Today’s topics

• Sets
  – Definitions
  – Operations
  – Proving Set Identities
• Reading: Sections 1.6-1.7
• Upcoming
  – Functions

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 \( \sim p \) follow logically from the axioms of the theory!
  – \( \vdash \). The conjunction of the axioms 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 \( S, T, U, \ldots \)
• 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 \( P(x) \).
**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 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 Natural numbers.
  \(\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}\) The Integers.
  \(\mathbb{R} = \) The “Real” numbers, such as
  \(374.1828471929498181917281943125\ldots\)
- “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!
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 \( S \).
  - \( \text{e.g.} \ 3 \in \mathbb{N}, \ “a” \in \{x \mid x \text{ is a letter of the alphabet}\} \)
  - Can define set equality in terms of \( \in \) relation:
    \( \forall S,T: S = T \iff (\forall x: x \in S \iff x \in T) \)
    “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

- \( \emptyset \) (“null”, “the empty set”) is the unique set that contains no elements whatsoever.
- \( \emptyset = \{\} = \{x \mid \text{False}\} \)
- 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 \( T \).
- \( S \subseteq T \iff \forall x (x \in S \rightarrow x \in T) \)
- \( \emptyset \subseteq S, \ S \subseteq \emptyset. \)
- \( S \supseteq T \) (“\( S \) is a superset of \( T \)”) means \( T \subseteq S. \)
- Note \( S = T \iff S \subseteq T \land T \supseteq S. \)
- \( S \not\subset T \) means \( \neg (S \subseteq T), \ i.e. \ \exists x(x \in S \land x \notin T) \)

Proper (Strict) Subsets & Supersets

- \( S \subset T \) (“\( S \) is a proper subset of \( T \)”) means that \( S \subseteq T \) but \( T \not\subset S. \) 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 $1 \neq \{1\} \neq \{\{1\}\}$ !!!!

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

Cardinality and Finiteness

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

Review: Set Notations So Far

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

- There are some naïve set descriptions that lead to pathological structures that are not well-defined.
  - (That do not have self-consistent properties.)
- These “sets” mathematically cannot exist.
- E.g. let \( S = \{ x \mid x \notin x \} \). Is \( S \subseteq S \)?
- 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 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 of Sets

- For sets \( A, B \), their Cartesian product \( A \times B := \{ (a, b) \mid a \in A \land b \in B \} \).
- 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 \( A_1 \times A_2 \times \ldots \times A_n \).

Review of §1.6

- Sets \( S, T, U \ldots \) Special sets \( \mathbb{N}, \mathbb{Z}, \mathbb{R} \).
- Set notations \( \{a,b,\ldots\}, \{x \mid P(x)\} \ldots \)
- 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: \( \cup, \cap, \neg \).
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 (“\lor”) in $B$ (or, of course, in both).
- Formally, $\forall A, B: A \cup B = \{ x \mid x \in A \lor x \in B \}$.
- Note that $A \cup B$ is a superset of both $A$ and $B$ (in fact, it is the smallest such superset):
  $\forall A, B: (A \cup B \supseteq A) \land (A \cup B \supseteq B)$

Union Examples

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

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

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

Intersection Examples

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

Think “The intersection of Main St. and 9th 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 \(A \cup B\)?
  \[|A \cup B| = |A| + |B| - |A \cap B|\]
- 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**

- 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:
  \[A - B := \{x \mid x \in A \land x \notin B\}\]
  \[= \{x \mid \neg (x \in A \rightarrow x \in B)\}\]
- Also called:
  The **complement of \(B\) with respect to \(A\)**.

**Set Difference Examples**

- \(\{1,2,3,4,5,6\} - \{2,3,5,7,9,11\} = \) 
- \(\mathbb{Z} - \mathbb{N} = \{\ldots, -1, 0, 1, 2, \ldots\} - \{0, 1, \ldots\} = \{x \mid x\) is an integer but not a nat. \#\}\)
  \[= \{x \mid x\) is a negative integer\}\)
  \[= \{\ldots, -3, -2, -1\}\)
More on Set Complements

• An equivalent definition, when $U$ is clear:
  $$\overline{A} = \{x \mid x \notin A\}$$

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

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: $\overline{\overline{A}} = A$

• 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.

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

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

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 a membership table.
3. Use set builder notation & logical equivalences.

Method 1: Mutual subsets

Example: 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 $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.

Method 2: 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 \((A \cup B) - B = A - B\).

\[
\begin{array}{c|c|c|c|c}
A & B & A \cup B & (A \cup B) - B & A - B \\
\hline
0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 \\
\end{array}
\]

Membership Table Exercise

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

\[
\begin{array}{c|c|c|c|c|c|c|c}
A & B & A \cup B & (A \cup B) - C & A - C & B - C & (A - C) \cup (B - C) \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 \\
\end{array}
\]

Review of §1.6-1.7

- Sets \(S, T, U\ldots\) Special sets \(N, Z, R\).
- Set notations \(\{a,b,\ldots\}, \{x \mid P(x)\} \ldots\)
- Relations \(x \in S, \subseteq T, \supseteq T, S = T, S \subset T, S \supset T\).
- 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 \((A_1, \ldots, A_n)\), or even on unordered sets of sets, \(X = \{A \mid P(A)\}\).
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: \(0:=\emptyset, 1:=\{0\}, 2:=\{0,1\}, 3:=\{0,1,2\}, \ldots\)
- Bit strings: \(0:=0, 1:=1, 2:=10, 3:=11, 4:=100, \ldots\)

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 \(B=b_1b_2\ldots b_n\) where \(\forall i: x_i\in S\iff (i<n \land b_i=1)\).

E.g. \(U=\mathbb{N}, S=\{2,3,5,7,11\}, B=001101010001\).

In this representation, the set operators “\(\cup\)”, “\(\cap\)”, “\(\setminus\)”, “\(\sim\)” are implemented directly by bitwise OR, AND, NOT!