

University of Florida
Dept. of Computer & Information Science & Engineering
COT 3100
Applications of Discrete Structures
Dr. Michael P. Frank

Slides for a Course Based on the Text
Discrete Mathematics & Its Applications
(5th Edition)
by Kenneth H. Rosen

**Module #3:
The Theory of Sets**

Rosen 5th ed., §§1.6-1.7
~43 slides, ~2 lectures

Introduction to Set Theory (§1.6)

- A *set* is a new type of structure, representing an *unordered* collection (group, plurality) of zero or more *distinct* (different) objects.
- Set theory deals with operations between, relations among, and statements about sets.
- Sets are ubiquitous in computer software systems.
- *All* of mathematics can be defined in terms of some form of set theory (using predicate logic).

Naïve set theory

- Basic premise: Any collection or class of objects (*elements*) that we can describe (by any means whatsoever) constitutes a set.
- But, the resulting theory turns out to be *logically inconsistent!*
 - This means, there exist naïve set theory propositions p such that you can prove that both p and $\neg p$ follow logically from the postulates of the theory!
 - \therefore The conjunction of the postulates is a contradiction!
 - This theory is fundamentally uninteresting, because any possible statement in it can be (very trivially) “proved” by contradiction!
- More sophisticated set theories fix this problem.

Basic notations for sets

- For sets, we'll use variables S, T, U, \dots
- 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, $\{x|P(x)\}$ is *the set of all x such that $P(x)$* .

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!
 - If $a=b$, then $\{a, b, c\} = \{a, c\} = \{b, c\} =$
 $\{a, a, b, a, b, c, c, c, c\}.$
 - This set contains at most 2 elements!

Definition of Set Equality

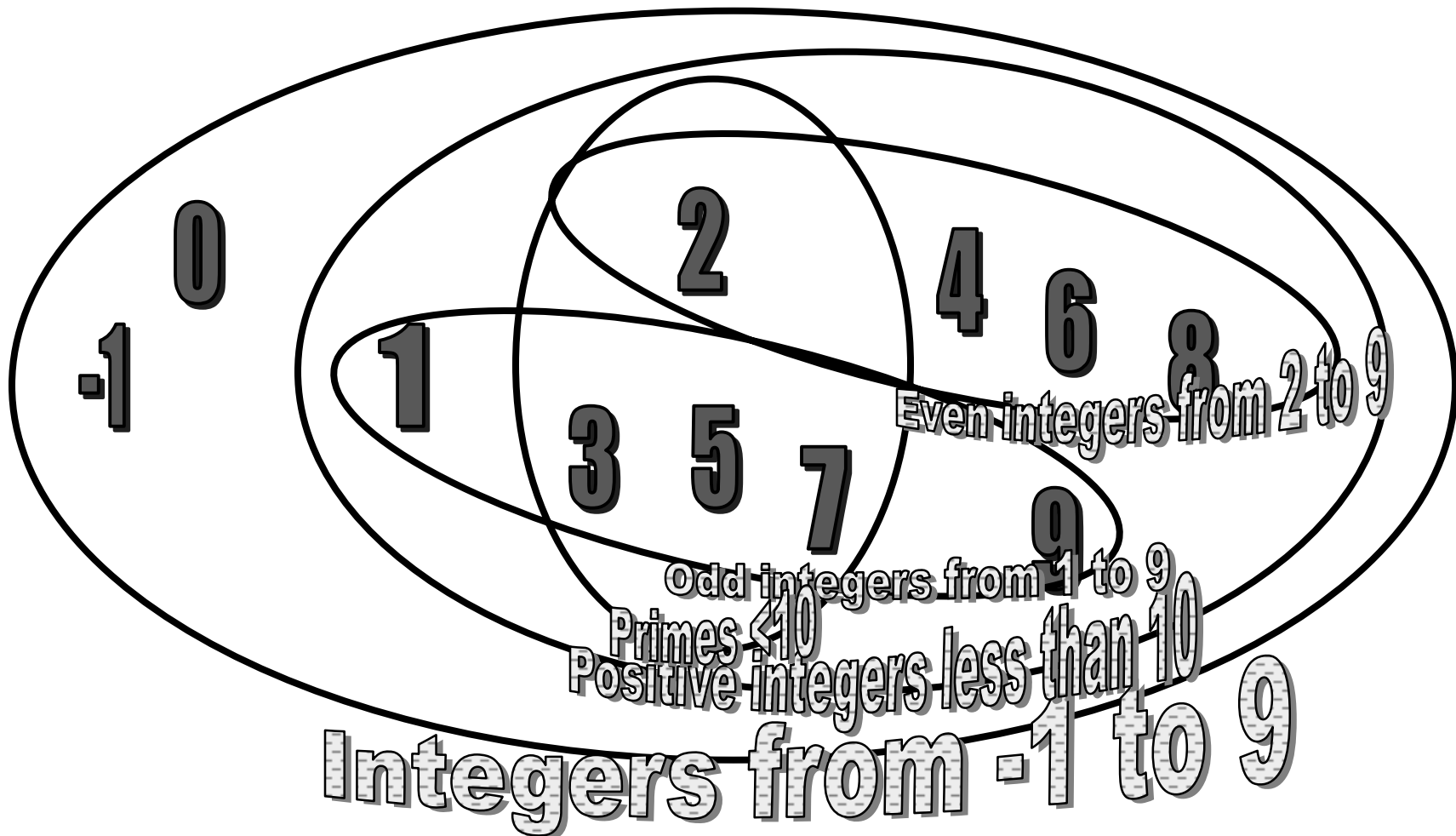
- Two sets are declared to be equal *if and only if* they contain exactly the same elements.
- In particular, it does not matter *how the set is defined or denoted*.
- For example: The set $\{1, 2, 3, 4\} =$
 $\{x \mid x \text{ is an integer where } x > 0 \text{ and } x < 5\} =$
 $\{x \mid x \text{ is a positive integer whose square}$
 $\text{is } > 0 \text{ and } < 25\}$

Infinite Sets

- Conceptually, sets may be *infinite* (i.e., not *finite*, without end, unending).
- Symbols for some special infinite sets:
 $\mathbf{N} = \{0, 1, 2, \dots\}$ The Natural numbers.
 $\mathbf{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ The Zntegers.
 \mathbf{R} = The “**R**real” numbers, such as
374.1828471929498181917281943125...
- Infinite sets come in different sizes!

More on this after module #4 (functions).

Venn Diagrams



Basic Set Relations: Member of

- $x \in S$ (“ x is in S ”) is the proposition that object x is an *element* or *member* of set S .
 - e.g. $3 \in \mathbf{N}$, “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

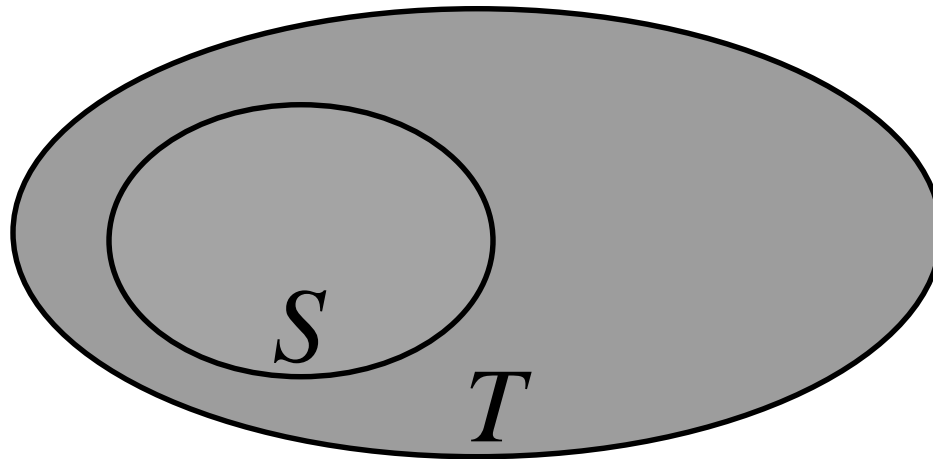
- \emptyset (“null”, “the empty set”) is the unique set that contains no elements whatsoever.
- $\emptyset = \{ \} = \{x/\mathbf{False}\}$
- No matter the domain of discourse, we have the axiom $\neg\exists x: x \in \emptyset$.

Subset and Superset Relations

- $S \subseteq T$ (“ S is a subset of T ”) means that every element of S is also an element of T .
- $S \subseteq T \Leftrightarrow \forall x (x \in S \rightarrow x \in T)$
- $\emptyset \subseteq S, S \subseteq S$.
- $S \supseteq T$ (“ S is a superset of T ”) means $T \subseteq S$.
- Note $S = T \Leftrightarrow S \subseteq T \wedge S \supseteq T$.
- $S \not\subseteq T$ means $\neg(S \subseteq T)$, *i.e.* $\exists x(x \in S \wedge x \notin T)$

Proper (Strict) Subsets & Supersets

- $S \subset T$ (“ 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 $S = \{\emptyset,$
 $\{1\}, \{2\}, \{3\},$
 $\{1,2\}, \{1,3\}, \{2,3\},$
 $\{1,2,3\}\}$
- Note that $1 \neq \{1\} \neq \{\{1\}\} !!!!$

← Very Important!

Cardinality and Finiteness

- $|S|$ (read “the *cardinality* of S ”) is a measure of how many different elements S has.
- *E.g.*, $|\emptyset|=0$, $|\{1,2,3\}|=3$, $|\{a,b\}|=2$,
 $|\{\{1,2,3\},\{4,5\}\}|= \underline{2}$
- If $|S| \in \mathbf{N}$, then we say S is *finite*.
Otherwise, we say S is *infinite*.
- What are some infinite sets we’ve seen?

NZR

The *Power Set* Operation

- 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.* $P(\{a,b\}) = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$.
- Sometimes $P(S)$ is written 2^S .
Note that for finite S , $|P(S)| = 2^{|S|}$.
- It turns out that $|P(\mathbf{N})| > |\mathbf{N}|$.
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 $\{x|P(x)\}$.
- \in relational operator, and the empty set \emptyset .
- Set relations $=, \subseteq, \supseteq, \subset, \supset, \not\subset$, etc.
- Venn diagrams.
- Cardinality $|S|$ and infinite sets **N, Z, R**.
- Power sets $P(S)$.

Naïve Set Theory is Inconsistent

- There are some naïve set *descriptions* that lead pathologically to structures that are not *well-defined*. (That do not have consistent properties.)
- These “sets” mathematically *cannot* exist.
- *E.g.* 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!

Bertrand Russell
1872-1970



Ordered n -tuples

- These are like sets, except that duplicates matter, and the order makes a difference.
- For $n \in \mathbf{N}$, an *ordered n -tuple* or a *sequence of length n* is written (a_1, a_2, \dots, 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

- For sets A, B , their *Cartesian product* $A \times B := \{(a, b) \mid a \in A \wedge b \in B\}$.
- *E.g.* $\{a, b\} \times \{1, 2\} = \{(a, 1), (a, 2), (b, 1), (b, 2)\}$
- Note that for finite A, B , $|A \times B| = |A| |B|$.
- Note that the Cartesian product is *not* commutative: $\neg \forall A, B: A \times B = B \times A$.
- Extends to $A_1 \times A_2 \times \dots \times A_n \dots$



René Descartes
(1596-1650)

Review of §1.6

- Sets $S, T, U \dots$ Special sets $\mathbf{N}, \mathbf{Z}, \mathbf{R}$.
- Set notations $\{a, b, \dots\}, \{x | P(x)\} \dots$
- 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: §1.5: More set ops: $\cup, \cap, -$.

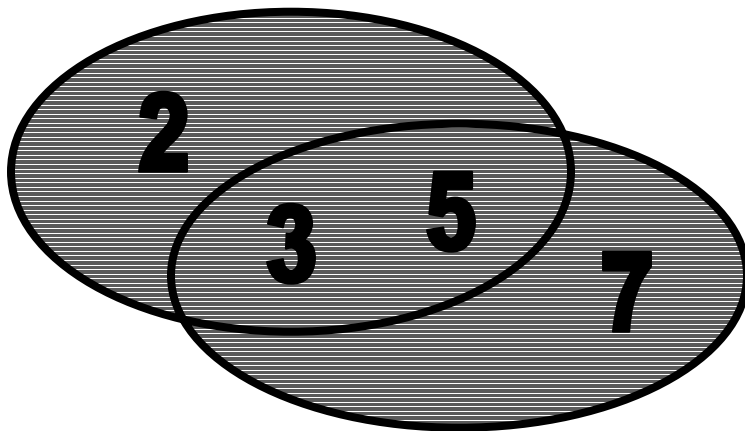
Start §1.7: The Union Operator

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

Union Examples

- $\{a,b,c\} \cup \{2,3\} = \{a,b,c,2,3\}$
- $\{2,3,5\} \cup \{3,5,7\} = \{2,3,5,3,5,7\} \neq \{2,3,5,7\}$

Required Form



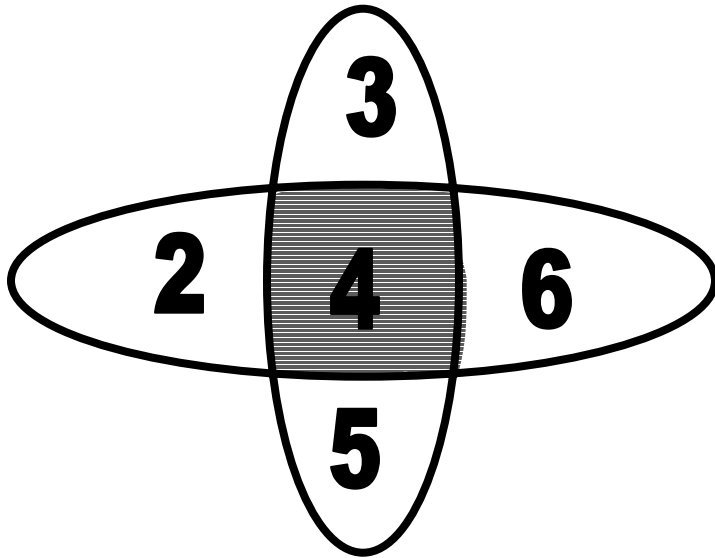
Think “The United States of America includes every person who worked in any U.S. state last year.” (This is how the IRS sees it...)

The Intersection Operator

- 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, $\forall A, B: A \cap B \equiv \{x \mid x \in A \wedge x \in B\}$.
- 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

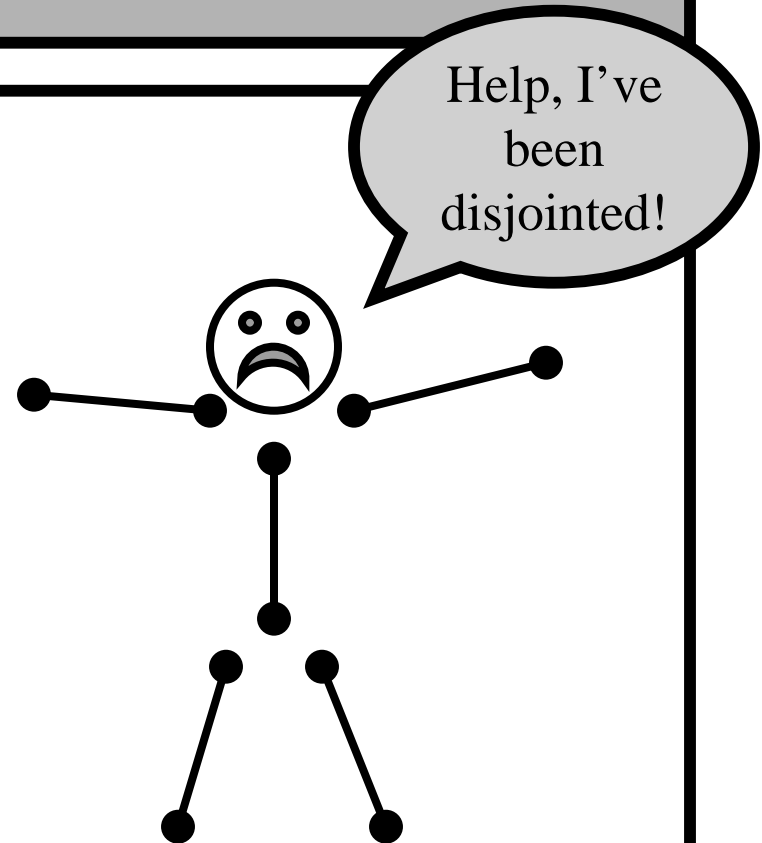
- $\{a,b,c\} \cap \{2,3\} = \underline{\emptyset}$
- $\{2,4,6\} \cap \{3,4,5\} = \underline{\{4\}}$



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

Disjointedness

- Two sets A, B are called *disjoint* (i.e., unjoined) iff their intersection is empty. ($A \cap B = \emptyset$)
- Example: the set of even integers is disjoint with the set of odd integers.



Inclusion-Exclusion Principle

- How many elements are in $I \cup M$?

Subtract out items

- Example: How many students are in the class?

Consider set $E = I \cup M$,
 $I = \{s \mid s \text{ turned in an assignment}\}$

$M = \{s \mid s \text{ has the required credit}\}$

compensate for

- Some students

double-counting them!

$$|I| + |M| - |I \cap M|$$

Set Difference

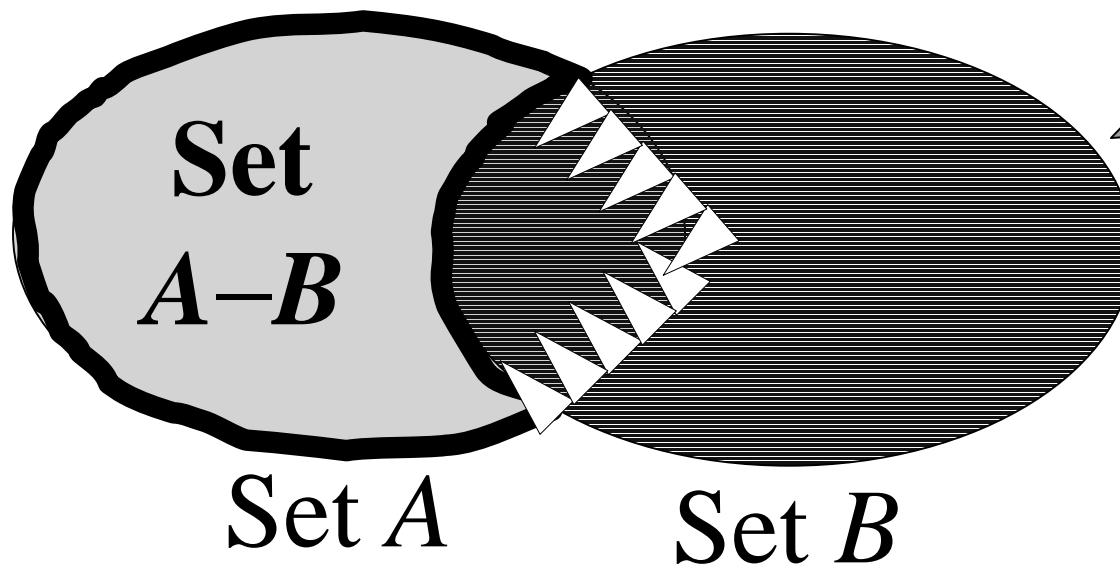
- For sets A , B , the *difference of A and B* , written $A - B$, is the set of all elements that are in A but not B .
- $$A - B := \{x \mid x \in A \wedge x \notin B\}$$
$$= \{x \mid \neg(x \in A \rightarrow x \in B)\}$$
- Also called:
The complement of B with respect to A .

Set Difference Examples

- $\{\cancel{1}, \cancel{2}, \cancel{3}, \cancel{4}, \cancel{5}, \cancel{6}\} - \{2, 3, 5, 7, 9, 11\} =$
 $\underline{\{1, 4, 6\}}$
- $\mathbf{Z} - \mathbf{N} = \{\dots, -1, 0, 1, 2, \dots\} - \{0, 1, \dots\}$
 $= \{x \mid x \text{ is an integer but not a nat. \#}\}$
 $= \{x \mid x \text{ is a negative integer}\}$
 $= \{\dots, -3, -2, -1\}$

Set Difference - Venn Diagram

- $A-B$ is what's left after B
“takes a bite out of A ”



Chomp!

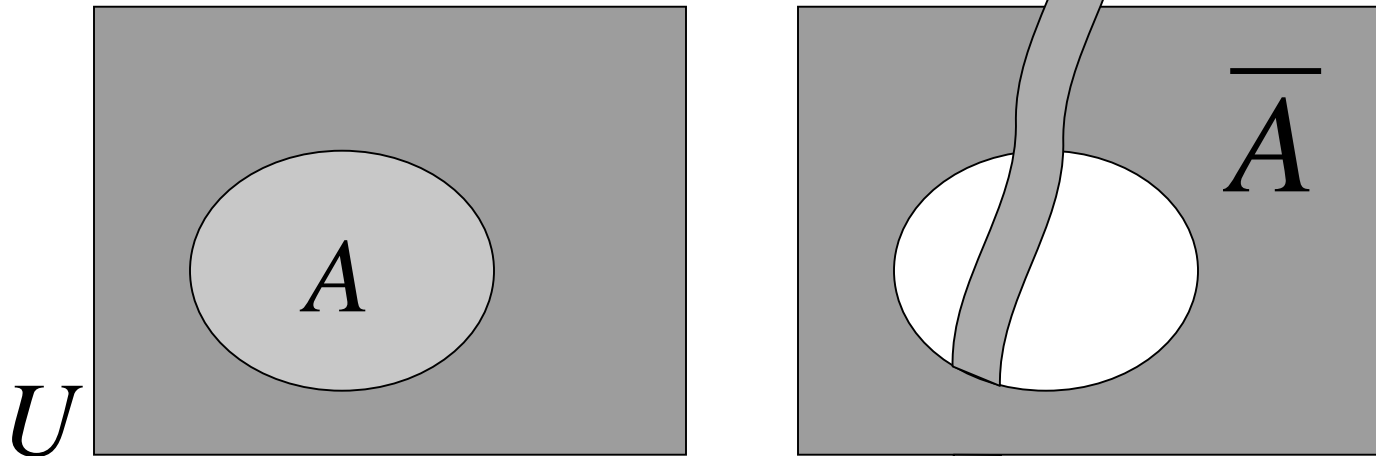
Set Complements

- 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 $U - A$.
- *E.g.*, If $U = \mathbf{N}$, $\overline{\{3,5\}} = \{0,1,2,4,6,7,\dots\}$

More on Set Complements

- An equivalent definition, when U is clear:

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



Set Identities

- Identity: $A \cup \emptyset = A$ $A \cap U = A$
- Domination: $A \cup U = U$ $A \cap \emptyset = \emptyset$
- Idempotent: $A \cup A = A = A \cap A$
- Double complement: $\overline{\overline{A}} = A$
- Commutative: $A \cup B = B \cup A$ $A \cap B = B \cap A$
- 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

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

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

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

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

- 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, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.
- 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 $(A \cup B) - B = A - B$.

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

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 §1.6-1.7

- Sets $S, T, U \dots$ Special sets $\mathbf{N}, \mathbf{Z}, \mathbf{R}$.
- Set notations $\{a, b, \dots\}, \{x | P(x)\} \dots$
- Relations $x \in S, S \subseteq T, S \supseteq T, S = T, S \subset T, S \supset T$.
- Operations $|S|, P(S), \times, \cup, \cap, -, \bar{S}$
- 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, \dots, A_n) , or even unordered *sets* of sets, $X = \{A / P(A)\}$.

Generalized Union

- Binary union operator: $A \cup B$

- n -ary union:

$$A \cup A_2 \cup \dots \cup A_n \equiv ((\dots((A_1 \cup A_2) \cup \dots) \cup A_n)$$

(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:

$$A \cap A_2 \cap \dots \cap A_n \equiv ((\dots((A_1 \cap A_2) \cap \dots) \cap A_n)$$

(grouping & order is irrelevant)

- “Big Arch” notation: $\bigcap_{i=1}^n A_i$

- Or for infinite sets of sets: $\bigcap_{A \in X} A$

Representations

- A frequent theme of this course will be methods of *representing* one discrete structure using another discrete structure of a different type.
- *E.g.*, one can represent natural numbers as
 - Sets: $\mathbf{0}:\equiv\emptyset$, $\mathbf{1}:\equiv\{\mathbf{0}\}$, $\mathbf{2}:\equiv\{\mathbf{0},\mathbf{1}\}$, $\mathbf{3}:\equiv\{\mathbf{0},\mathbf{1},\mathbf{2}\}$, ...
 - Bit strings:
 $\mathbf{0}:\equiv 0$, $\mathbf{1}:\equiv 1$, $\mathbf{2}:\equiv 10$, $\mathbf{3}:\equiv 11$, $\mathbf{4}:\equiv 100$, ...

Representing Sets with Bit Strings

For an enumerable u.d. U with ordering $\{x_1, x_2, \dots\}$, represent a finite set $S \subseteq U$ as the finite bit string $B = b_1 b_2 \dots b_n$ where $\forall i: x_i \in S \leftrightarrow (i < n \wedge b_i = 1)$.

E.g. $U = \mathbf{N}$, $S = \{2, 3, 5, 7, 11\}$, $B = 001101010001$.

In this representation, the set operators “ \cup ”, “ \cap ”, “ $\bar{}$ ” are implemented directly by bitwise OR, AND, NOT!