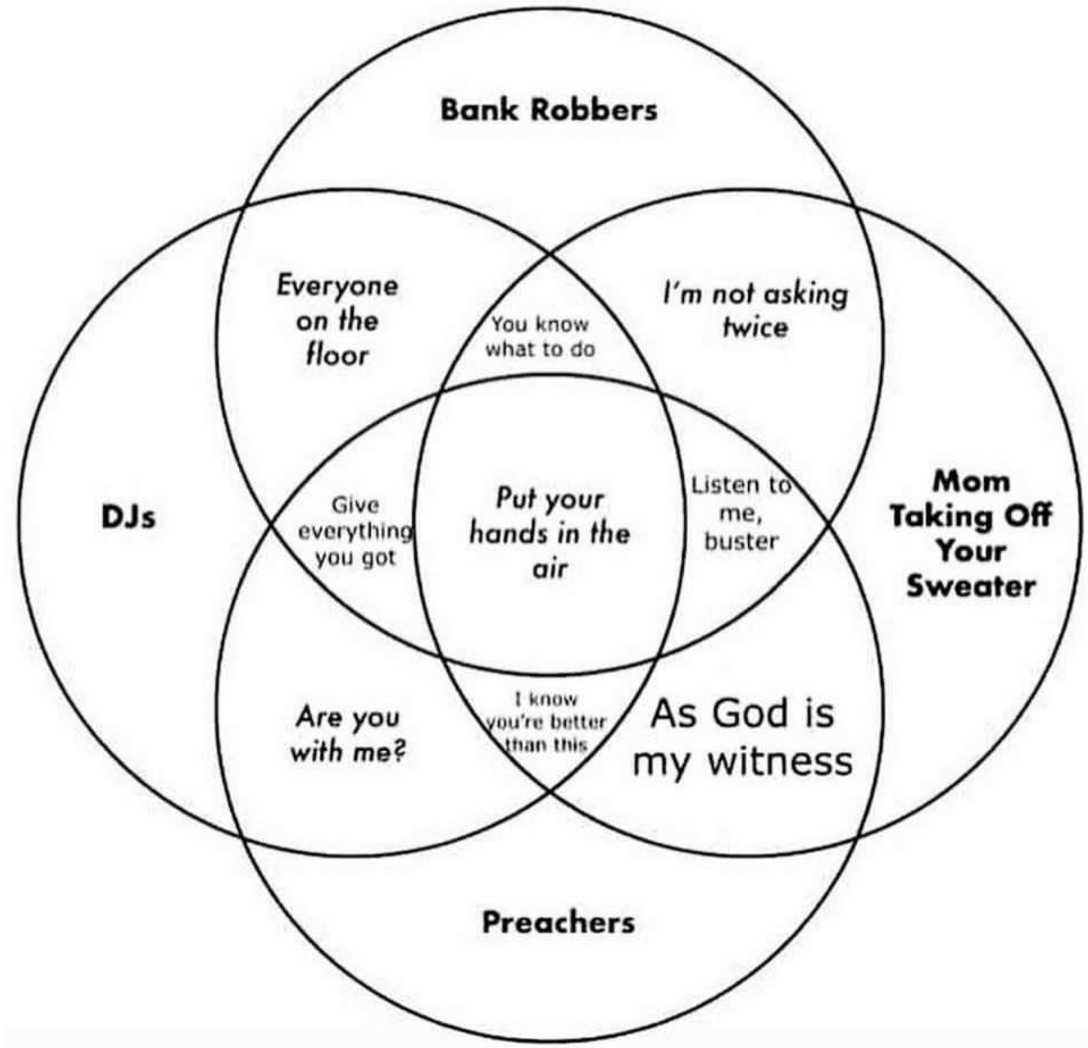
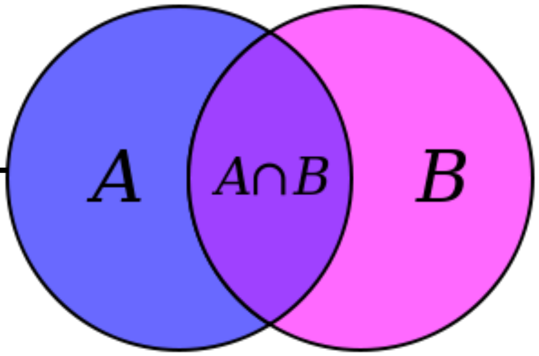
CSE 311: Foundations of Computing

Lecture 10: Sets & Number Theory



Last Time: Set Theory



Sets are collections of objects called **elements.**

Write a ∈ B to say that a is an element of set B,
and a ∉ 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}

Last Time: Operations on Sets

- **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 based on ¬**

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

De Morgan's Laws

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

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

De Morgan's Laws

Prove that $(A \cup B)^C = A^C \cap B^C$

Formally, prove $\forall x\ (x \in (A \cup B)^C \leftrightarrow x \in A^C \cap B^C)$

Proof: Let x be an arbitrary object.

Since x was arbitrary, we have shown, by definition, that $(A \cup B)^C = A^C \cap B^C$.

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

De Morgan's Laws

Formally, prove $\forall x\ (x \in (A \cup B)^C \leftrightarrow x \in A^C \cap B^C)$

1. Let x be arbitrary
    2.1. $x \in (A \cup B)^C$ Assumption
    ...
    2.3. $x \in A^C \cap B^C$
2. $x \in (A \cup B)^C \rightarrow x \in A^C \cap B^C$ Direct Proof
    3.1. $x \in A^C \cap B^C$ Assumption
    ...
    3.3. $x \in (A \cup B)^C$
3. $x \in A^C \cap B^C \rightarrow x \in (A \cup B)^C$ Direct Proof
4. $(x \in (A \cup B)^C \rightarrow x \in A^C \cap B^C) \land (x \in A^C \cap B^C \rightarrow x \in (A \cup B)^C)$ Intro $\land$: 2, 3
5. $x \in (A \cup B)^C \leftrightarrow x \in A^C \cap B^C$ Biconditional: 4
6. $\forall x\ (x \in (A \cup B)^C \leftrightarrow x \in A^C \cap B^C)$ Intro $\forall$: 1-5

De Morgan's Laws

Prove that $(A \cup B)^C = A^C \cap B^C$

Formally, prove $\forall \mathrm{x}\ (x \in (A \cup B)^C \leftrightarrow x \in A^C \cap B^C)$

Proof: Let x be an arbitrary object.

Suppose $x \in (A \cup B)^C$.

…

Thus, we have $x \in A^C \cap B^C$.

De Morgan's Laws

Prove that $(A \cup B)^C = A^C \cap B^C$

Formally, prove $\forall x\ (x \in (A \cup B)^C \leftrightarrow x \in A^C \cap B^C)$

Proof: Let x be an arbitrary object.

Suppose $x \in (A \cup B)^C$. Then, by the definition of complement, we have $\neg(x \in A \cup B)$.

…

Thus, we have $x \in A^C \cap B^C$.

De Morgan's Laws

Prove that $(A \cup B)^C = A^C \cap B^C$

Formally, prove $\forall$x $(x \in (A \cup B)^C \leftrightarrow x \in A^C \cap B^C)$

Proof: Let x be an arbitrary object.

Suppose $x \in (A \cup B)^C$. Then, by the definition of complement, we have $\neg(x \in A \cup B)$. The latter says, by definition, that $\neg(x \in A \vee x \in B)$.

…

Thus, we have $x \in A^C \cap B^C$.

De Morgan's Laws

Prove that $(A \cup B)^C = A^C \cap B^C$

Formally, prove $\forall$x $(x \in (A \cup B)^C \leftrightarrow x \in A^C \cap B^C)$

Proof: Let x be an arbitrary object.

Suppose $x \in (A \cup B)^C$. Then, by the definition of complement, we have $\neg(x \in A \cup B)$. The latter says, by definition, that $\neg(x \in A \vee x \in B)$.

…

Thus, $x \in A^C$ and $x \in B^C$, so we we have $x \in A^C \cap B^C$ by the definition of intersection.

De Morgan's Laws

Prove that $(A \cup B)^C = A^C \cap B^C$

Formally, prove $\forall x\ (x \in (A \cup B)^C \leftrightarrow x \in A^C \cap B^C)$

Proof: Let x be an arbitrary object.

Suppose $x \in (A \cup B)^C$. Then, by the definition of complement, we have $\neg(x \in A \cup B)$. The latter says, by definition, that $\neg(x \in A \vee x \in B)$.

…

Thus, $\neg(x \in A)$ and $\neg(x \in B)$, so $x \in A^C$ and $x \in B^C$ by the definition of compliment, and we can see that $x \in A^C \cap B^C$ by the definition of intersection.

De Morgan's Laws

Prove that $(A \cup B)^C = A^C \cap B^C$

Formally, prove $\forall \mathrm{x}\ (x \in (A \cup B)^C \leftrightarrow x \in A^C \cap B^C)$

Proof: Let x be an arbitrary object.

Suppose $x \in (A \cup B)^C$. Then, by definition of complement, we have $\neg(x \in A \cup B)$. The latter says, by definition, that $\neg(x \in A \vee x \in B)$, or equivalently $\neg(x \in A) \wedge \neg(x \in B)$ by De Morgan's law. Thus, we have $x \in A^C$ and $x \in B^C$ by the definition of compliment, and we can see that $x \in A^C \cap B^C$ by the definition of intersection.

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

De Morgan's Laws

Prove that $(A \cup B)^C = A^C \cap B^C$

Formally, prove $\forall$x $(x \in (A \cup B)^C \leftrightarrow x \in A^C \cap B^C)$

Proof: Let x be an arbitrary object.

Suppose $x \in (A \cup B)^C$.... Then, $x \in A^C \cap B^C$.

Suppose $x \in A^C \cap B^C$. Then, by the definition of intersection, we have $x \in A^C$ and $x \in B^C$. That is, we have $\neg(x \in A) \wedge \neg(x \in B)$, which is equivalent to $\neg(x \in A \vee x \in B)$ by De Morgan's law. The last is equivalent to $\neg(x \in A \cup B)$, by the definition of union, so we have shown $x \in (A \cup B)^C$, by the definition of complement.

De Morgan's Laws

Prove that $(A \cup B)^C = A^C \cap B^C$

Formally, prove $\forall x\, (x \in (A \cup B)^C \leftrightarrow x \in A^C \cap B^C)$

Proof: Let x be an arbitrary object.

The stated biconditional holds since:

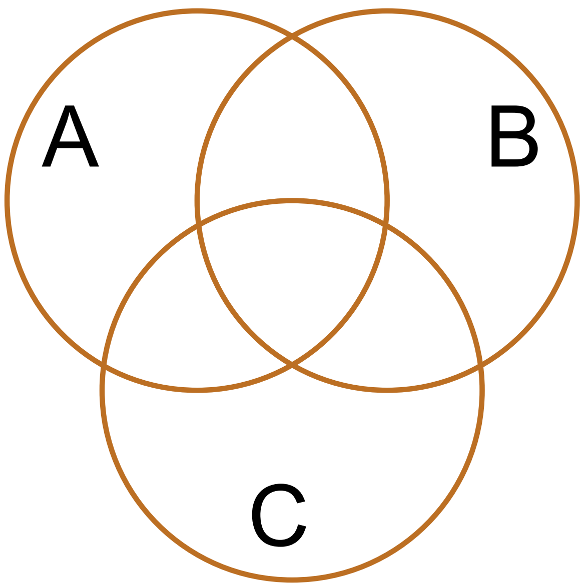
$x \in (A \cup B)^C$	$\equiv \neg(x \in A \cup B)$	Def of -^{C}
	$\equiv \neg(x \in A \lor x \in B)$	Def of ∪
	$\equiv \neg(x \in A) \land \neg(x \in B)$	De Morgan
	$\equiv x \in A^C \land x \in B^C$	Def of -^{C}
	$\equiv x \in A^C \cap B^C$	Def of ∩

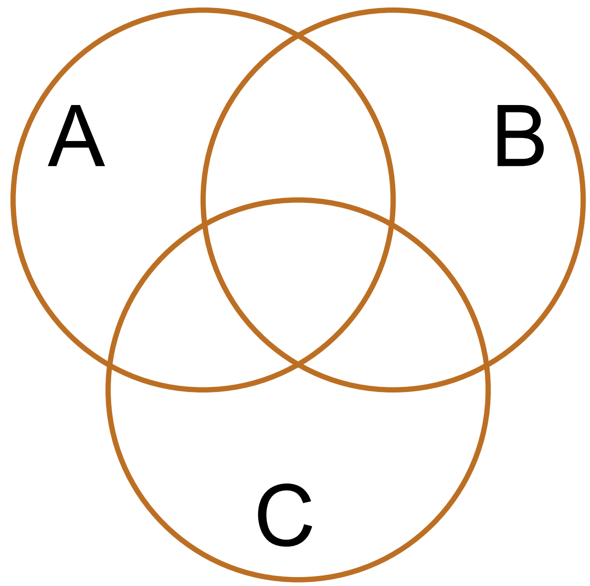
Chains of equivalences are often easier to read like this rather than as English text

itrary, we have shown the sets are equal. ■

Distributive Laws

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





It's Propositional Logic Again!

Meta-Theorem: Translate any Propositional Logic equivalence into "=" relationship between sets by replacing ∪ with ∨, ∩ with ∧, and $\cdot^C$ with ¬.

"Proof": Let x be an arbitrary object.

The stated bi-condition holds since:

x ∈ left side ≡ replace set ops with propositional logic

≡ apply Propositional Logic equivalence

≡ replace propositional logic with set ops

≡ x ∈ right side

Since x was arbitrary, we have shown the sets are equal. ■

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

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

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

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**

$\mathcal{P}$(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)}.

Cartesian Product

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

$\mathbb{R} \times \mathbb{R}$ 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)}.

What is $A \times \emptyset$?

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)}.

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

Russell's Paradox

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

Suppose that $S \in S$**...**

Russell's Paradox

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

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

Suppose that $S \notin S$. Then, by the definition of 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

Number Theory (and applications to computing)

- Branch of Mathematics with direct relevance to computing

- Many significant applications
  - Cryptography
  - Hashing
  - Security

- Important toolkit

Modular Arithmetic

- Arithmetic over a finite domain
- Almost all computation is 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: "b divides a"

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

$$b \mid a \leftrightarrow \exists q \in \mathbb{Z}\ (a = qb)$$

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: "b divides a"

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

$$b \mid a \leftrightarrow \exists q \in \mathbb{Z} \ (a = qb)$$

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

Recall: Elementary School Division

For $a, b \in \mathbb{Z}$ with $b > 0$, we can divide b into a.

If $b \mid a$, then, by definition, we have $a = qb$ for some $q \in \mathbb{Z}$. The number q is called the quotient.

Dividing both sides by a, we can write this as

$$\frac{a}{b} = d$$

(We want to stick to integers, though, so we'll write $a = qb$.)

Recall: Elementary School Division

For $a, b \in \mathbb{Z}$ with $b > 0$, we can divide b into a.

If $b \nmid a$, then we end up with a *remainder* $r \in \mathbb{Z}$ with $0 < r < b$.
Now,

instead of $\frac{a}{b} = q$ we have $\frac{a}{b} = q + \frac{r}{b}$

Multiplying both sides by a gives us $a = qb + r$
(A bit nicer since it has no fractions.)

Recall: Elementary School Division

For $a, b \in \mathbb{Z}$ with $b > 0$, we can divide b into a.

If $b \mid a$, then we have $a = qb$ for some $q \in \mathbb{Z}$.
If $b \nmid a$, then we have $a = qb + r$ for some $q, r \in \mathbb{Z}$ with $0 < \mathrm{r} < \mathrm{b}$.

In general, we have $a = qb + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < b$, where $r = 0$ iff $b \mid a$.

Division Theorem

Division Theorem

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

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

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

Division Theorem

Division Theorem

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

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

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

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

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

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