# Discrete Mathematics

Chih-Wei Yi

Dept. of Computer Science
National Chiao Tung University

March 16, 2009

# §2.1 Sets

# Basic Notations for Sets

- For sets, we'll use variables $S, T, U, \cdots$.
- We can denote a set $S$ in writing by listing all of its elements in curly braces:
  - $\{a, b, c\}$ is the set of whatever 3 objects are denoted by $a$, $b$, $c$.
- *Set builder notation*: For any proposition $P(x)$ over any universe of discourse, $\{x \mid P(x)\}$ is *the set of all $x$ such that* $P(x)$.
  - $Q = \{p/q \mid p, q \in \mathbb{Z}, and q \neq 0\}$.

# Basic Properties of Sets

- Sets are inherently *unordered*:
  - No matter what objects $a$, $b$, and $c$ denote, $\{a, b, c\} = \{a, c, b\} = \{b, a, c\} = \{b, c, a\} = \{c, a, b\} = \{c, b, a\}$.
- All elements are *distinct* (unequal); multiple listings make no difference!
  - $\{a, a, b\} = \{a, b, b\} = \{a, b\} = \{a, a, a, a, b, b, b\}$.
  - This set contains at most 2 elements!

# Definition of Set Equality

- Two sets are declared to be equal *if and only if* they contain exactly the same elements.
- In particular, it does not matter *how the set is defined or denoted*.

**Example**

$$\{1, 2, 3, 4\}$$
$$= \{x \mid x \text{ is an integer where } x > 0 \text{ and } x < 5\}$$
$$= \{x \mid x \text{ is a positive integer whose square is} > 0 \text{ and } < 25\}.$$

# Infinite Sets

- Conceptually, sets may be *infinite* (i.e., not *finite*, without end, unending). Symbols for some special infinite sets:
  - $\mathbb{N} = \{0, 1, 2, \ldots\}$ The $\mathbb{N}$atural numbers.
- Infinite sets come in different sizes!

# Infinite Sets

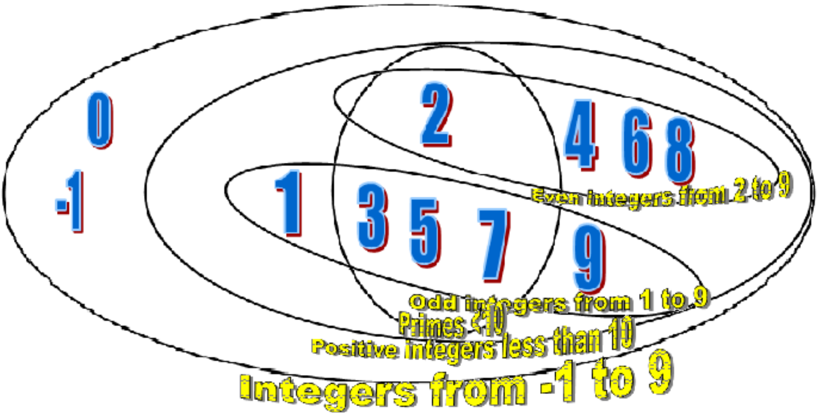
- Conceptually, sets may be *infinite* (i.e., not *finite*, without end, unending). Symbols for some special infinite sets:
  - $\mathbb{N} = \{0, 1, 2, \ldots\}$ The $\mathbb{N}$atural numbers.
  - $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ The $\mathbb{Z}$ntegers.

- Infinite sets come in different sizes!

# Infinite Sets

- Conceptually, sets may be *infinite* (i.e., not *finite*, without end, unending). Symbols for some special infinite sets:
  - $\mathbb{N} = \{0, 1, 2, \ldots\}$ The $\mathbb{N}$atural numbers.
  - $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ The $\mathbb{Z}$ntegers.
  - $\mathbb{R}$ =The "$\mathbb{R}$eal" numbers, such as 374.1828471929498181917281943125….
- Infinite sets come in different sizes!

# Venn Diagrams



# Basic Set Relations: Member of

## Definition

$x \in S$ ("$x$ is in $S$") is the proposition that object $x$ is an $\in$lement or member of set $S$.

- E.g.,
  - $3 \in \mathbb{N}$.
  - $a \in \{x \mid x \text{ is a letter of the alphabet}\}$.
- Can define set equality in terms of $\in$ relation:

$$\forall S, T : S = T \leftrightarrow (\forall x : x \in S \leftrightarrow x \in T).$$

"Two sets are equal iff they have all the same members."

- $x \notin S :\equiv \neg(x \in S)$ "$x$ is not in $S$"!!!

# The Empty Set

## Definition

$\varnothing$ ("null", "the empty set") is the unique set that contains no elements whatsoever.

- $\varnothing = \{\} = \{x \mid \textbf{False}\}$
- No matter the domain of discourse, we have the axiom $\neg\exists x :\equiv x \in \varnothing$.

# Subset and Superset Relations

## Definition

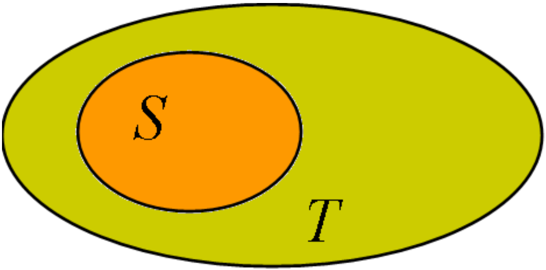
$S \subseteq T$ ("$S$ is a subset of $T$") means that every element of $S$ is also an element of $T$.

- $S \subseteq T \iff \forall x\,(x \in S \rightarrow x \in T)$.
- $\varnothing \subseteq S$, $S \subseteq S$.
- $S \supseteq T$ ("$S$ is a superset of $T$") means $T \subseteq S$.
- Proof skills
  - $S = T \Leftrightarrow S \subseteq T \wedge S \supseteq T$.
  - $S \nsubseteq T$ means $\neg(S \subseteq T)$, i.e $\exists x\,(x \in S \wedge x \notin T)$.

# Proper (Strict) Subsets & Supersets

## Definition

$S \subset T$ ("$S$ is a proper subset of $T$") means that $S \subseteq T$ but $T \not\subseteq S$. Similar for $S \supset T$.




Example:
$\{1,2\} \subset \{1,2,3\}$

Venn Diagram equivalent of $S \subset T$

# Sets Are Objects, Too!

- The objects that are elements of a set may themselves be sets.
- E.g, let $S = \{x \mid x \subseteq \{1, 2, 3\}\}$ then

$$S = \{\phi, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

  We denote $S$ by $2^{\{1,2,3\}}$.
- Note that $1 \neq \{1\} \neq \{\{1\}\}$

# Cardinality and Finiteness

## Definition

$|S|$ (read "the cardinality of $S$") is a measure of how many different elements $S$ has.

- E.g.,
  - $|\varnothing| = 0$
  - $|\{1, 2, 3\}| = 3$
  - $|\{a, b\}| = 2$
  - $|\{\{1, 2, 3\}, \{4, 5\}\}| = 2$
- If $|S| \in \mathbb{N}$, then we say $S$ is *finite*. Otherwise, we say $S$ is *infinite*.
- What are some infinite sets we've seen?

$$\mathbb{N},\ \mathbb{Z},\ \mathbb{R},\ \ldots$$

# The Power Set Operation

## Definition

The power set $P(S)$ of a set S is the set of all subsets of $S$.
$P(S) = \{x \mid x \subseteq S\}$.

- E.g., $P(\{a, b\}) = \{\phi, \{a\}, \{b\}, \{a, b\}\}$.
- Sometimes $P(S)$ is written $2^S$. Note that for finite $S$, $|P(S)| = 2^{|S|}$.
- It turns out that $|P(\mathbb{N})| > |\mathbb{N}|$. There are different sizes of infinite sets!

# Review: Set Notations So Far

- Variable objects $x, y, z$; sets $S$, $T$, $U$.
- Literal set$\{a, b, c\}$ and set-builder$\{x \mid P(x)\}$.
- relational operator, and the empty set $\varnothing$.
- Set relations $=$, $\subseteq$, $\supseteq$, $\subset$, $\supset$, etc.
- Venn diagrams.
- Cardinality $|S|$ and infinite sets $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.
- Power sets $P(S)$.

# Naive Set Theory is Inconsistent

- There are some naive set *descriptions* that lead pathologically to structures that are not *well-defined*. (That do not have consistent properties.)
- These "sets" mathematically *cannot* exist.
- Let $S = \{x \mid x \notin x\}$. Is $S \in S$?
- Therefore, consistent set theories must restrict the language that can be used to describe sets.
- For purposes of this class, don't worry about it!

# Ordered n-Tuples

- These are like sets, except that duplicates matter, and the order makes a difference.
- For $n \in \mathbb{N}$, an *ordered n-tuple* or a *sequence of length n* is written $(a_1, a_2, \cdots, a_n)$. The *first* element is $a_1$, etc.
- Note $(1,2) \neq (2,1) \neq (2,1,1)$.
- Empty sequence, singlets, pairs, triples, quadruples, quintuples, ..., $n$-tuples.

# Cartesian Products of Sets

## Definition

For sets $A, B$, their Cartesian product
$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$.

- E.g., $\{a, b\} \times \{1, 2\} = \{(a, 1), (a, 2), (b, 1), (b, 2)\}$.
- For finite sets $A, B$, $|A \times B| = |A|\,|B|$.
- The Cartesian product is not commutative, i.e.

$$\neg\forall AB : A \times B = B \times A.$$

- Extends to $A_1 \times A_2 \times \cdots \times A_n$.

# Review of §2.1

- Sets $S$, $T$, $U$, $\cdots$. Special sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$.
- Set notations $\{a, b, ...\}$, $\{x \mid P(x)\}$, $\cdots$.
- Set relation operators $x \in S$, $S \subseteq T$, $S \supseteq T$, $S = T$, $S \subset T$, $S \supset T$. (These form propositions.)
- Finite vs. infinite sets.
- Set operations $|S|$, $P(S)$, $S \times T$.
- Next up: §2.2: More set ops: $\cup$, $\cap$, $-$, $\cdots$.

# §2.2 Set Operations

# The Union Operator

**Definition**

For sets $A$, $B$, their Union $A \cup B$ is the set containing all elements that are either in $A$, **or** ("$\vee$") in $B$ (or, of course, in both).

- Formally, $\forall A, B : A \cup B = \{x \mid x \in A \vee x \in B\}$.
- Note that $A \cup B$ contains all the elements of $A$ **and** it contains all the elements of $B$:

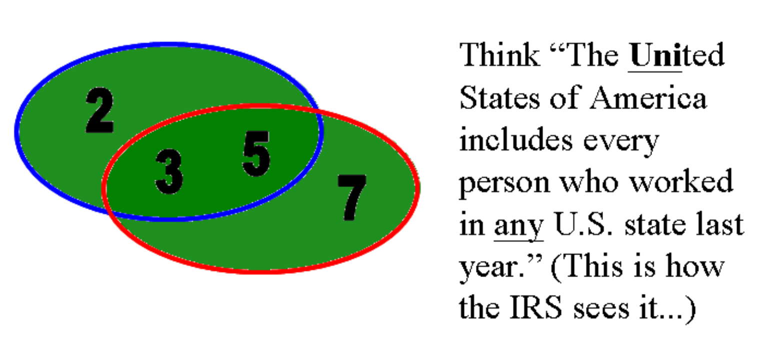
$$\forall A, B : (A \cup B \supseteq A) \wedge (A \cup B \supseteq B).$$

## Example

$\{a, b, c\} \cup \{2, 3\} = \{a, b, c, 2, 3\}$.

## Example

$\{2, 3, 5\} \cup \{3, 5, 7\} = \{2, 3, 5, 3, 5, 7\} = \{2, 3, 5, 7\}$



# The Intersection Operator

## Definition

For sets $A$, $B$, their intersection $A \cap B$ is the set containing all elements that are simultaneously in $A$ **and** ("$\wedge$") in $B$.

- Formally, $\forall A, B : A \cap B = \{x \mid x \in A \wedge x \in B\}$.
- Note that $A \cap B$ is a subset of $A$ **and** it is a subset of $B$:

$$\forall A, B : (A \cap B \subseteq A) \wedge (A \cap B \subseteq B).$$

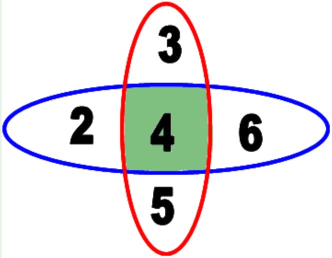
# Intersection Examples

## Examples

$\{a, b, c\} \cap \{2, 3\} = \varnothing.$

## Examples

$\{2, 4, 6\} \cap \{3, 4, 5\} = \{4\}.$




Think "The **intersection** of University Ave. and W 13th St. is just that part of the road surface that lies on *both* streets."

# Disjointedness

## Definition

Two sets $A, B$ are called disjoint (i.e., unjoined) iff their intersection is empty. (i.e., $A \cap B = \varnothing$.)

## Example

the set of even integers is disjoint with the set of odd integers

# Inclusion-Exclusion Principle

- How many elements are in $A \cup B$?

$$|A \cup B| = |A| + |B| - |A \cap B| .$$

## Example

How many students are on our class email list? Consider set $E = I \cup M$, where $I = \{s \mid s \text{ turned in an information sheet}\}$ and $M = \{s \mid s \text{ sent the TAs their email address}\}$. Some students did both! So,

$$|E| = |I \cup M| = |I| + |M| - |I \cap M| .$$

# Set Difference

## Definition

For sets $A$, $B$, the difference of $A$ and $B$, written $A - B$, is the set of all elements that are in $A$ but not $B$.

$$A - B :\equiv \{x \mid x \in A \wedge x \notin B\} = \{x \mid \neg(x \in A \longrightarrow x \in B)\}.$$

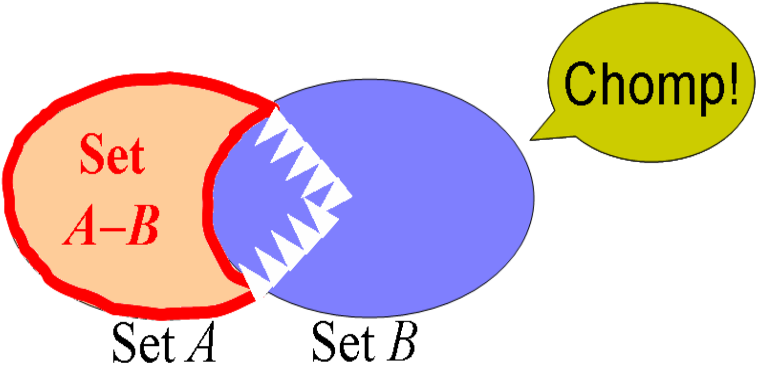
Also called: The complement of $B$ with respect to $A$.

- E.g., $\{1, 2, 3, 4, 5, 6\} - \{2, 3, 5, 7, 9, 11\} = \{1, 4, 6\}$, and

$$\begin{aligned} \mathbb{Z} - \mathbb{N} &= \{\ldots, -1, 0, 1, 2, \ldots\} - \{0, 1, \ldots\} \\ &= \{x \mid x \text{ is an integer but not a nat. } \#\} \\ &= \{x \mid x \text{ is a negative integer}\} \\ &= \{\ldots, -3, -2, -1\}. \end{aligned}$$

# Set Difference - Venn Diagram

- $A - B$ is what's left after $B$ "takes a bite out of $A$".



# Set Complements

## Definition

The universe of discourse can itself be considered a set, call it $U$. When the context clearly defines $U$, we say that for any set $A \subseteq U$, the complement of $A$, written $\overline{A}$, is the complement of $A$ w.r.t. $U$, i.e., it is $U - A$.

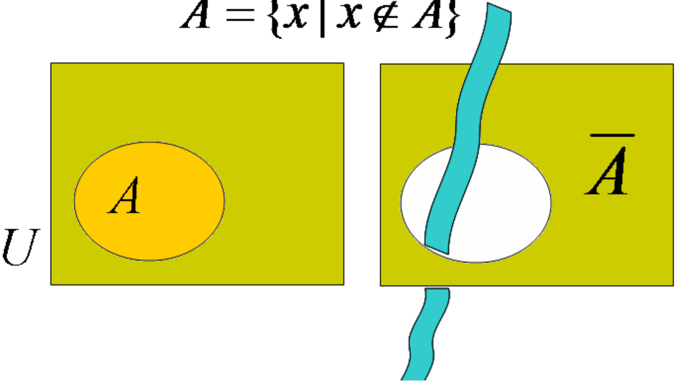
## Example

If $U = \mathbb{N}, \overline{\{3, 5\}} = \{0, 1, 2, 4, 6, 7.....\}$.

# More on Set Complements

- An equivalent definition, when $U$ is clear:

$$\overline{A} = \{x \mid x \notin A\}$$



# Set Identities

**Theorem**

| | |
|---|---|
| *Identity* | $A \cup \varnothing = A$; $A \cap U = A$. |
| *Domination* | $A \cup U = U$; $A \cap \varnothing = \varnothing$. |
| *Idempotent* | $A \cup A = A$; $A \cap A = A$. |
| *Double complement* | $\overline{\overline{A}} = A$. |
| *Commutative* | $A \cap B = B \cap A$; $A \cup B = B \cup A$. |
| *Associative* | $A \cup (B \cup C) = (A \cup B) \cup C$; $A \cap (B \cap C) = (A \cap B) \cap C$. |

# DeMorgan's Law for Sets

## Theorem

*Exactly analogous to (and derivable from) DeMorgan's Law for propositions.*

$$\begin{aligned} \overline{A \cup B} &= \overline{A} \cap \overline{B}, \\ \overline{A \cap B} &= \overline{A} \cup \overline{B}. \end{aligned}$$

# Proving Set Identities

To prove statements about sets, of the form $E_1 = E_2$ (where E's are set expressions), here are three useful techniques:

- Prove $E_1 \subseteq E_2$ and $E_2 \subseteq E_1$ separately.
- Use set builder notation & logical equivalences.
- Use a membership table.

# Method 1: Mutual Subsets

## Example

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

## Solution

*First, show* $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

- *Assume* $x \in A \cap (B \cup C)$, *& show* $x \in (A \cap B) \cup (A \cap C)$.
- *We know that* $x \in A$, *and either* $x \in B$ *or* $x \in C$.
  - *Case 1:* $x \in B$. *Then* $x \in A \cap B$, *so* $x \in (A \cap B) \cup (A \cap C)$.
  - *Case 2:* $x \in C$. *Then* $x \in A \cap C$, *so* $x \in (A \cap B) \cup (A \cap C)$.
- *Therefore,* $x \in (A \cap B) \cup (A \cap C)$.
- *Therefore,* $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

*Nest, show* $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. ...

# Method 3: Membership Tables

- Just like truth tables for propositional logic.
- Columns for different set expressions.
- Rows for all combinations of memberships in constituent sets.
- Use "1" to indicate membership in the derived set, "0" for non-membership.
- Prove equivalence with identical columns.

# Membership Table

## Example

Prove $(A \cup B) - B = A - B$.

## Solution

| $A$ | $B$ | $A \cup B$ | $(A \cup B) - B$ | $A - B$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 | 0 |
| 1 | 0 | 1 | 1 | 1 |
| 1 | 1 | 1 | 0 | 0 |

# Membership Table Exercise

## Example

Prove $(A \cup B) - C = (A - C) \cup (B - C)$.

| $A$ | $B$ | $C$ | $A \cup B$ | $(A \cup B) - C$ | $A - C$ | $B - C$ | $(A - C) \cup (B - C)$ |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | | | | | |
| 0 | 0 | 1 | | | | | |
| 0 | 1 | 0 | | | | | |
| 0 | 1 | 1 | | | | | |
| 1 | 0 | 0 | | | | | |
| 1 | 0 | 1 | | | | | |
| 1 | 1 | 0 | | | | | |
| 1 | 1 | 1 | | | | | |

# Review of §2.1-§2.1

- Sets $S$, $T$, $U$, ... Special sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$.
- Set notations $\{a, b, ...\}$, $\{x \mid P(x)\}\ldots$
- Relations $x \in S$, $S \subseteq T$, $S \supseteq T$, $S = T$, $S \subset T$, $S \supset T$.
- Operations $|S|$, $P(S)$, $\times$, $\cup$, $\cap$, $-$, $\ldots$
- Set equality proof techniques:
  - Mutual subsets.
  - Derivation using logical equivalences.

# Generalized Unions & Intersections

Since union & intersection are commutative and associative, we can extend them from operating on ordered pairs of sets $(A, B)$ to operating on sequences of sets $(A_1, \ldots, A_n)$, or even unordered sets of sets, $X = \{A \mid P(A)\}$.

# Generalized Union

- Binary union operator: $A \cup B$
- $n$-ary union:
  $A_1 \cup A_2 \cup \cdots \cup A_n :\equiv ((\cdots((A_1 \cup A_2) \cup \cdots) \cup A_n)$
  (grouping & order is irrelevant)
- "Big U" notation: $\bigcup_{i=1}^{n} A_i$.
- Or for infinite sets of sets: $\bigcup_{A \in X} A$.

# Generalized Intersection

- Binary intersection operator: $A \cap B$.
- $n$-ary intersection:
  $A_1 \cap A_2 \cap \cdots \cap A_n :\equiv ((\ldots(A_1 \cap A_2) \cap \ldots) \cap A_n)$ (grouping & order is irrelevant).
- "Big Arch" notation: $\bigcap_{i=1}^{n} A_i$.
- Or for infinite sets of sets: $\bigcap_{A \in X} A$.

# Representing Sets with Bit Strings

- For an enumerable u.d. $U$ with ordering $\{x_1, x_2, \ldots\}$, represent a finite set $S \subseteq U$ as the finite bit string $B = b_1 b_2 \ldots b_n$ where $\forall i : x_i \in S \longleftrightarrow (i < n \wedge b_i = 1)$.
  - E.g., $U = \mathbb{N}$, $S = \{2, 3, 5, 7, 11\}$, $B = 001101010001$.
- In this representation, the set operators "$\cup$", "$\cap$", "$-$" are implemented directly by bitwise OR, AND, NOT!