American University of Beirut
Dept. of Computer Science

CMPS/Math 211

Discrete Structures

Module #3:
The Theory of Sets

Introduction to Set Theory

- A *set* is a 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.

Naïve set theory

- **Basic premise:** Any collection or class of objects (*elements*) that we can *describe* (by any means whatsoever) constitutes a set.

Basic notations for sets

- For sets, we'll use variables S, T, U, …
- 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!

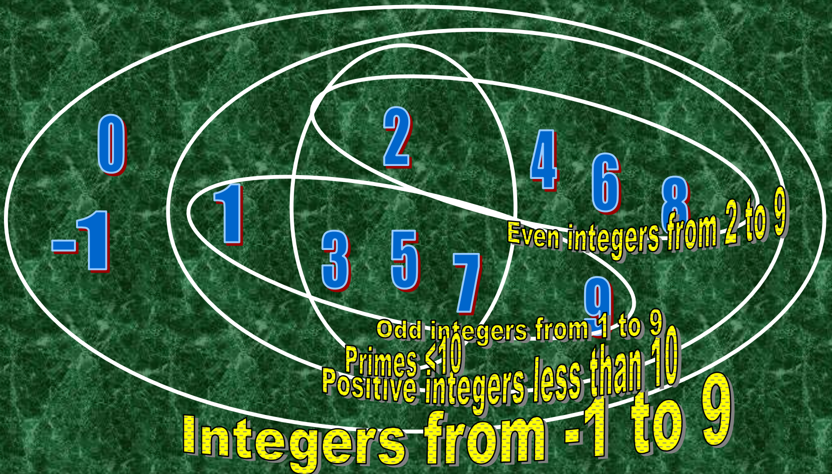
Definition of Set Equality

- 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} =
  $\{x \mid x$ is an integer where $x>0$ and $x<5\}$ =
  $\{x \mid x$ is a positive integer whose square is >0 and $<25\}$

Infinite Sets

- Conceptually, sets may be *infinite* (*i.e.,* not *finite*, without end, unending).
- Symbols for some special infinite sets:
  N = {0, 1, 2, …} The **N**atural numbers.
  Z = {…, -2, -1, 0, 1, 2, …} The **Z**ntegers.
  R = The "**R**eal" numbers, such as 374.1828471929498181917281943125…
- "Blackboard Bold" or double-struck font ($\mathbb{N}$,$\mathbb{Z}$,$\mathbb{R}$) is also often used for these special number sets.

Venn Diagrams



Basic Set Relations: Member of

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

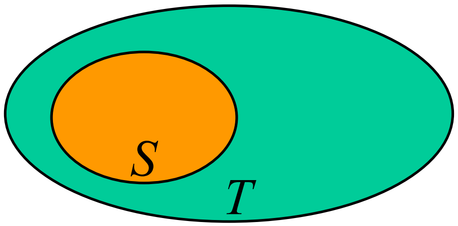
- $\varnothing$ ("null", "the empty set") is the unique set that contains no elements whatsoever.
- $\varnothing = \{\} = \{x \mid \mathbf{False}\}$
- No matter the domain of discourse, we have the axiom $\neg\exists x$: $x \in \varnothing$.

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.
- $S \subseteq T \Leftrightarrow \forall x\, (x \in S \rightarrow x \in T)$
- $\varnothing \subseteq S$, $S \subseteq S$.
- $S \supseteq T$ ("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 $T \not\subseteq S$. Similarly for $S \supset T$.



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

Venn Diagram equivalent of $S \subset T$

Exercise

- Show that $\varnothing \subseteq S$.

Proof: Let S be a set. To show that $\varnothing \subseteq S$, we must show that $\forall x\,(x \in \varnothing \rightarrow x \in S)$ is true. Because the empty set contains no elements, it follows that $x \in \varnothing$ is always false. It follows that the conditional statement $x \in \varnothing \rightarrow x \in S$ *is always true, because its hypothesis is always false and a conditional statement with a false hypothesis is true. That is, $\forall x\,(x \in \varnothing \rightarrow x \in S)$ is true. This complete the proof (a vacuous one).*

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 $S=\{\varnothing,$
  $\{1\}, \{2\}, \{3\},$
  $\{1,2\}, \{1,3\}, \{2,3\},$
  $\{1,2,3\}\}$
- Note that $1 \neq \{1\} \neq \{\{1\}\}$!!!!

Cardinality and Finiteness

- $|S|$ (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 $|S| \in \mathbf{N}$, then we say S is *finite*. Otherwise, we say S is *infinite*.

The *Power Set* Operation

- The *power set* P(S) of a set S is the set of all subsets of S. $P(S) :\equiv \{x \mid x \subseteq S\}$.
- *E.g.* $P(\{a,b\}) = \{\varnothing, \{a\}, \{b\}, \{a,b\}\}$.
- Sometimes P(S) is written $\mathbf{2}^S$. Note that for finite S, $|P(S)| = 2^{|S|}$.
- It turns out $\forall S{:}|P(S)|>|S|$, *e.g.* $|P(\mathbf{N})| > |\mathbf{N}|$. *There are different sizes of infinite sets*!

Exercise

- What is the power set of the empty set? What is the power set of the set $\{\varnothing\}$?

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* or *list of length n* is written $(a_1, a_2, \ldots, a_n)$. Its *first* element is a_1, *etc.*
- Note that $(1, 2) \neq (2, 1) \neq (2, 1, 1)$.
- Empty sequence, singles, pairs, triples, quadruples, quintuples, …, n-tuples.

Contrast with sets' {}

Cartesian Products of Sets

- For sets A, B, their *Cartesian product* $A \times B :\equiv \{(a, b) \mid a \in A \land b \in B\}$.
- *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: *i.e.*, $\neg\forall AB{:}\ A \times B = B \times A$.
- Extends to $A_1 \times A_2 \times \ldots \times A_n$...

Exercise

- Let *A* represent the set of all students at a university, and let *B* represent the set of all courses offered at the university. What is the Cartesian product $A \times B$?
- What is the Cartesian product $A \times B \times C$, where $A = \{0,1\}$, $B = \{1,2\}$, and $C = \{0,1,2\}$?

Using Set Notation With Quantifiers

- Universal Quantifier: $\forall x \in S(P(x))$ is a shorthand for $\forall x\, (x \in S \rightarrow P(x))$
- Existential Quantifier: $\exists x \in S(P(x))$ is a shorthand for $\exists x\, (x \in S \wedge P(x))$

Exercise

- What do the statements $\forall x \in \mathbf{R}\, (x^2 \geq 0)$ and $\exists x \in \mathbf{N}\, (x^2 = 1)$ mean?

Truth Set of Quantifiers

- Given a predicate *P* and a domain *D*, the truth set of *P* is the set of elements *x* in *D* for which *P*(*x*) is true. It is denoted by $\{x \in D \mid P(x)\}$.
- Exercise: what are the truth sets of the predicates P(x), Q(x), and R(x), where *D* is the set of integers, and P(x) is `` $|x| = 1$'', Q(x) is ``$x^2 = 2$'', and R(x) is `` $|x| = x$''?

Set Operations: The Union Operator

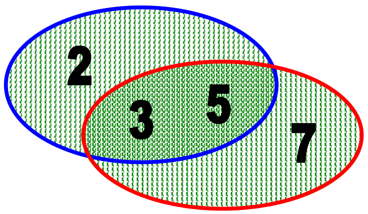
- For sets A, B, their *∪nion* $A\cup B$ is the set containing all elements that are either in A, **or** ("$\vee$") in B (or, of course, in both).
- Formally, $\forall A,B: A\cup B = \{x \mid x\in A \vee x\in B\}$.
- Note that $A\cup B$ is a **superset** of both A and B (in fact, it is the smallest such superset):

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

Union Examples

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

Required Form



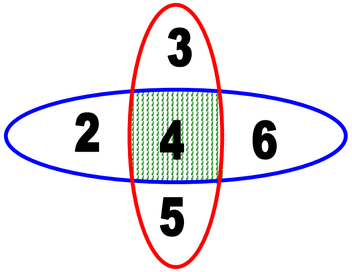
The Intersection Operator

- 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, $\forall A,B: A\cap B=\{x \mid x\in A \wedge x\in B\}$.
- Note that $A\cap B$ is a **subset** of both A and B (in fact it is the largest such subset):

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

Intersection Examples

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



Disjointedness

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

Inclusion-Exclusion Principle

- How many elements are in $A \cup B$?
  $|A \cup B| = |A| + |B| - |A \cap B|$ *(why?)*
- Example: How many students are on our class email list? Consider set $E = I \cup M$,
  $I = \{s \mid s \text{ turned in an information sheet}\}$
  $M = \{s \mid s \text{ sent the TAs their email address}\}$
- Some students did both!
  $|E| = |I \cup M| = |I| + |M| - |I \cap M|$

Set Difference

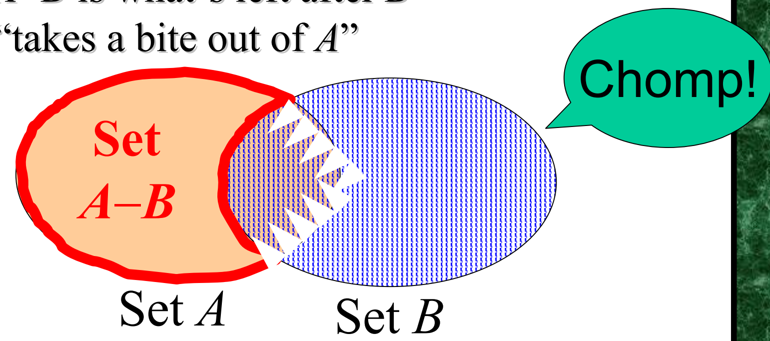
- For sets A, B, the *difference of A and B*, written $A - B$, is the set of all elements that are in A but not B. Formally:
  $$A - B :\equiv \{x \mid x \in A \wedge x \notin B\}$$
  $$= \{x \mid \neg(x \in A \rightarrow x \in B)\}$$
- Also called:
  The *complement of B with respect to A*.

Set Difference Examples

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

Set Difference - Venn Diagram

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



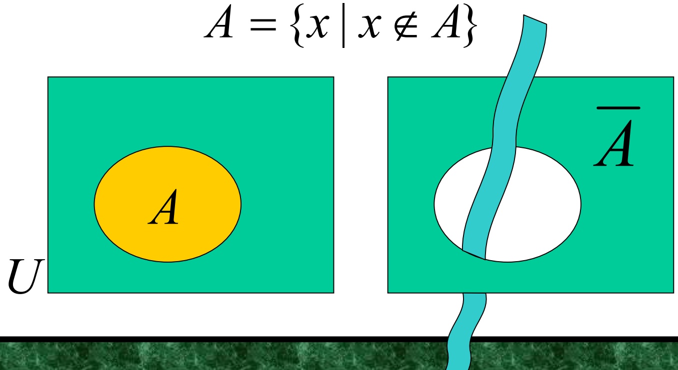
Set Complements

- 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 $U=\mathbf{N}$, $\overline{\{3,5\}} = \{0,1,2,4,6,7,\ldots\}$

More on Set Complements

- An equivalent definition, when U is clear:

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



Set Identities

- Identity: $A\cup\varnothing = A = A\cap U$
- Domination: $A\cup U = U$, $A\cap\varnothing = \varnothing$
- 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 provable from) DeMorgan's Law for propositions.

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

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

More Laws

- Absorption: $A \cup (A \cap B) = A$
  $A \cap (A \cup B) = A$
- Complement: $A \cup \overline{A} = U$
  $A \cap \overline{A} = \varnothing$

Proving Set Identities

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

1. Prove $E_1 \subseteq E_2$ and $E_2 \subseteq E_1$ separately.
2. Use set builder notation & logical equivalences.
3. Use a *membership table*.

Exercise

- Prove that $\overline{A \cap B} = \overline{A} \cup \overline{B}$
- Use set builder notation to prove the same identity.

Exercise

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

Exercise

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

- Part 1: 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, $A\cap(B\cup C)\subseteq(A\cap B)\cup(A\cap C)$.
- Part 2: Show $(A\cap B)\cup(A\cap C)\subseteq A\cap(B\cup C)$. …

Exercise

- Show that $\overline{A\cup(B\cap C)}=(\overline{C}\cup\overline{B})\cap\overline{A}$

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 on unordered *sets* of sets.

Generalized Union

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

Exercise

- Let $A_i = \{i, i+1, i+2, \ldots\}$. Find $\bigcup_{i=1}^{n} A_i$ and $\bigcap_{i=1}^{n} A_i$.
- Let $A_i = \{1, 2, 3, \ldots, i\}$. Find $\bigcup_{i=1}^{\infty} A_i$ and $\bigcap_{i=1}^{\infty} A_i$.

Generalized Intersection

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

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: **0**:≡∅, **1**:≡{**0**}, **2**:≡{**0**,**1**}, **3**:≡{**0**,**1**,**2**}, …
  - Bit strings: **0**:≡`0`, **1**:≡`1`, **2**:≡`10`, **3**:≡`11`, **4**:≡`100`, …

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 $\forall i: x_i \in S \leftrightarrow (i < n \wedge b_i = 1)$.

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

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