Introduction to Set Theory (§2.1)

• 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 (universal) in computer software systems.

• All of mathematics can be defined in terms of some form of set theory (using predicate logic).

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 $\{a, b, c\} = \{a, c\} = \{b, c\} = \{a, b, a, b, c, c, c, c\}$.
  – 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 | x is an integer where x>0 and x<5 \} = \{x | 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:
  - \( \mathbb{N} = \{0, 1, 2, \ldots\} \) The Natural numbers.
  - \( \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \) The Integers.
  - \( \mathbb{R} \) = The “Real” numbers, such as 374.182847192948181917281943125...
- “Blackboard Bold” or double-struck font (\( \mathbb{N}, \mathbb{Z}, \mathbb{R} \)) is also often used for these special number sets.
- Infinite sets come in different sizes!

More on this after module #4 (functions).

Basic Set Relations: Member of

- Def. \( x \in S \) (“\( x \) is in \( S \)”) is the proposition that object \( x \) is an element or member of set \( S \).
  - e.g. \( 3 \in \mathbb{N} \), “\( a \)”\( \in \{x | x \) is a letter of the alphabet\}"
  - Can define set equality in terms of \( \in \) relation:
    \( \forall S, T: S = T \iff (\forall x: x \in S \iff x \in T) \)
    “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

- Def. \( \emptyset \) ("null", "the empty set") is the unique set that contains no elements whatsoever.
- \( \emptyset = \{\} = \{x | \text{False}\} \)
- No matter the domain of discourse, we have:
  - Axiom. \( \neg \exists x: \ x \in \emptyset \).

Subset and Superset Relations

- Def. \( S \subseteq T \) ("\( S \) is a subset of \( T \)"; also pronounced \( S \) is contained in \( T \)) means that every element of \( S \) is also an element of \( T \).
- \( S \subseteq T \iff \forall x \ (x \in S \rightarrow x \in T) \)
- \( \emptyset \subseteq S, \ S \subseteq S \).
- Def. \( S \supseteq T \) ("\( S \) is a superset of \( T \)"; also pronounced \( S \) includes \( T \)) means \( T \subseteq S \).
- Note \( S = T \iff S \subseteq T \land S \supseteq T \).
- \( S \not\subseteq T \) means \( \neg(S \subseteq T) \), i.e. \( \exists x \ (x \in S \land x \not\in T) \).

Proper (Strict) Subsets & Supersets

- Def. \( S \subset T \) ("\( S \) is a proper subset of \( T \)"
 means that \( S \subseteq T \) but \( T \not\subseteq S \).
  i.e. there exists at least one element of \( T \) not contained in \( S \).

Example:

Consider a set \( \{a, b, c, d, e\} \).

Then sets \( \{d, b, a\} \), \( \{c, e\} \), \( \{e\} \) and \( \emptyset \) are proper subsets
but, \( \{a, b, f\} \), \( \{k\} \) and \( \{e, b, a, d, c\} \) are not!
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 \( 1 \neq \{1\} \neq \{\{1\}\} \)

Cardinality and Finiteness

- **Def.** \( |S| \) (read "the cardinality of \( S \)") is a measure of how many different elements \( S \) has.
- \( E.g., \) \( |\emptyset|=0, \quad |\{1,2,3\}| = 3, \quad |\{a,b\}| = 2, \quad |\{\{1,2,3\},\{4,5\}\}| = 2 \)
- 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?
  - \( \mathbb{N}, \mathbb{Z}, \mathbb{R} \)

The Power Set Operation

- **Def.** 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 \( 2^S \).
- Remark. For finite \( S \), \( |P(S)| = 2^{|S|} \).
- It turns out \( \forall S: |P(S)| > |S|, \) e.g. \( |P(\mathbb{N})| > |\mathbb{N}| \).
- **There are different sizes of infinite sets!**

Ordered \( n \)-tuples

- These are like sets, except that duplicates matter, and the order makes a difference.
- **Def.** For \( n \in \mathbb{N} \), 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, singlets, pairs, triples, quadruples, quintuples, …, \( n \)-tuples.
Cartesian Products

- Def. For sets $A$, $B$, their Cartesian product $A \times B : \equiv \{(a, b) \mid a \in A \wedge b \in B \}$.
- E.g. $(a, b) \times \{1, 2\} = \{(a, 1), (a, 2), (b, 1), (b, 2)\}$
- Remarks ($A \times B$ is a set of ORDERED $n$-tuples)
  - For finite $A$, $B$, $|A \times B| = |A||B|$
  - The Cartesian product is not commutative; i.e., $\neg \forall AB: A \times B = B \times A$
  - Extends to $A_1 \times A_2 \times \ldots \times A_n$...

Review: Set Notations So Far

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

Start §2.2: The Union Operator

- Def. For sets $A$, $B$, their union $A \cup B$ is the SET containing all elements that are either in $A$, or (“\lor”) in $B$ (or, of course, in both).
- Formally, $\forall A, B: A \cup B = \{x \mid x \in A \lor x \in B\}$.
- Remark. $A \cup B$ is a superset of both $A$ and $B$
  (in fact, it is the smallest such superset): $\forall A, B: (A \cup B \supseteq A) \land (A \cup B \supseteq B)$

Union Examples

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

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

- **Def.** For sets $A$, $B$, their *intersection* $A \cap B$ is the set containing all elements that are simultaneously in $A$ and (“$\cap$”) in $B$.
- Formally, $\forall A, B: A \cap B = \{x \mid x \in A \land x \in B\}$.
- **Remark.** $A \cap B$ is a *subset* of both $A$ and $B$ (in fact it is the largest such subset): $\forall A, B: (A \cap B \subseteq A) \land (A \cap B \subseteq B)$.

Intersection Examples

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

Disjointedness

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

• Def. For sets $A$, $B$, the difference of $A$ and $B$, written $A \setminus B$, is the set of all elements that are in $A$ but not $B$.
• Formally:
  \[ A \setminus B := \{ x \mid x \in A \land x \not\in B \} \]
  \[ = \{ x \mid \neg(x \in A \implies x \in B) \} \]
• Also called: The complement of $B$ with respect to $A$.

Set Difference - Venn Diagram

• $A \setminus B$ is what’s left after $B$ “takes a bite out of $A$”

Set Difference Examples

• \[ \{1,2,3,4,5,6\} \setminus \{2,3,5,7,9,11\} = \{1,4,6\} \]
• \[ \mathbb{Z} - \mathbb{N} = \{\ldots, -1, 0, 1, 2, \ldots\} - \{0, 1, \ldots\} = \{x \mid x \text{ is an integer but not a nat. #}\} \]
• \[ = \{x \mid x \text{ is a negative integer}\} \]
• \[ = \{\ldots, -3, -2, -1\} \]

Set Complements

• Def. 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 $U \setminus A$.
• E.g., If $U = \mathbb{N}$, $\overline{\{3,5\}} = \{0,1,2,4,6,7,\ldots\}$
More on Set Complements

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

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

Set Identities

• Identity: $A \cup \emptyset = A = A \cap U$
• Domination: $A \cup U = U$, $A \cap \emptyset = \emptyset$
• Idempotent: $A \cup A = A = A \cap A$
• Double complement: $(\overline{A}) = A$
• 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.

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

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

Proving Set Identities

• To prove statements about sets, of the form $E_1 = E_2$ (where the $E$s 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.
Method 1: Mutual subsets

• Example:
  
  \[ A \cap (B \cup C) = (A \cap B) \cup (A \cap C). \]

  \[ \text{Part 1: Show } A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C). \]
  
  – 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, \( A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C) \).
  
  \[ \text{Part 2: Show } (A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C). \ldots \]

Method 2: Use set builder notation & logical equivalences

• Show \( A \cap B = \overline{A \cup \overline{B}} \)

See Ex. 11, page 125 in edition 6 of our textbook

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.
  (trick is, use MAX for \( \cup \), and min for \( \cap \))
• Prove equivalence with identical columns.

Membership Table Example

• Prove \( (A \cup B) \setminus B = A \setminus B \).

  Hint: think about an element \( x \) which does or doesn’t belong to \( A \) and/or \( B \)

  \[ \begin{array}{c|c|c|c|c}
  A & B & A \cup B & (A \cup B) \setminus B & A \setminus B \\
  \hline
  0 & 0 & 0 & 0 & 0 \\
  0 & 1 & 1 & 1 & 0 \\
  1 & 0 & 1 & 1 & 1 \\
  1 & 1 & 1 & 1 & 0 \\
  \end{array} \]
Membership Table Exercise

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

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>((A \cup B) - C)</th>
<th>(A - C)</th>
<th>(B - C)</th>
<th>((A - C) \cup (B - C))</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

09/02/2016 37/44

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,

\[ X = \{A \mid P(A)\}. \]

09/02/2016 38/44

Generalized Union

• Binary union operator:
  \( A \cup B \)

• \(n\)-ary union:
  \( A_1 \cup A_2 \cup \ldots \cup A_n \) :
  \(((\ldots((A_1 \cup A_2) \cup \ldots) \cup A_n))\)
  (grouping & order is irrelevant)

• “Big U” notation: \( \bigcup_{i=1}^{n} A_i \)

• or for infinite sets of sets: \( \bigcup_{A \in X} A \)

09/02/2016 39/44

Generalized Intersection

• Binary intersection operator:
  \( A \cap B \)

• \(n\)-ary intersection:
  \( A_1 \cap A_2 \cap \ldots \cap A_n \) :
  \(((\ldots((A_1 \cap A_2) \cap \ldots) \cap A_n))\)
  (grouping & order is irrelevant)

• “Big Arch” notation: \( \bigcap_{i=1}^{n} A_i \)

• or for infinite sets of sets: \( \bigcap_{A \in X} A \)

09/02/2016 40/44
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 x₁, x₂, ..., represent a finite set S ⊆ U as the finite bit string B = b₁b₂...bₙ where ∀i: xi ∈ S ⇔ (i < n ∧ bᵢ = 1).
  • E.g. U = N, S = {2, 3, 5, 7, 11},
    B = 01101010001.

Review: Set Operations § 2.2

• Union
• Intersection
• Set difference
• Set complements
• Set identities
• Set equality proof techniques:
  – Mutual subsets.
  – Derivation using logical equivalences.
• Set representations

References

• Rosen
  Discrete Mathematics and its Applications, 6e