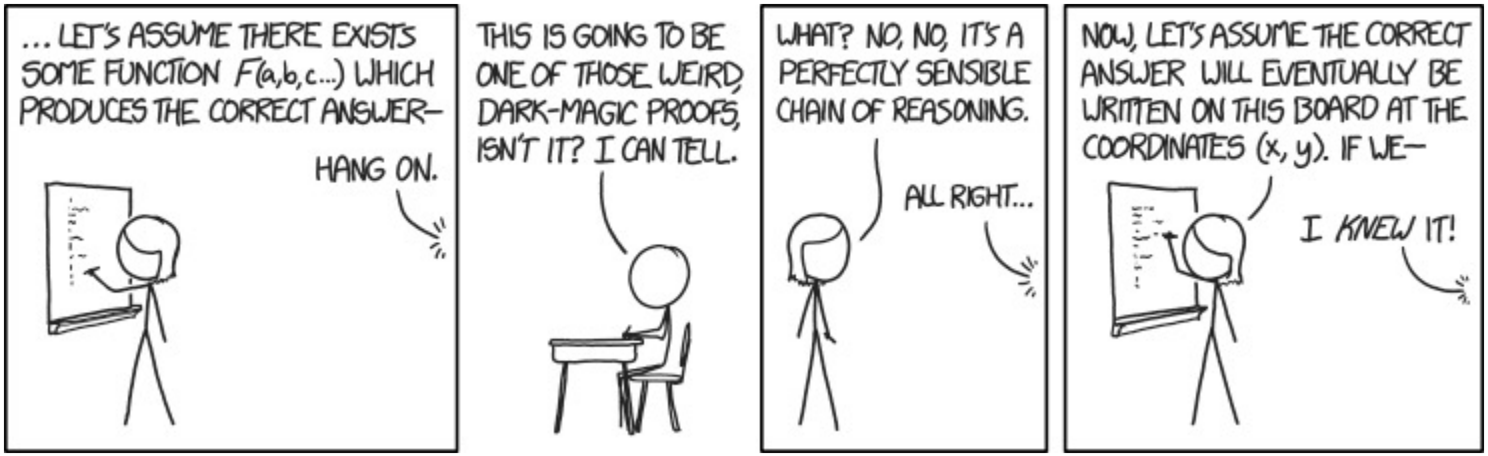
CSE 311: Foundations of Computing

Lecture 10: English proofs and proof strategies



Recap from last lecture: Inference proofs

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

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

Intro ∀
$$\frac{\text{"Let } a \text{ be arbitrary*"} \ldots P(a)}{\therefore\ \forall x\, P(x)}$$

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

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

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

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

Recap from last lecture: Inference proofs

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

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

Intro $\forall$: $\dfrac{\text{"Let } a \text{ be arbitrary*"} \ldots P(a)}{\therefore \quad \forall x\, P(x)}$

Elim $\exists$: $\dfrac{\exists x\, P(x)}{\therefore \; P(c) \text{ for some } \textit{special}^{**}\; c}$

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

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

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

1. Let **a** be an arbitrary integer
   - 2.1 $\text{Even}(\mathbf{a})$ — Assumpt.
   - 2.2 $\exists y\, (\mathbf{a} = 2y)$ — Def. Even
   - 2.3 $\mathbf{a} = 2\mathbf{b}$ — Elim $\exists$: **b** special depends on **a**
   - 2.4 $\mathbf{a}^2 = 4\mathbf{b}^2 = 2(2\mathbf{b}^2)$ — Algebra
   - 2.5 $\exists y\, (\mathbf{a}^2 = 2y)$ — Intro $\exists$ rule
   - 2.6 $\text{Even}(\mathbf{a}^2)$ — Definition of Even
2. $\text{Even}(\mathbf{a}) \rightarrow \text{Even}(\mathbf{a}^2)$ — Direct proof rule
3. $\forall x\, (\text{Even}(x) \rightarrow \text{Even}(x^2))$ — Intro $\forall$: 1,2

Used $\mathbf{a}^2 = 2c$ for $c = 2\mathbf{b}^2$

English Proofs

- We often write proofs in English rather than as fully formal proofs
  - They are more natural to read

- English proofs follow the structure of the corresponding formal proofs
  - Formal proof methods help to understand how proofs really work in English…

    … and give clues for how to produce them.

Formal Proofs

- 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

- But they are **tedious** and impractical
  - e.g., applications of commutativity and associativity
  - Russell & Whitehead's formal proof that 1+1 = 2 is *several hundred pages* long

    we allowed ourselves to cite "Arithmetic", "Algebra", etc.

- Similar situation exists in programming…

Programming

```
%a = add %i, 1
%b = mod %a, %n
%c = add %arr, %b
%d = load %c
%e = add %arr, %i
store %e, %d
```

```
arr[i] = arr[(i+1) % n];
```

Assembly Language

High-level Language

Programming vs Proofs

%a = add %i, 1	Given
%b = mod %a, %n	Given
%c = add %arr, %b	∧ Elim: 1
%d = load %c	Double Negation: 4
%e = add %arr, %i	∨ Elim: 3, 5
store %e, %d	MP: 2, 6
Assembly Language for Programs	**Assembly Language for Proofs**

Proofs

Given

Given

$\wedge$ Elim: 1

Double Negation: 4

$\vee$ Elim: 3, 5

MP: 2, 6

what is the "Java" for proofs?

Assembly Language for Proofs

High-level Language for Proofs

Proofs

Given

Given

∧ Elim: 1

Double Negation: 4

∨ Elim: 3, 5

MP: 2, 6

English

Assembly Language for Proofs

High-level Language for Proofs

Proofs

- **Formal proofs follow simple well-defined rules and should be easy for a machine to check**
  - as assembly language is easy for a machine to execute

- **English proofs correspond to those rules but are designed to be easier for humans to read**
  - **also easy to check with practice**

    (almost all actual math and theory CS is done this way)
  - **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)

Last class: Even and Odd

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

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

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

1.	Let **a** be an arbitrary integer	
2.1	$\text{Even}(\mathbf{a})$	Assumption
2.2	$\exists y\ (\mathbf{a} = 2y)$	Definition of Even
2.3	$\mathbf{a} = 2\mathbf{b}$	Elim $\exists$: **b** special depends on **a**
2.4	$\mathbf{a}^2 = 4\mathbf{b}^2 = 2(2\mathbf{b}^2)$	Algebra
2.5	$\exists y\ (\mathbf{a}^2 = 2y)$	Intro $\exists$ rule
2.6	$\text{Even}(\mathbf{a}^2)$	Definition of Even
2.	$\text{Even}(\mathbf{a}) \rightarrow \text{Even}(\mathbf{a}^2)$	Direct proof rule
3.	$\forall x\,(\text{Even}(x) \rightarrow \text{Even}(x^2))$	Intro $\forall$: 1,2

English Proof: Even and Odd

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

Prove "The square of every even integer is even."

Let a be an arbitrary integer.	1. Let a be an arbitrary integer
Suppose a is even.	2.1 $\text{Even}(a)$ — Assumption
Then, by definition, $a = 2b$ for some integer b (dep on a).	2.2 $\exists y\ (a = 2y)$ — Definition 2.3 $a = 2b$ — b special depends on a
Squaring both sides, we get $a^2 = 4b^2 = 2(2b^2)$.	2.4 $a^2 = 4b^2 = 2(2b^2)$ — Algebra
So a^2 is, by definition, even.	2.5 $\exists y\ (a^2 = 2y)$ 2.6 $\text{Even}(a^2)$ — Definition
Since a was arbitrary, we have shown that the square of every even number is even.	2. $\text{Even}(a) \rightarrow \text{Even}(a^2)$ 3. $\forall x\ (\text{Even}(x) \rightarrow \text{Even}(x^2))$

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, $a = 2b$ for some integer b (depending on **a**). 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. ■

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

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."

Proof: Let x and y be arbitrary integers. Suppose that both are odd.

Then, $x = 2a + 1$ for some integer a (depending on x) and $y = 2b + 1$ for some integer b (depending on x). 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(x) ≡ ∃y (x=2y)
Odd(x) ≡ ∃y (x=2y+1)
Domain: Integers

English Proof: Even and Odd

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

English		Formal	
Let x and y be arbitrary integers.	1.	Let **x** be an arbitrary integer	
	2.	Let **y** be an arbitrary integer	
Suppose that both are odd.	2.1	Odd(**x**) ∧ Odd(**y**)	Assumption
	2.2	Odd(**x**)	Elim ∧: 2.1
	2.3	Odd(**y**)	Elim ∧: 2.1
Then, x = 2a+1 for some integer a (depending on x) and	2.4	∃**z** (**x** = 2**z**+1)	Def of Odd: 2.2
	2.5	**x** = 2**a**+1	Elim ∃: 2.4 (**a** dep **x**)
y = 2b+1 for some integer b (depending on x).	2.5	∃**z** (**y** = 2**z**+1)	Def of Odd: 2.3
	2.6	**y** = 2**b**+1	Elim ∃: 2.5 (**b** dep **y**)
Their sum is x+y = ... = 2(a+b+1)	2.7	**x+y = ... =** 2(**a+b+1**)	Algebra
so x+y is, by definition, even.	2.8	∃z (**x+y** = 2z)	Intro ∃: 2.4
	2.9	Even(x+y)	Def of Even
Since x and y were arbitrary, the sum of any odd integers is even.	2.	(Odd(**x**) ∧ Odd(y)) → Even(**x+y**)	
	3.	∀x ∀ y ((Odd(**x**) ∧ Odd(y)) → Even(**x+y**))	

Lecture 10 Activity

- You will be assigned to **breakout rooms**. Please:
- Introduce yourself
- Choose someone to share screen, showing this PDF
- Consider the statement:

The sum of two even numbers is even.

- Recall that an integer x is even if and only if there is an integer z with $x = 2z$.
- Please do the following
  1. Write the statement in predicate logic
  2. Write an English proof

Fill out a poll everywhere for Activity Credit!
Go to pollev.com/thomas311 and login with your UW identity

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

Proof: Let x and y be arbitrary integers. Suppose that both are odd. Then, $x = 2a + 1$ for some integer a (depending on x) and $y = 2b + 1$ for some integer b (depending on x). 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.

Rational Numbers

Domain of Discourse
Real Numbers

- **A real number x is *rational* iff there exist integers p and q with $q \neq 0$ such that $x = p/q$.**

$$\text{Rational}(x) \equiv \exists p\, \exists q\, ((x = p/q) \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge q \neq 0)$$

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) $\equiv \exists p\, \exists q\, ((x = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0))$

Prove: "If x and y are rational, then xy is rational."

Formally, prove $\forall x\, \forall y\, \big(\big(Rational(x) \land Rational(y)\big) \rightarrow Rational(x \cdot y)\big)$

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) $\equiv \exists p\, \exists q\ ((x = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0))$

Prove: "If x and y are rational, then xy is rational."

Proof: Suppose that x and y are rational. Then, x = a/b for some integers a, b, where b≠0, and y = c/d for some integers c,d, where d≠0.

Multiplying, we get that xy = (ac)/(bd). Since b and d are both non-zero, so is bd. Furthermore, ac and bd are integers. By definition, then, xy is rational.

■

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) $\equiv \exists p\ \exists q\ ((x = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0))$

Prove: "The product of two rationals is rational."

Proof: Let x and y be arbitrary.

Suppose that x and y are rational. Then, x = a/b for some integers a, b, where b≠0, and y = c/d for some integers c,d, where d≠0.

Multiplying, we get that xy = (ac)/(bd). Since b and d are both non-zero, so is bd. Furthermore, ac and bd are integers. By definition, then, xy is rational.

Since x and y were arbitrary, we have shown that the product of any two rationals is rational. ■

English Proofs

- High-level language let us work more quickly
  - should not be necessary to spill out every detail
  - reader checks that the writer is not skipping too much
  - examples so far

    skipping Intro ∧ and Elim ∧

    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 reader 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 $\exists\neg P(x)$:

- Works by de Morgan's Law: $\neg\forall \boldsymbol{x}\ \boldsymbol{P(x)} \equiv \exists \boldsymbol{x} \neg \boldsymbol{P(x)}$
- All we need to do that is find an $\boldsymbol{x}$ where $\boldsymbol{P(x)}$ is **false**
- This example is called a ***counterexample*** to $\forall \boldsymbol{x}\ \boldsymbol{P(x)}$.

e.g. Prove "Not every prime number is odd"

Proof: 2 is prime but not odd, a counterexample to the claim that every prime number is odd. $\blacksquare$

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 $p \rightarrow q$.

	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 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. $p \rightarrow$ 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 shows F, 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 $\neg \exists x\ (\text{Even}(x) \wedge \text{Odd}(x))$

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 $\neg \exists x\ (\mathrm{Even}(x) \wedge \mathrm{Odd}(x))$

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=2b+1 and hence a=b+½.

But two integers cannot differ by ½, so this is a contradiction. ■

A proof with multiples

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

A proof with multiples

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) $\equiv \exists a\ (a \geq 2 \wedge y = ax)$

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.

A proof with multiples

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

<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.

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

A proof with multiples

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

<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>

A proof with multiples

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

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.

A proof with multiples

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

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.

A proof with multiples

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

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.

A proof with multiples

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

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.
Assume for the sake of contradiction that z is a strict multiple of x and y is a strict multiple of z.

A proof with multiples

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

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 $b \geq 2$.

A proof with multiples

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

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 $2x = y = bz = abx$.

A proof with multiples

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

<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.
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)

Applications of Predicate Logic

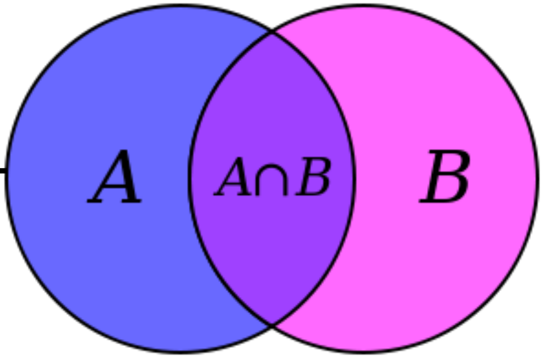
- Remainder of the course will use predicate logic to prove important properties of interesting objects
  - start with math objects that are widely used in CS
  - eventually more CS-specific objects

- 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



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 = {☐, 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

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

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

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}

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

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

(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 Boolean algebra 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 $\forall \mathrm{x}\ (x \in (A \cup B)^C \leftrightarrow x \in A^C \cap B^C)$

Proof: Let x be an arbitrary object.

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

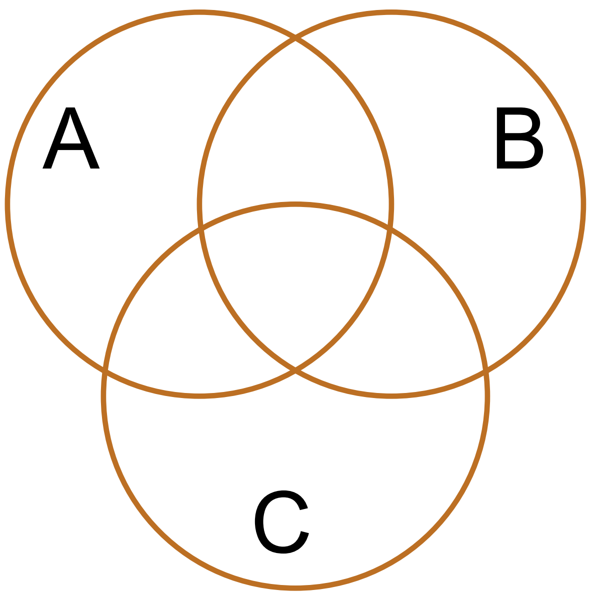
The stated bi-condition holds since:

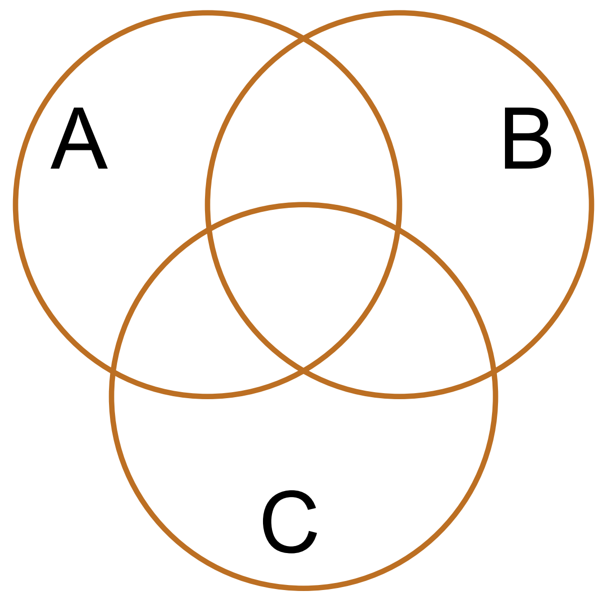
$x \in (A \cup B)^C$	$\equiv \neg(x \in A \cup B)$	def of $-^C$
	$\equiv \neg(x \in A \vee x \in B)$	def of $\cup$
	$\equiv \neg(x \in A) \wedge \neg(x \in B)$	De Morgan
	$\equiv x \in A^C \wedge x \in B^C$	def of $-^C$
	$\equiv x \in A^C \cap B^C$	def of $\cap$

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

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

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

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)}.

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

Representing Sets Using Bits

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

$$b_1 b_2 \ldots b_n \text{ where } \quad \begin{array}{l} b_i = 1 \text{ when } i \in B \\ b_i = 0 \text{ when } i \notin B \end{array}$$

  - **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`

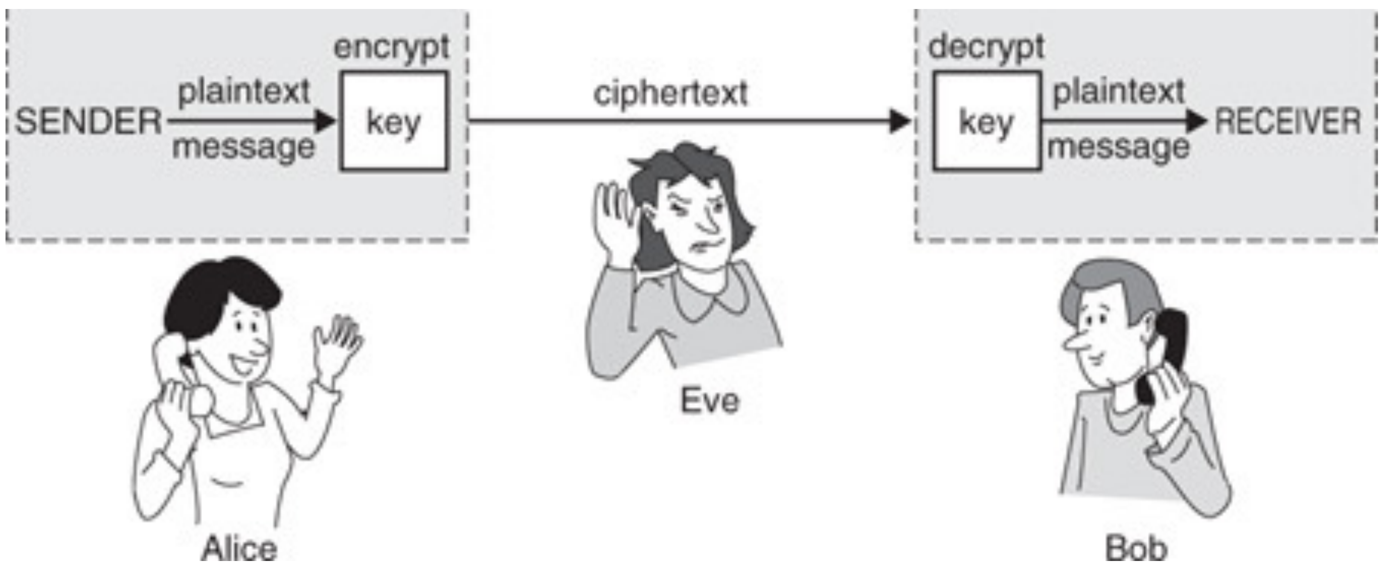
A Useful Identity

- 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."