Announcements

• Reading assignments
  — Wednesday:
    • 4.1-4.2  7th Edition
    • 3.4, 3.6 up to p. 227  6th Edition
    • 2.4, 2.5 up to p. 177  5th Edition
• Homework 4
  — Coming soon . . .

Set Theory

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

Definition: A set is an unordered collection of objects

\[ x \in A : \quad \text{“} x \text{ is an element of } A \text{”} \]
\[ x \notin A : \quad \neg (x \in A) \]

Definitions

• A and B are *equal* if they have the same elements

\[ A = B \iff \forall x \ (x \in A \leftrightarrow x \in B) \]

• A is a *subset* of B if every element of A is also in B

\[ A \subseteq B \iff \forall x \ (x \in A \rightarrow x \in B) \]

Empty Set and Power Set

• Empty set \( \emptyset \) does not contain any elements

• Power set of a set \( A \) = set of all subsets of \( A \)

\[ \mathcal{P}(A) = \{ B : B \subseteq A \} \]
**Cartesian Product:** $A \times B$

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

**Set operations**

- $A \cup B = \{ x \mid (x \in A) \lor (x \in B) \}$
- $A \cap B = \{ x \mid (x \in A) \land (x \in B) \}$
- $A - B = \{ x \mid (x \in A) \land (x \notin B) \}$
- $A \oplus B = \{ x \mid (x \in A) \oplus (x \in B) \}$
- $\overline{A} = \{ x \mid x \notin A \}$ (with respect to universe $U$)

**De Morgan’s Laws**

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

**Proof technique:**

To show $C = D$, show

$\forall x \in C \rightarrow x \in D$ and

$\forall x \in D \rightarrow x \in C$

**Distributive Laws**

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

**Characteristic vectors:**

Representing sets using bits

- Suppose universe $U$ is $\{1,2,...,n\}$
- Can represent set $B \subseteq U$ as a vector of bits:
  
  $b_1b_2...b_n$ where $b_i=1 \equiv (i \in B)$
  
  $b_i=0 \equiv (i \notin B)$

  – Called the characteristic vector of set $B$

- Given characteristic vectors for $A$ and $B$
  
  – What is characteristic vector for $A \cup B$? $A \cap B$?
Boolean operations on bit-vectors: (a.k.a. bit-wise operations)

- 01101101                Java: \( z = x \oplus y \)
  \( \lor \) 00110111
  01111111

- 00101010                Java: \( z = x \land y \)
  \( \land \) 00001111
  00001010

- 01101101                Java: \( z = x \oplus y \)
  \( \oplus \) 00110111
  01011010

A simple 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 be able 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 \( K \)

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.

Russell’s Paradox

\[ S = \{ x \mid x \notin x \} \]
Functions review

• A function from $A$ to $B$
  • an assignment of exactly one element of $B$
    to each element of $A$.
  • We write $f: A \rightarrow B$.
  • “Image of $a$” = $f(a)$
  • Domain of $f$: $A$
  • Range of $f$ = set of all images of elements of $A$

Is this a function? one-to-one? onto?

Image, Preimage