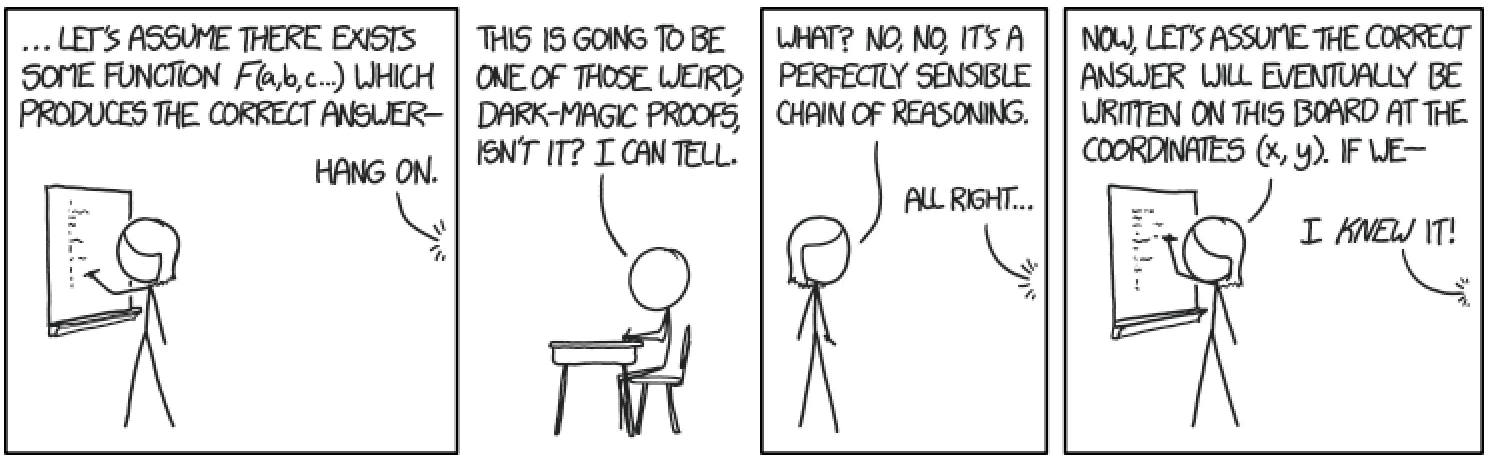
CSE 311: Foundations of Computing

Lecture 9: English Proofs, Strategies, Set Theory



Last class: Inference Rules for Quantifiers

Intro ∃

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

Elim ∀

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

Intro ∀

$$\frac{\text{“}\textbf{Let } a \textbf{ be arbitrary*}\text{”} \ldots P(a)}{\therefore \quad \forall x\, P(x)}$$

* in the domain of P. No other name in P depends on a

Elim ∃

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

** c is a NEW name.
List all dependencies for c.

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

Last class: Even and Odd

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	Even(**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	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

Last Class: 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 even integer.

1. Let a be an arbitrary integer
   - 2.1 Even(a) — Assumption

Then, by definition, $a = 2b$ for some integer b (depending 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

Since $2b^2$ is an integer, by definition, a^2 is even.

   - 2.5 $\exists y\ (a^2 = 2y)$
   - 2.6 Even(a^2) — Definition

Since a was arbitrary, it follows that the square of every even number is even. ■

2. Even(a)$\rightarrow$Even(a^2)
3. $\forall x$ (Even(x)$\rightarrow$Even(x^2))

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 in 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)

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."

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."

Formally, prove $\forall x\ \forall y\ ((\text{Odd}(x) \land \text{Odd}(y)) \rightarrow \text{Even}(x+y))$

5. $\forall \mathbf{x}\ \forall \mathbf{y}\ ((\text{Odd}(\mathbf{x}) \land \text{Odd}(\mathbf{y})) \rightarrow \text{Even}(\mathbf{x}+\mathbf{y}))$

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."

Formally, prove $\forall x\ \forall y\ ((\text{Odd}(x) \wedge \text{Odd}(y)) \rightarrow \text{Even}(x+y))$

5. $\forall \mathbf{u}\ \forall \mathbf{v}\ ((\text{Odd}(\mathbf{u}) \wedge \text{Odd}(\mathbf{v})) \rightarrow \text{Even}(\mathbf{u}+\mathbf{v}))$

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."

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

Let x and y be arbitrary integers.

Suppose that x and y are odd

∴ x+y is even

Since x and y were arbitrary, the sum of ~~any~~ two odd integers is even.

1. **Let x be an arbitrary integer**
2. **Let y be an arbitrary integer**

3.1 Odd(x) ∧ Odd(y) Assump

?.? Even(x+y)

3. (Odd(**x**) ∧ Odd(**y**)) → Even(**x+y**)
4. ∀v ((Odd(**x**) ∧ Odd(**v**)) → Even(x+v)) Intro ∀
5. ∀**u** ∀v ((Odd(**u**) ∧ Odd(**v**)) → Even(**u**+v)) Intro ∀

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 ∀x ∀y ((Odd(x) ∧ Odd(y))→Even(x+y))

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.	3.1 Odd(**x**) ∧ Odd(**y**) Assumption
so x+y is even.	3.9 Even(**x+y**)
Since x and y were arbitrary, the sum of any odd integers is even.	3. (Odd(**x**) ∧ Odd(**y**)) → Even(**x+y**) Direct Proof 4. ∀**v** ((Odd(**x**) ∧ Odd(**v**)) → Even(**x**+**v**)) Intro ∀ 5. ∀**u** ∀**v** ((Odd(**u**) ∧ Odd(**v**)) → Even(**u**+**v**)) Intro ∀

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

Let x and y be arbitrary integers.

Suppose that both are odd.

∴ x=2a+1 for some integer a (depends on x)

y=2b+1 for some integer b (depends on y)

so x+y is even.

Since x and y were arbitrary, the sum of any odd integers is even.

1. **Let x be an arbitrary integer**
2. **Let y be an arbitrary integer**

3.1	Odd(**x**) ∧ Odd(**y**)	Assumption
3.2	Odd(**x**)	Elim ∧: 2.1
3.3	Odd(**y**)	Elim ∧: 2.1
3.4	∃z (x=2z+1)	def
3.5	∃z (y=2z+1)	def
	x=2a+1	Elim ∃, a dep x
	y=2b+1	Elim ∃, b dep y
3.9	Even(**x+y**)	

3. (Odd(**x**) ∧ Odd(**y**)) → Even(**x+y**)
4. ∀v ((Odd(**x**) ∧ Odd(**v**)) → Even(**x+v**)) Intro ∀
5. ∀u ∀v ((Odd(**u**) ∧ Odd(**v**)) → Even(**u+v**)) Intro ∀

English Proof: Even and Odd

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

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

English	Line	Statement	Justification
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.	3.1	Odd(**x**) ∧ Odd(**y**)	Assumption
	3.2	Odd(**x**)	Elim ∧: 2.1
	3.3	Odd(**y**)	Elim ∧: 2.1
Then, x = 2a+1 for some integer a (depending on x) and	3.4	∃**z** (**x** = 2**z**+1)	Def of Odd: 2.2
	3.5	**x** = 2**a**+1	Elim ∃: 2.4 (**a** dep **x**)
y = 2b+1 for some integer b (depending on x).	3.6	∃**z** (**y** = 2**z**+1)	Def of Odd: 2.3
	3.7	**y** = 2**b**+1	Elim ∃: 2.5 (**b** dep **y**)
∴ x+y = 2a+1+2b+1 = 2(a+b+1)	3.8	x+y = 2a+1+2b+1 = 2(a+b+1)	
so x+y is, by definition, even.	3.9	∃z (**x+y** = 2z)	Intro ∃: ~~2.4~~ 3.8
	3.10	Even(**x+y**)	Def of Even
Since x and y were arbitrary, the sum of any odd integers is even.	3.	(Odd(**x**) ∧ Odd(**y**)) → Even(**x+y**)	
	4.	∀**v** ((Odd(**x**) ∧ Odd(**v**)) → Even(**x+v**))	Intro ∀
	5.	∀**u** ∀**v** ((Odd(**u**) ∧ Odd(**v**)) → Even(**u+v**))	Intro ∀

English Proof: Even and Odd

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

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

English proof	Formal proof		
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.	**3.1**	Odd(**x**) ∧ Odd(**y**)	Assumption
	3.2	Odd(**x**)	Elim ∧: 2.1
	3.3	Odd(**y**)	Elim ∧: 2.1
Then, x = 2a+1 for some integer a (depending on x) and	**3.4**	∃**z** (**x** = 2**z**+1)	Def of Odd: 2.2
	3.5	**x** = 2**a**+1	Elim ∃: 2.4 (**a** dep **x**)
y = 2b+1 for some integer b (depending on x).	**3.6**	∃**z** (**y** = 2**z**+1)	Def of Odd: 2.3
	3.7	**y** = 2**b**+1	Elim ∃: 2.5 (**b** dep **y**)
Their sum is x+y = ... = 2(a+b+1)	**3.8**	**x+y** = 2(**a**+**b**+1)	Algebra
so x+y is, by definition, even.	**3.9**	∃z (**x+y** = 2z)	Intro ∃: 2.4
	3.10	Even(**x+y**)	Def of Even
Since x and y were arbitrary, the sum of any odd integers is even.	**3.**	(Odd(**x**) ∧ Odd(**y**)) → Even(**x+y**)	
	4.	∀**v** ((Odd(**x**) ∧ Odd(**v**)) → Even(**x**+**v**))	Intro ∀
	5.	∀**u** ∀**v** ((Odd(**u**) ∧ Odd(**v**)) → Even(**u**+**v**))	Intro ∀

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 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 **odd** integers.

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. ■

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

Proof Strategies: Counterexamples

To *disprove* ∀x P(x) prove ∃x¬P(x) :

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

e.g. Disprove "Every prime number is odd"

$\neg\forall x\,(\text{Prime}(x) \to \text{Odd}(x))$

$\equiv \exists x\,(\text{Prime}(x) \land \neg\text{Odd}(x))$

$\text{Prime}(2) \land \neg\text{Odd}(2)$ ✓

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 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

Even and Odd

Predicate Definitions
Even(x) ≡ $\exists y\ (x = 2y)$
Odd(x) ≡ $\exists y\ (x = 2y + 1)$

Domain of Discourse
Integers

Prove: "No integer is both even and odd."

English proof: $\neg\exists x\ (\text{Even}(x) \wedge \text{Odd}(x))$ $\neg p$

$\equiv \forall x\ \neg(\text{Even}(x) \wedge \text{Odd}(x))$

Proof by contradiction:

Suppose that integer x is both even and odd

$\therefore$ $x = 2a$ and $x = 2b+1$ for integers a and b depending on x.

$\therefore$ $2a = 2b+1$ $\therefore$ $a = b + 1/2$

This a contradiction since no two integers differ by 1/2

$\therefore$ No integer is both odd and even

Even and Odd

Predicate Definitions
Even(x) ≡ $\exists y\ (x = 2y)$
Odd(x) ≡ $\exists y\ (x = 2y + 1)$

Domain of Discourse
Integers

Prove: "No integer is both even and odd."

English proof: $\neg \exists x\ (\text{Even}(x) \wedge \text{Odd}(x))$

$\equiv \forall x\ \neg(\text{Even}(x) \wedge \text{Odd}(x))$

Proof: We work by contradiction. Let x be an arbitrary integer and suppose that it is both even and odd. Then x=2a for some integer a and x=2b+1 for some integer b. Therefore 2a=2b+1 and hence a=b+½.

But two integers cannot differ by ½ so this is a contradiction. So, no integer is both even and odd. ■

Rationality

Domain of Discourse
Real Numbers

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

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

Rationality

Domain of Discourse
Real Numbers

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

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

Formally, prove $\forall x\ \forall y\ ((\text{Rational}(x) \wedge \text{Rational}(y)) \rightarrow \text{Rational}(xy))$

Rationality

Domain of Discourse
Real Numbers

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

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

Proof: Let x and y be arbitrary rational numbers.

$\therefore$ $x = a/b$ for integers a, b, $b \neq 0$ (depend on x)

$y = c/d$ for integers c, d, $d \neq 0$ (— on y)

$\therefore$ $xy = (a/b)(c/d) = \frac{ac}{bd}$

$bd \neq 0$

ac, bd integers

$\therefore$ xy is rational

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

Rationality

Domain of Discourse
Real Numbers

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

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

Proof: Let x and y be arbitrary rational numbers.

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 xy = (a/b)(c/d) = (ac)/(bd).
Since b and d are both non-zero, so is bd. Furthermore, ac and bd are integers. So, by definition, xy is rational.

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

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

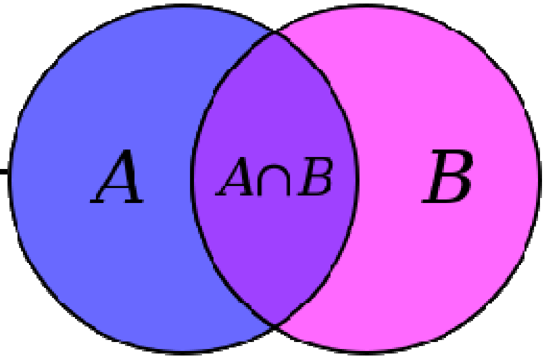
- Remainder of the course will use predicate logic to prove <u>important</u> properties of <u>interesting</u> objects
  - start with math objects that are widely used in CS
  - eventually more CS-specific objects

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

Domain of Discourse
Integers

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

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

ℕ is the set of **Natural Numbers;** ℕ = {0, 1, 2, …}

zahlen ℤ is the set of **Integers**; ℤ = {…, -2, -1, 0, 1, 2, …}

quotient ℚ is the set of **Rational Numbers**; e.g. ½, -17, 32/48

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

[n] {1, 2, …, n}

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

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

$A \subset B$ means $A \subseteq B$ but $A \neq B$

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

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}}

C = D = E

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

$$S = \{x \in A : P(x)\}$$ ← *

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

*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**

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

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

QUESTIONS

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

[6] = A ∪ B ∪ C

{3} = A ∩ B = A ∩ C

{1,2} = A \ B = A \ C

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 ∪ based on ∨**

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

- **Definition for ∩ based on ∧**

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

- **Complement works like ¬**

$$\overline{A} = \{\, x : \neg(x \in A)\}$$

$$0 \leftrightarrow \emptyset$$
$$1 \leftrightarrow U$$

De Morgan's Laws

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

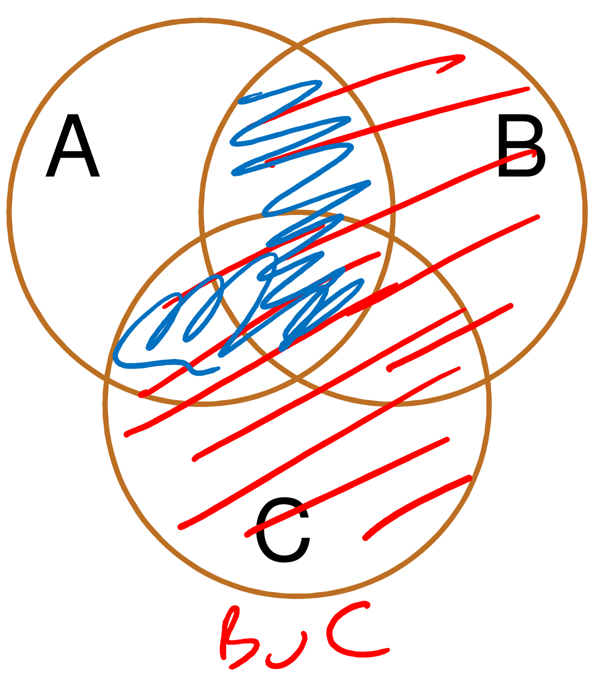
$$(x \in \overline{A \cup B}) \equiv x \notin A \cup B$$
$$\equiv \neg(x \in A \vee x \in B)$$
$$\equiv \neg(x \in A) \wedge \neg(x \in B)$$
$$\equiv x \notin A \wedge x \notin B$$
$$\equiv x \in \bar{A} \wedge x \in \bar{B}$$
$$\equiv x \in \bar{A} \cap \bar{B}$$

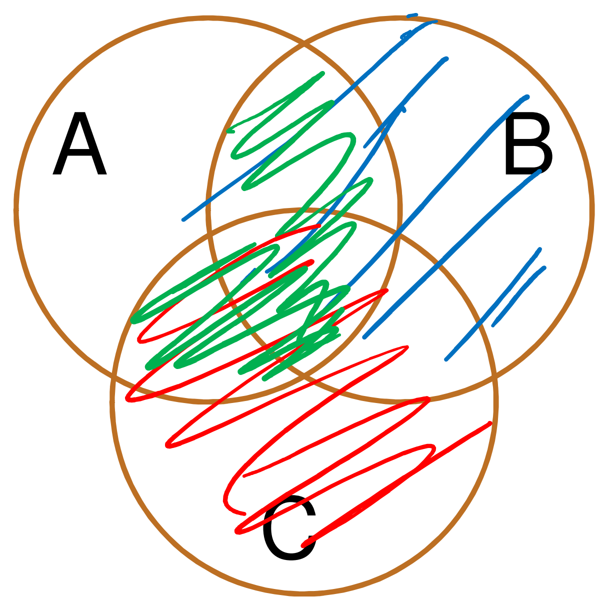
$$\overline{A \cap B} = \bar{A} \cup \bar{B}$$

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

Distributive Laws

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





A Simple Set Proof

Prove that for any sets A and B we have $(A \cap B) \subseteq A$

Remember the definition of subset?

$$X \subseteq Y \equiv \forall x\, (x \in X \to x \in Y)$$

A Simple Set Proof

Prove that for any sets A and B we have $(A \cap B) \subseteq A$

Remember the definition of subset?

$$X \subseteq Y \equiv \forall x\,(x \in X \to x \in Y)$$

Proof: Let A and B be arbitrary sets and x be an arbitrary element of $A \cap B$.
Then, by definition of $A \cap B$, $x \in A$ and $x \in B$.
It follows that $x \in A$, as required. ■

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**

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

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

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)}.

$$\boldsymbol{A} \times \emptyset = \{(\boldsymbol{a}, \boldsymbol{b}) : \boldsymbol{a} \in \boldsymbol{A} \land \boldsymbol{b} \in \emptyset\} = \{(\boldsymbol{a}, \boldsymbol{b}) : \boldsymbol{a} \in \boldsymbol{A} \land \mathbf{F}\} = \emptyset$$

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 $A \cup B$? $A \cap B$?

UNIX/Linux File Permissions

- `ls -l`

```
drwxr-xr-x ... Documents/
-rw-r--r-- ... file1
```

- Permissions maintained as bit vectors
  - Letter means bit is 1
  - “–” means bit is 0.

Bitwise Operations

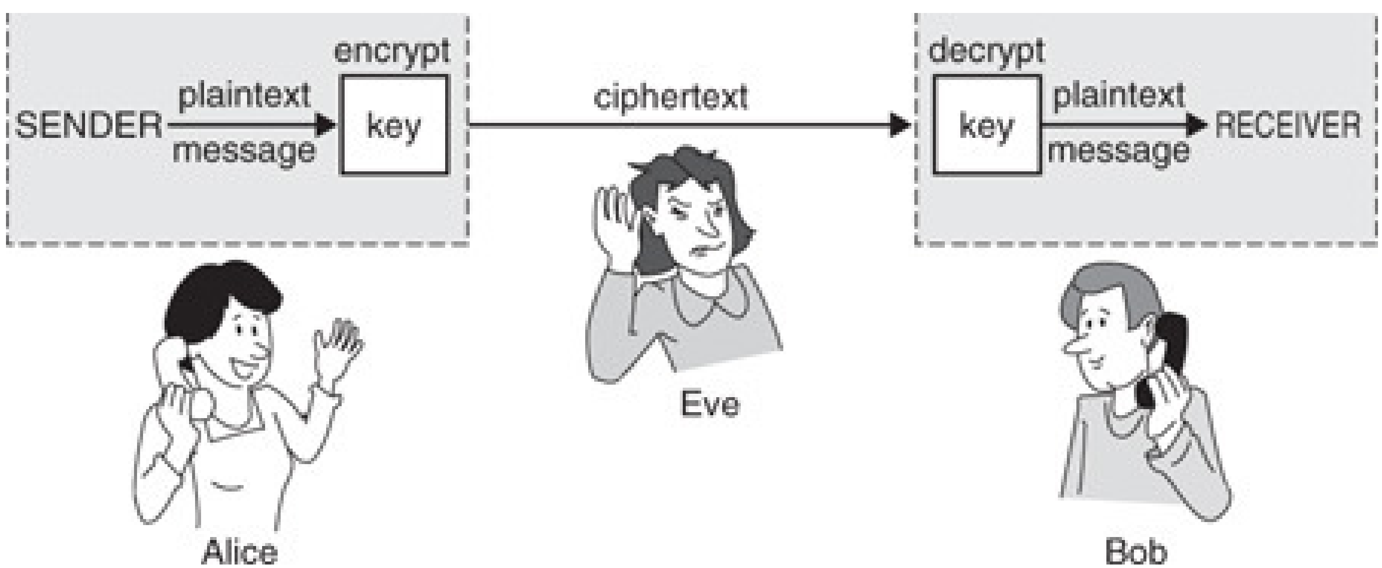
	01101101	Java:	`z=x|y`
$\vee$	00110111		
	01111111		
	00101010	Java:	`z=x&y`
$\wedge$	00001111		
	00001010		
	01101101	Java:	`z=x^y`
$\oplus$	00110111		
	01011010		

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

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

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."