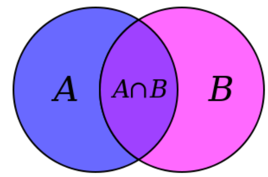
cse 311: foundations of computing

Spring 2015
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**; $\mathbb{N} = \{0, 1, 2, \ldots\}$
$\mathbb{Z}$ 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, 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 write $2 \in E$; $3 \notin E$.

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

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"

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

- "The set of all powers of two"

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

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

$\bar{A} = \{ x : x \notin A \}$ (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 $\bar{S}$ is…
If the universe is B, then $\bar{S}$ is…
If the universe is C, then $\bar{S}$ is…

it's Boolean algebra again! (yay…?)

- 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

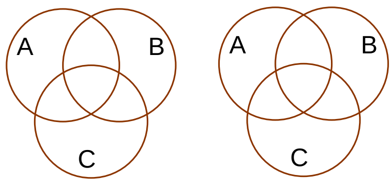
$$\overline{A \cup B} = \bar{A} \cap \bar{B}$$

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

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

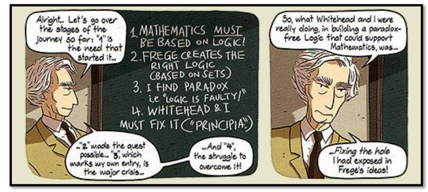
distributive laws

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



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:
  - $b_1 b_2 \cdots b_n$ 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

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

Java: `z=x|y`

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

Java: `z=x&y`

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

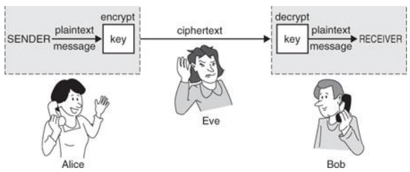
Java: `z=x^y`

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