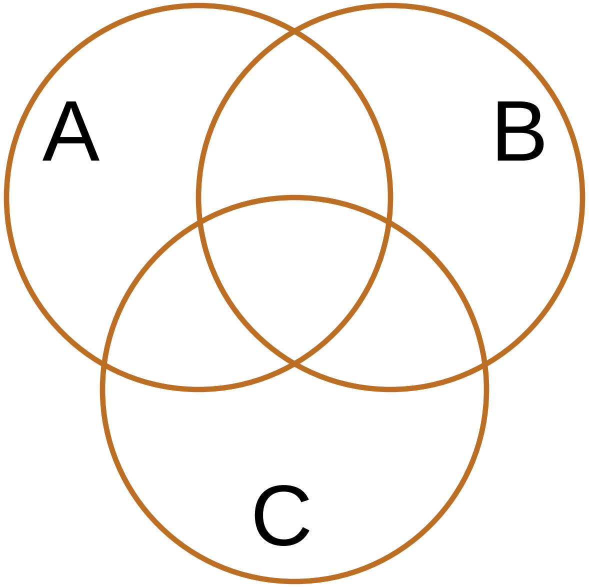
$x \in (A \cup B)^C$	$\equiv \neg(x \in A \cup B)$	def of $-^C$
	$\equiv \neg(x \in A \vee x \in B)$	def of $\cup$
	$\equiv \neg(x \in A) \wedge \neg(x \in B)$	De Morgan
	$\equiv x \in A^C \wedge x \in B^C$	def of $-^C$
	$\equiv x \in A^C \cap B^C$	def of $\cap$

Chains of equivalences are often easier to read like this rather than as English text

Distributive Laws

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$





Power Set

- **Power Set of a set A = set of all subsets of A**

$$\mathcal{P}(A) = \{ B : B \subseteq A \}$$

- **e.g., let** Days={M,W,F} **and consider all the possible sets of days in a week you could ask a question in class**

$\mathcal{P}$(Days)=?

$\mathcal{P}(\varnothing)$=?

Power Set

- **Power Set of a set A = set of all subsets of A**

$$\mathcal{P}(A) = \{ B : B \subseteq A \}$$

- **e.g., let Days={M,W,F} and consider all the possible sets of days in a week you could ask a question in class**

$\mathcal{P}(\text{Days})=\{\{\text{M}, \text{W}, \text{F}\}, \{\text{M}, \text{W}\}, \{\text{M}, \text{F}\}, \{\text{W}, \text{F}\}, \{\text{M}\}, \{\text{W}\}, \{\text{F}\}, \varnothing\}$

$\mathcal{P}(\varnothing)=\{\varnothing\} \neq \varnothing$

Cartesian Product

$$A \times B = \{ (a, b) : a \in A, b \in B \}$$

$\mathbb{R} \times \mathbb{R}$ is the real plane. You've seen ordered pairs before.

These are just for arbitrary sets.

$\mathbb{Z} \times \mathbb{Z}$ is "the set of all pairs of integers"

If A = {1, 2}, B = {a, b, c}, then A × B = {(1,a), (1,b), (1,c),
(2,a), (2,b), (2,c)}.

Cartesian Product

$$A \times B = \{\, (a, b) : a \in A, b \in B \,\}$$

$\mathbb{R} \times \mathbb{R}$ is the real plane. You've seen ordered pairs before.

These are just for arbitrary sets.

$\mathbb{Z} \times \mathbb{Z}$ is "the set of all pairs of integers"

If A = {1, 2}, B = {a, b, c}, then A × B = {(1,a), (1,b), (1,c),
(2,a), (2,b), (2,c)}.

What is $A \times \emptyset$?

Cartesian Product

$$A \times B = \{\ (a,b) : a \in A, b \in B\ \}$$

$\mathbb{R} \times \mathbb{R}$ is the real plane. You've seen ordered pairs before.

These are just for arbitrary sets.

$\mathbb{Z} \times \mathbb{Z}$ is "the set of all pairs of integers"

If A = {1, 2}, B = {a, b, c}, then A × B = {(1,a), (1,b), (1,c), (2,a), (2,b), (2,c)}.

$$A \times \emptyset = \{(a,b) : a \in A \wedge b \in \emptyset\} = \{(a,b) : a \in A \wedge \mathrm{F}\} = \emptyset$$

Representing Sets Using Bits

- Suppose universe U is $\{1,2,\ldots,n\}$
- Can represent set $B \subseteq U$ as a vector of bits:

  $b_1 b_2 \ldots b_n$ where $b_i = 1$ when $i \in B$

  $b_i = 0$ when $i \notin B$

  – Called the *characteristic vector* of set B

- Given characteristic vectors for A and B
  – What is characteristic vector for $A \cup B$? $A \cap B$?

Bitwise Operations

$$\begin{array}{rl} & 01101101 \\ \vee & \underline{00110111} \\ & 01111111 \end{array}$$

Java: `z=x|y`

$$\begin{array}{rl} & 00101010 \\ \wedge & \underline{00001111} \\ & 00001010 \end{array}$$

Java: `z=x&y`

$$\begin{array}{rl} & 01101101 \\ \oplus & \underline{00110111} \\ & 01011010 \end{array}$$

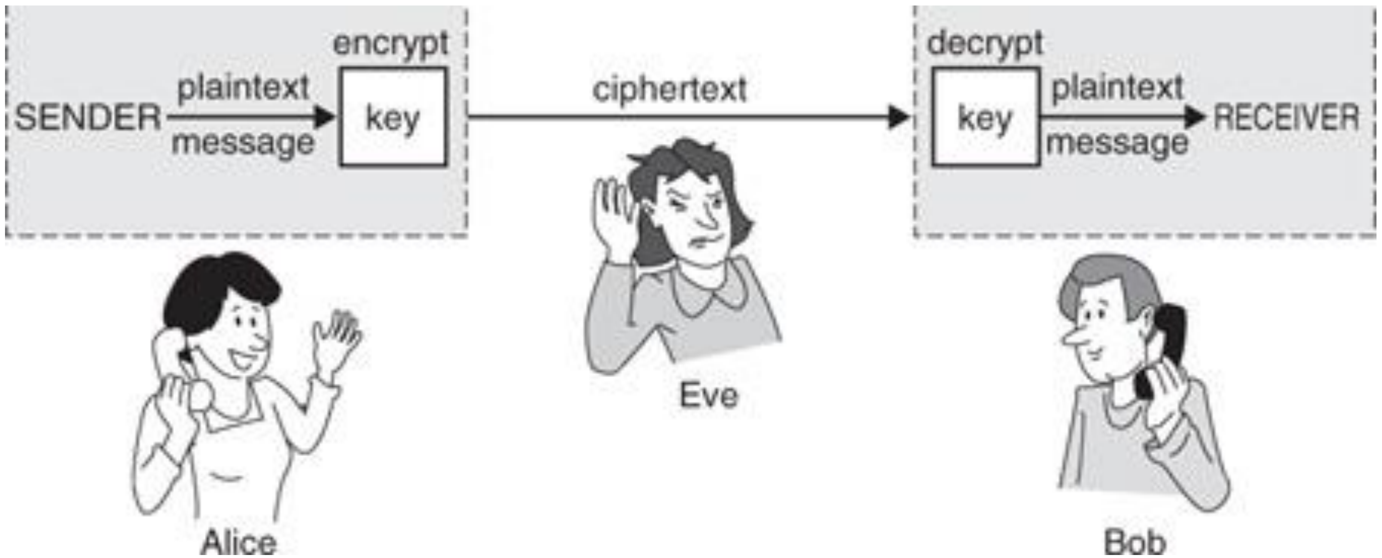
Java: `z=x^y`

A Useful Identity

- If x and y are bits: $(x \oplus y) \oplus y = ?$
- What if x and y are bit-vectors?

Private Key Cryptography

- **Alice** wants to communicate message secretly to **Bob** so that eavesdropper **Eve** who hears their conversation cannot tell what **Alice**'s message is.
- **Alice** and **Bob** can get together and privately share a secret key K ahead of time.



One-Time Pad

- Alice and Bob privately share random n-bit vector K
  - Eve does not know K
- Later, Alice has n-bit message m to send to Bob
  - Alice computes $C = m \oplus K$
  - Alice sends C to Bob
  - Bob computes $m = C \oplus K$ which is $(m \oplus K) \oplus K$
- Eve cannot figure out m from C unless she can guess K

Russell's Paradox

$$\boxed{S = \{\, x : x \notin x \,\}}$$

Suppose for contradiction that $S \in S$...

Russell's Paradox

$$S = \{ x : x \notin x \}$$

Suppose for contradiction that $S \in S$. Then, by definition of S, $S \notin S$, but that's a contradiction.

Suppose for contradiction that $S \notin S$. Then, by definition of the set S, $S \in S$, but that's a contradiction, too.

This is reminiscent of the truth value of the statement "This statement is false."