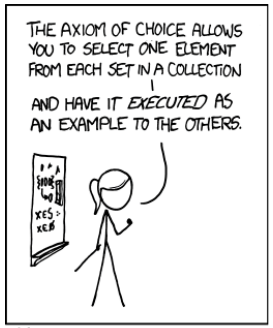
CSE 311



Foundations of Computing I

Fall 2014

Inference rules for quantifiers

$$\frac{P(c) \text{ for some } c}{\therefore \exists x\, P(x)} \qquad \frac{\forall x\, P(x)}{\therefore P(a) \text{ for any } a}$$

$$\frac{\text{“Let } a \text{ be anything*”} \ldots P(a)}{\therefore \forall x\, P(x)} \qquad \frac{\exists x\, P(x)}{\therefore \mathbf{P(c)} \text{ for some } \textit{special}^{**}\ c}$$

* in the domain of P

** 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 variable!

Proof by Contrapositive: Strategy for implications

If we assume $\neg q$ and derive $\neg p$, then we have proven $\neg q \rightarrow \neg p$, which is the same as $p \rightarrow q$.

	1. $\neg q$	Assumption
	...	
	3. $\neg p$	
4. $\neg q \rightarrow \neg p$		Direct Proof Rule
5. $p \rightarrow q$		Contrapositive

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. p	assumption
	...	
	3. F	
4. $p \rightarrow F$		direct Proof rule
5. $\neg p \vee F$		Law of Implication: 4
6. $\neg p$		Identity: 5

Even and Odd

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

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

English proof: ¬ ∃x (Even(x)∧Odd(x))
≡∀x ¬(Even(x)∧Odd(x))

We go by contradiction. Let x be any integer and suppose that it is both even and odd. Then x=2k for some integer k and x=2m+1 for some integer m. Therefore 2k=2m+1 and hence k=m+½.

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

Rational Numbers

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

  Rational(x) ≡ ∃p ∃q ((x=p/q) ∧ Integer(p) ∧ Integer(q) ∧ q≠0)

- **Prove: If x and y are rational then xy is rational**

  ∀x ∀y ((Rational(x) ∧ Rational(y)) → Rational(xy))

Domain: Real numbers

Rationality

Rational(x) ≡ ∃p ∃q ((x=p/q) ∧ Integer(p) ∧ Integer(q) ∧ q≠0)
Domain: Reals

"If x and y are rational then xy is rational."

Proof: Let x and y be 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.

Then xy = (ac)/(bd).

Since b and d are both non-zero, so is bd; furthermore, ac and bd are integers. It follows that xy is rational, by definition of rational.

Rationality

Rational(x) ≡ ∃p ∃q ((x=p/q) ∧ Integer(p) ∧ Integer(q) ∧ q≠0)
Domain: Reals

"If x and y are rational then x+y is rational."

Proofs

- Formal proofs follow simple well-defined rules and should be easy to check
  - In the same way that code should be easy to execute
- English proofs correspond to those rules but are designed to be easier for humans to read
  - Easily checkable in principle
- Simple proof strategies already do a lot
  - Later we will cover a specific strategy that applies to loops and recursion (mathematical induction)

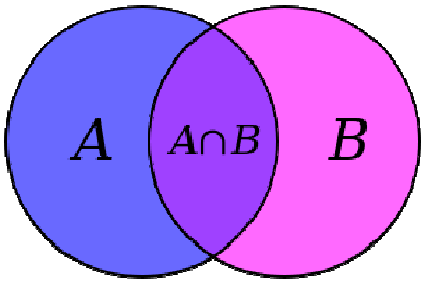
CSE 311: Foundations of Computing

Fall 2014

Lecture 9: Set Theory

Set Theory

- Formal treatment dates from late 19th century
- Direct ties between set theory and logic
- Important foundational language



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
[n] is the set {1, 2, …, n} when n is a natural number
{} = ∅ is the **empty set**; the *only* set with no elements

EXAMPLES
Are these sets?
A = {1, 1}
B = {1, 3, 2}
C = {□, 1}
D = {{}, 17}
E = {1, 2, 7, cat, dog, ∅, α}

We say 2 ∈ E; 3 ∉ E.

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

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

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

Building sets from predicates

- The following says "S is the set of all x's where P(x) is true.

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

- The following says "S is the set of those elements of A for which P(x) is true."

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

- "The set of all the real numbers less than one"

$$\{x \quad \mathbb{R} : x < 1\}$$

- "The set of all powers of two"

$$\{x \quad \mathbb{N} : \exists j\,(x = 2^j)\}$$

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 = {4, 5, 6}
C = {3, 4}

QUESTIONS
Using A, B, C and set operations, make…
[6] = ?
{3} = ?
{1,2} = ?
{1,3} = ?

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, 4, 2, 6}
C = {1, 2, 3, 4}

QUESTIONS

Let S = {1, 2}.
If the universe is A, then $\overline{S}$ is…
If the universe is B, then $\overline{S}$ is…
If the universe is C, then $\overline{S}$ is…

It's Boolean algebra again

- Definition for $\cup$ based on $\vee$
- Definition for $\cap$ based on $\wedge$
- Complement works like $\neg$

Empty Set and power set

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

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

e.g. $\text{Days} = \{M, W, F\}$

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

e.g. $\mathcal{P}(\varnothing) = ?$

Cartesian Product

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

De Morgan's Laws

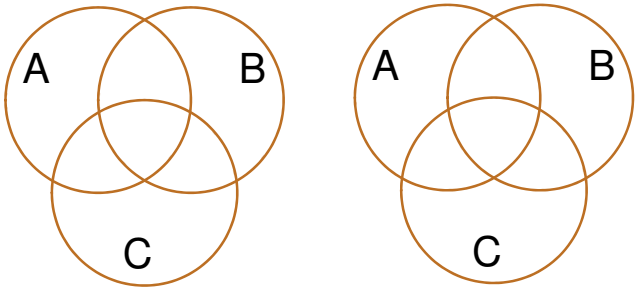
$$\overline{A \cup B} = \bar{A} \cap \bar{B}$$

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

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

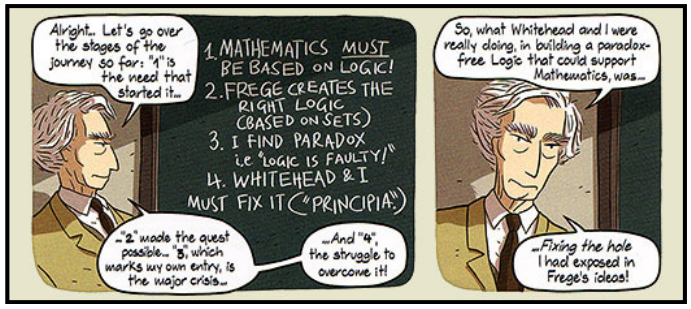
Distributive Laws

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



Russell's Paradox

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



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

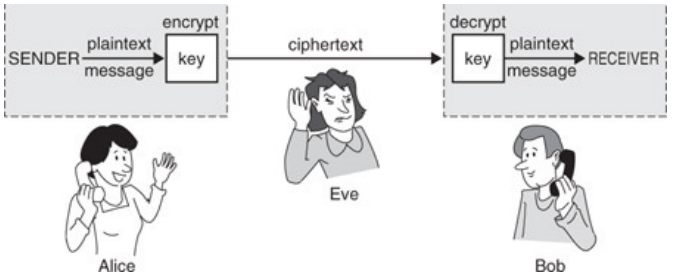
```
  01101101        Java:   z=x|y
∨ 00110111
  01111111

  00101010        Java:   z=x&y
∧ 00001111
  00001010

  01101101        Java:   z=x^y
⊕ 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 ⊕ K
  - Alice sends C to Bob
  - Bob computes m = C ⊕ K which is (m ⊕ K) ⊕ K
- Eve cannot figure out m from C unless she can guess K