CSE 311: Foundations of Computing

Lecture 10: Set Operations & Representation, Modular Arithmetic

Updates on 2 questions on HW #3 over the weekend

#1, #3

My OH today after class until 12

from 3-3:30

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

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}

<u>QUESTIONS</u>

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

$[6] = A \cup B \cup C$

$\{3\} = A \cap B = A \cap C$

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

More Set Operations

$$A \oplus B = \{ x : (x \in A) \oplus (x \in B)\}$$

Symmetric Difference

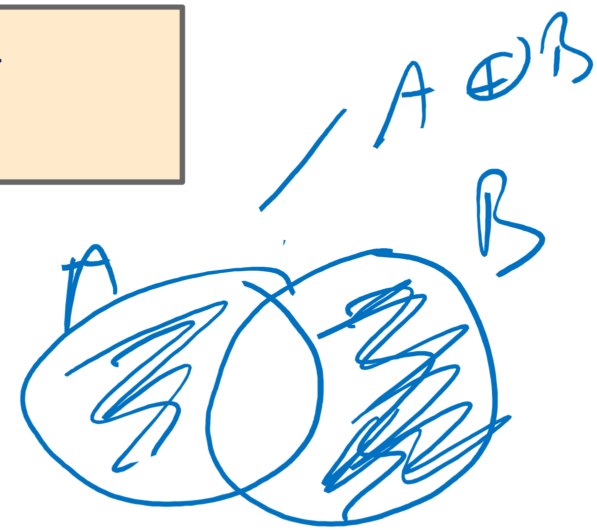
$$\bar{A} = \{ x : x \notin A \} = \{ x : \neg(x \in A)\}$$

(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}
$\bar{A}$ = {4,5,6}



It's Boolean algebra again

- Definition for ∪ based on ∨

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

- Definition for ∩ based on ∧

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

- Complement works like ¬

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

De Morgan's Laws

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

$\subseteq$

- let $x \in \overline{A \cup B}$ be arbitrary.
- $\neg(x \in A \cup B)$
- $\therefore \neg(x \in A \vee x \in B)$
- $\therefore \neg(x \in A) \wedge \neg(x \in B)$ De Morgan
- $\therefore x \notin A$ and $x \notin B$
- $\therefore x \in \bar{A}$ and $x \in \bar{B}$
- $\therefore x \in \bar{A} \cap \bar{B}$.
- $\therefore \overline{A \cup B} \subseteq \bar{A} \cap \bar{B}$

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

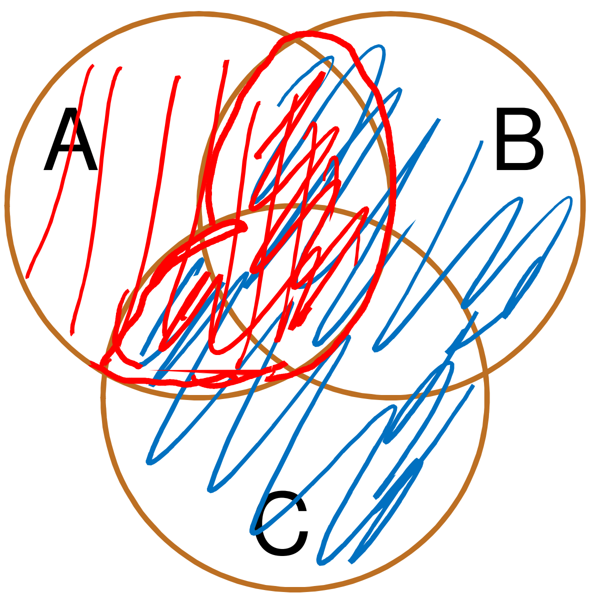
$C \subseteq D$

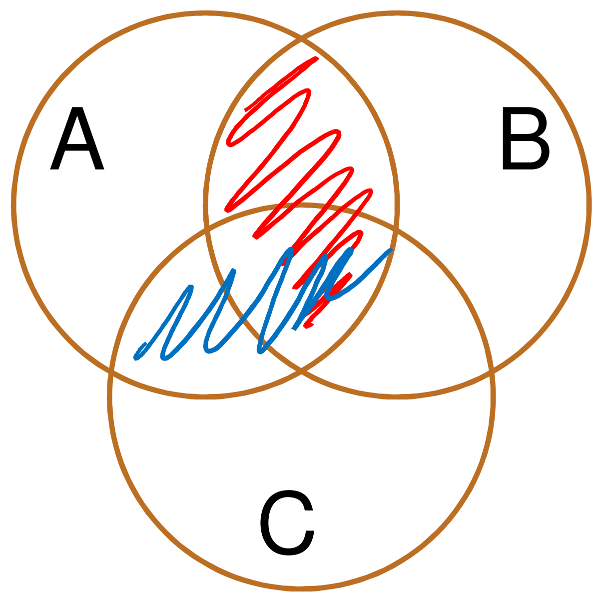
$D \subseteq C$

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

Distributive Laws

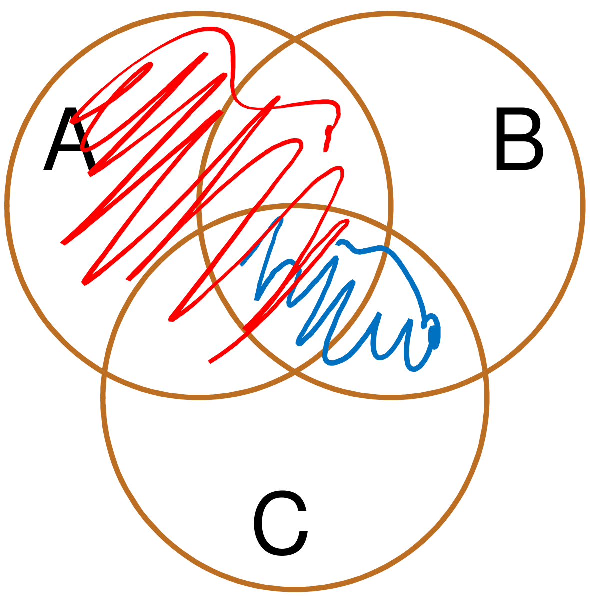
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

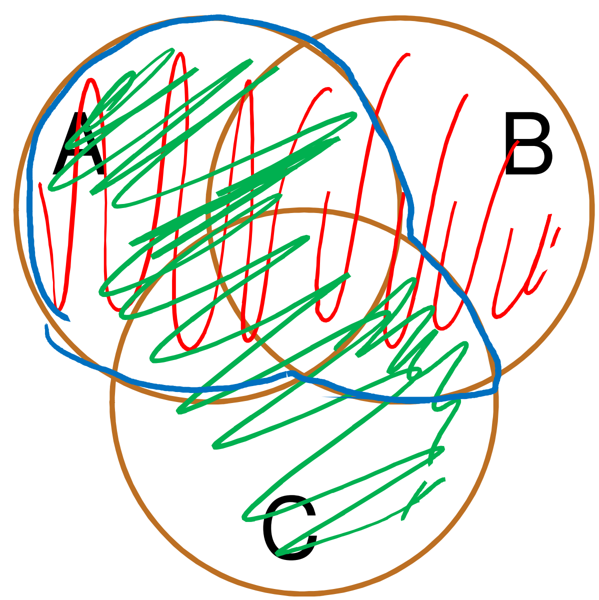




Distributive Laws

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





A Simple Set Proof

intersect

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

Remember the definition of subset?

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

Let a be an arbitrary element of $A \cap B$

Let $a \in A \cap B$ be arbitrary

$\therefore$ $a \in A \wedge a \in B$ by defn of "$\cap$"

$\therefore$ $a \in A$

$\therefore$ $A \cap B \subseteq A$

A Simple Set Proof

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

Remember the definition of subset?

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

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

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

3

- 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

8

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

$\mathcal{P}$(∅)=? $\{ \emptyset \}$

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)}.

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

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

011 01

{2,3,5}

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

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

Java: `z=x|y`

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

Java: `z=x&y`

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

Java: `z=x^y`

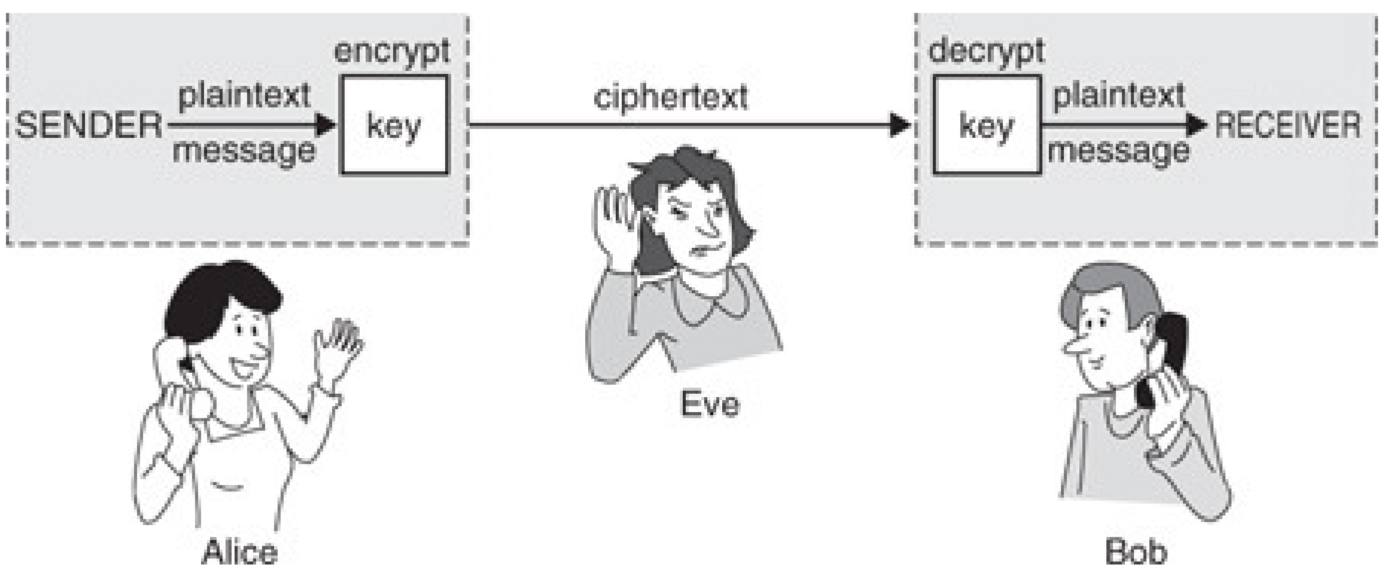
A Useful Identity

- 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 $(m \oplus K) \oplus K = m$
- Eve cannot figure out m from C unless she can guess K

Russell's Paradox

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

Suppose that $S \in S$...

$\therefore$ S doesn't satisfy $x \notin x$

so $S \notin S$

Suppose that $S \notin S$

by this $S \in S$

$x \notin x$ is always true

Russell's Paradox

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

Suppose that $S \in S$. Then, by definition of S, $S \notin S$, but that's a contradiction.

Suppose 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."

Number Theory (and applications to computing)

- Branch of Mathematics with direct relevance to computing
- Many significant applications
  - Cryptography
  - Hashing
  - Security
- Important tool set

Modular Arithmetic

- Arithmetic over a finite domain
- In computing, almost all computations are over a finite domain

I’m ALIVE!

```
public class Test {
    final static int SEC_IN_YEAR = 364*24*60*60*100;
    public static void main(String args[]) {
        System.out.println(
            “I will be alive for at least ” +
            SEC_IN_YEAR * 101 + “ seconds.”
        );
    }
}
```

I’m ALIVE!

```
public class Test {
    final static int SEC_IN_YEAR = 364*24*60*60*100;
    public static void main(String args[]) {
        System.out.println(
            “I will be alive for at least ” +
            SEC_IN_YEAR * 101 + “ seconds.”
        );
    }
}
```

```
 ----jGRASP exec: java Test
I will be alive for at least -186619904 seconds.

 ----jGRASP: operation complete.
```

Divisibility

Definition: "a divides b"

For $a \in \mathbb{Z}, b \in \mathbb{Z}$ with $a \neq 0$:

$$a \mid b \leftrightarrow \exists k \in \mathbb{Z}\ (b = ka)$$

Check Your Understanding. Which of the following are true?

5 | 1	25 | 5	5 | 0	3 | 2
1 | 5	5 | 25	0 | 5	2 | 3

Divisibility

Definition: "a divides b"

For $a \in \mathbb{Z}, b \in \mathbb{Z}$ with $a \neq 0$:

$$a \mid b \leftrightarrow \exists k \in \mathbb{Z}\ (b = ka)$$

Check Your Understanding. Which of the following are true?

5 | 1	25 | 5	5 | 0	3 | 2
5 | 1 iff 1 = 5k	25 | 5 iff 5 = 25k	5 | 0 iff 0 = 5k	3 | 2 iff 2 = 3k
1 | 5	5 | 25	0 | 5	2 | 3
1 | 5 iff 5 = 1k	5 | 25 iff 25 = 5k	0 | 5 iff 5 = 0k	2 | 3 iff 3 = 2k

Division Theorem

Division Theorem

For $a \in \mathbb{Z}, d \in \mathbb{Z}$ with $d > 0$
there exist *unique* integers *q*, *r* with $0 \leq r < d$
such that $a = dq + r$.

To put it another way, if we divide *d* into *a*, we get a unique quotient $q = a$ **div** d
and non-negative remainder $r = a$ **mod** d

$5 = 1 \cdot 3 + 2$ (q, r)

$8 = 2 \cdot 3 + 2$ (q, r)

$-1 = (-1)3 + 2$ (q, r)

Note: r ≥ 0 even if a < 0.
Not quite the same as `a%d`.

Division Theorem

Division Theorem

For $a \in \mathbb{Z}, d \in \mathbb{Z}$ with $d > 0$
there exist *unique* integers *q, r* with $0 \leq r < d$
such that $a = dq + r$.

To put it another way, if we divide *d* into *a*, we get a unique quotient $q = a$ **div** d
and non-negative remainder $r = a$ **mod** d

```
public class Test2 {
    public static void main(String args[]) {
        int a = -5;
        int d = 2;
        System.out.println(a % d);
    }
}
```

$-5 = (-3) \cdot 2 + 1$

```
 ----jGRASP exec: java Test2
-1

 ----jGRASP: operation complete.
```

Note: r ≥ 0 even if a < 0.
Not quite the same as **`a%d`**.

Arithmetic, mod 7

$$a +_7 b = (a + b) \bmod 7$$

$$a \times_7 b = (a \times b) \bmod 7$$

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

x	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Modular Arithmetic

Definition: "a is congruent to b modulo m"

For $a, b, m \in \mathbb{Z}$ with $m > 0$

$$a \equiv b \ (\text{mod}\ m) \leftrightarrow m \mid (a - b)$$

Check Your Understanding. What do each of these mean? When are they true?

$x \equiv 0 \ (\text{mod}\ 2)$

$2 \mid (x - 0)$ i.e. $2 \mid x$

"x is even"

$-1 \equiv 19 \ (\text{mod}\ 5)$ ✓

$-1 - 19 = -20 = (-4) \cdot 5$

$\therefore 5 \mid (-1 - 19)$

$y \equiv 2 \ (\text{mod}\ 7)$

$-19, -12, -5, 2, 9, 16, 23, 30, \ldots 1423$

Modular Arithmetic

Definition: "a is congruent to b modulo m"

For $a, b, m \in \mathbb{Z}$ with $m > 0$

$$a \equiv b \pmod{m} \leftrightarrow m \mid (a - b)$$

Check Your Understanding. What do each of these mean? When are they true?

x ≡ 0 (mod 2)

This statement is the same as saying "x is even"; so, any x that is even (including negative even numbers) will work.

-1 ≡ 19 (mod 5)

This statement is true. 19 - (-1) = 20 which is divisible by 5

y ≡ 2 (mod 7)

This statement is true for y in { ..., -12, -5, 2, 9, 16, ...}. In other words, all y of the form 2+7k for k an integer.

Modular Arithmetic: A Property

Let a, b, m be integers with $m > 0$.
Then, $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

Suppose that $a \equiv b \pmod{m}$.

Suppose that $a \bmod m = b \bmod m$.

Modular Arithmetic: A Property

Let a, b, m be integers with $m > 0$.
Then, $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

Suppose that $a \equiv b \pmod{m}$.

Then, $m \mid (a - b)$ by definition of congruence.

So, $a - b = km$ for some integer k by definition of divides.

Therefore, $a = b + km$.

Taking both sides modulo m we get:

$$a \bmod m = (b + km) \bmod m = b \bmod m.$$

Suppose that $a \bmod m = b \bmod m$.

By the division theorem, $a = mq + (a \bmod m)$ and
$b = ms + (b \bmod m)$ for some integers q,s.

Then, $a - b = (mq + (a \bmod m)) - (ms + (b \bmod m))$
$= m(q - s) + (a \bmod m - b \bmod m)$
$= m(q - s)$ since $a \bmod m = b \bmod m$

Therefore, $m \mid (a - b)$ and so $a \equiv b \pmod{m}$.