Discrete Mathematics: Lecture 7

- Today:
  - Chap 2.1: Sets
  - Chap 2.2: Set Operations
- Next time:
  - Chap 2.3: Functions

Chap 2.1: Sets (集合)

- Definition: A set is an unordered collection of objects.
- Note: the definition is based on the intuitive notion of an object.
- Definition: The objects in a set are called the elements, or members, of the set. A set is said to contain its elements.
- Notation:
  - $a \in A$: a is an element of the set A
  - $a \notin A$: a is not an element of the set A
  - we usually use lowercase letters to denote elements of sets

Describing a set by listing its members

- The set V of all vowels in the English alphabet:
  $V = \{a, e, i, o, u\}$
- The set O of odd positive integers less than 10:
  $O = \{1, 3, 5, 7, 9\}$
- Although sets are usually used to group together elements with common properties, this is not a requirement, *e.g.*, $\{a, 2,$Fred, New Jersey$\}$
- Sometimes we do not list all the elements: we list some elements, and use ... when the general pattern is obvious, eg, $\{1, 2, 3, \ldots, 99\}$

Commonly used sets

- $\mathbf{N} = \{0, 1, 2, 3, \ldots\}$, the set of natural numbers
- $\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, the set of integers
- $\mathbf{Z}^+ = \{1, 2, 3, \ldots\}$, the set of positive integers
- $\mathbf{Q}$, the set of rational numbers
- $\mathbf{R}$, the set of real numbers

Note: Sets can have other sets as members, *e.g.*, $\{\mathbf{N}, \mathbf{Z}, \mathbf{Q}, \mathbf{R}\}$

Describing a set with the set builder notation

We characterize all the elements by stating their common property

- The set O of odd positive integers less than 10:
  $\{x \in \mathbf{Z}^+ \mid x \text{ is odd and } x < 10\}$
- $\mathbf{Q}^+ = \{x \in \mathbf{R} \mid x = p/q \text{ for some positive integers } p \text{ and } q\}$

Russell's paradox (罗素悖论)

- We have defined a set as a collection of objects.
- Let $S = \{x \mid x \notin x\}$.
- Does $S \in S$?
- This paradox can be avoided by building set theory based on axioms, known as axiomatic set theory (公理集合论) .
- We will use naive set theory (朴素集合论): the sets we consider in this book won't lead to inconsistencies.

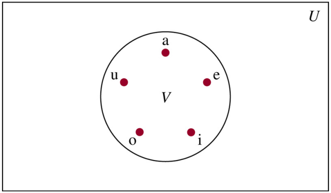
Equality between two sets

- Definition: Two sets are equal iff they have the same elements. That is, if A and B are sets, then A and B are equal iff $\forall x(x \in A \leftrightarrow x \in B)$. We write $A = B$ if A and B are equal sets.
- Example: $\{1, 3, 5\} = \{3, 5, 1\}$. Note: the order of elements does not matter.
- Example: $\{1, 3, 5\} = \{1, 1, 3, 3, 3, 5, 5\}$. Note: it does not matter if an element is listed more than once

Venn diagrams (韦恩图)

- Sets can be represented graphically using Venn diagrams
- The universal set (全集) U, containing all the elements under consideration, is represented by a rectangle. Note that the universal set varies depends on the context.
- Insider this rectangle, circles are used to represent sets
- Points are used to represent elements of the set
- Venn diagrams are often used to indicate the relationships between sets

Venn Diagram for the set of vowels

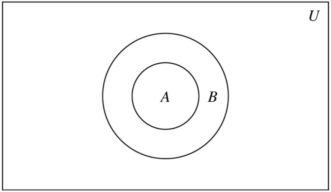


The empty set

- The special set with no elements is called the empty set (空集), or the null set, and is denoted by $\varnothing$, or $\{\}$.
- A set with a single element is called a singleton set (单元素集).
- The difference between $\varnothing$ and $\{\varnothing\}$.

Subsets

- Definition: A set A is said to be a subset (子集) of a set B if every element of A is also an element of B. We use $A \subseteq B$ to denote that A is a subset of B.
- $A \subseteq B$ iff $\forall x(x \in A \rightarrow x \in B)$, $A = B$ iff $A \subseteq B$ and $B \subseteq A$
- Definition: A is a proper subset (真子集) of B, denoted by $A \subset B$, if $A \subseteq B$ but $A \neq B$.
- $A \subset B$ iff $\forall x(x \in A \rightarrow x \in B) \wedge \exists x(x \in B \wedge x \notin A)$
- Example: $\mathbf{N} \subseteq \mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R}$
- Theorem: For every set S, (i) $\varnothing \subseteq S$ and (ii) $S \subseteq S$.



The size of sets

- Definition: Let S be a set. If there are exactly n distinct elements in S where $n \in \mathbf{N}$, we say that S is a finite set and n is the cardinality (基数) of S, denoted by $|S|$.
- Definition: A set is said to be infinite if it is not finite.
- $|\varnothing| = 0$
- Example: let A be the set of English letters. Then $|A| = 26$.

The power set

- Definition: Let S be a set. The power set (幂集) of S, denoted by $P(S)$, is the set of all subsets of S.
- Example: $P(\{0, 1, 2\})$
- $P(\varnothing)$, $P(\{\varnothing\})$
- If a set has n elements, then its power set has 2^n elements.

Cartesian products (笛卡尔乘积)

- Definition: The ordered n-tuple (有序n元组) $(a_1, a_2, \ldots, a_n)$ is the ordered collection that has a_1 as its first element, ..., and a_n as its nth element.
- Two ordered n-tuples are equal iff each element is equal to its corresponding element.
- Definition: Let A and B be sets. The Cartesian Product of A and B, denoted by $A \times B$, is the set of all ordered pairs (a, b), where $a \in A$ and $b \in B$. Hence, $A \times B = \{(a, b) \mid a \in A, b \in B\}$.
- Definition: A subset of $A \times B$ is called a relation (关系) from A to B.
- Example: Let $A = \{1, 2\}$, and $B = \{a, b, c\}$. What is $A \times B$? What is a relation from A to B? Show that $A \times B \neq B \times A$.

Generalized Cartesian product

- Definition: The Cartesian Product of the sets $A_1, A_2, \ldots, A_n$, denoted by $A_1 \times A_2 \times \ldots \times A_n$, is the set of all ordered n-tuples $(a_1, a_2, \ldots, a_n)$, where $a_i \in A_i$ for $i = 1, 2, \ldots, n$.
- Example: Let $A = \{1, 2\}$, $B = \{T, F\}$, $C = \{a, b, c\}$. What is $A \times B \times C$?

Using set notation with quantifiers

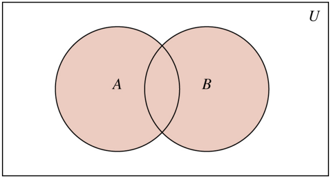
- $\forall x \in S(P(x))$ means $\forall x(x \in S \rightarrow P(x))$
- $\exists x \in S(P(x))$ means $\exists x(x \in S \wedge P(x))$
- Example: what is the truth value of $\exists x \in \mathbf{N} \forall y \in \mathbf{N}(x + y = y)$?

Truth sets of quantifiers

- Definition: Let D be a set, and P be a predicate. The truth set of P wrt D is the set $\{x \in D \mid P(x)\}$.
- Example: Let $D = \mathbf{Z}$. Let $P(x) : |x| = 1$, and $Q(x) : x^2 = 2$. What are the truth sets?

Two sets can be combined in many different ways.

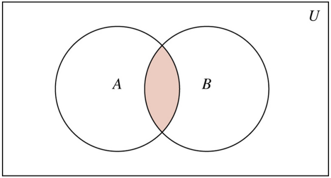
- Definition: Let A and B be sets. The union (并集) of A and B, denoted by $A \cup B$, is the set that contains those elements that are either in A or in B.
- So $A \cup B = \{x \mid x \in A \vee x \in B\}$
- Example: $\{1, 3, 5\} \cup \{1, 2, 3\}$
- Example: $CS \cup Math$, where CS (resp. $Math$): the set of all students majoring in computer science (resp. mathematics) at our school



A B is shaded.

Intersection

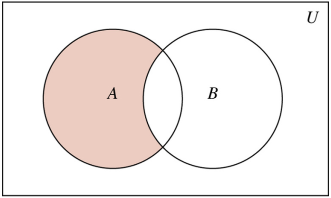
- Definition: Let A and B be sets. The intersection (交集) of A and B, denoted by $A \cap B$, is the set that contains those elements in both A and B.
- So $A \cap B = \{x \mid x \in A \land x \in B\}$
- Example: $\{1,3,5\} \cap \{1,2,3\}$, $CS \cap Math$
- Definition: two sets are disjoint (不相交的) if their intersection is the empty set.
- Example: the sets of even and odd numbers are disjoint.
- $|A \cup B| = |A| + |B| - |A \cap B|$



A B is shaded.

Difference

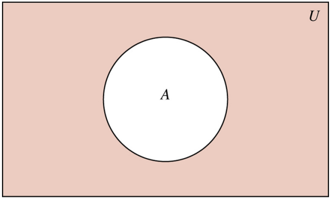
- Definition: Let A and B be sets. The difference of A and B, denoted by $A - B$ (差集), is the set that contains those elements in A but not in B.
- So $A - B = \{x \mid x \in A \wedge x \notin B\}$
- Example: $\{1, 3, 5\} - \{1, 2, 3\}$, $CS - Math$



$A - B$ is shaded.

Complement

- Definition: Let U be the universal set. The complement (补集) of a set A, denoted by $\overline{A}$, is the difference of U and A.
- So $\overline{A} = \{x \mid x \notin A\}$
- Example: Let U be the set of English letters, and $V = \{a, e, i, o, u\}$. What is $\overline{V}$?



$\overline{A}$ is shaded.

Set identities (集合恒等式)

$A \cup \varnothing = A$ $A \cap U = A$	Identity laws
$A \cup U = U$ $A \cap \varnothing = \varnothing$	Domination laws
$A \cup A = A$ $A \cap A = A$	Idempotent laws
$\overline{(\overline{A})} = A$	Complementation law
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws

同一律，零律，幂等律，双重否定律，交换律

Set identities

$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative laws
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Distributive laws
$\overline{A \cup B} = \overline{A} \cap \overline{B}$ $\overline{A \cap B} = \overline{A} \cup \overline{B}$	De Morgan's laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption laws
$A \cup \overline{A} = U$ $A \cap \overline{A} = \varnothing$	Complement laws

结合律，分配律，德摩根律，吸收律，补律

Proving set identities

Different methods

- show that each is a subset of the other
- use set builder notation and logical equivalences
- use membership table
- use existing set identities

Examples:

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

Membership tables

To prove $S_1 = S_2$, we consider different combination of memberships, and show that in each case, membership in S_1 iff membership in S_2

A	B	C	$B \cup C$	$A \cap (B \cup C)$	$A \cap B$	$A \cap C$	$(A \cap B) \cup (A \cap C)$
1	1	1	1	1	1	1	1
1	1	0	1	1	1	0	1
1	0	1	1	1	0	1	1
1	0	0	0	0	0	0	0
0	1	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	0	1	1	0	0	0	0
0	0	0	0	0	0	0	0

Generalized unions and intersections

- Due to associative laws, $A \cup B \cup C$ and $A \cap B \cap C$ are well-defined
- Definition: The union of a collection of sets is the set that contains elements that are in at least one of the sets.
- Notation: $A_1 \cup A_2 \cup \ldots \cup A_n = \bigcup_{i=1}^{n} A_i$
- Definition: The intersection of a collection of sets is the set that contains elements that are in all of the sets.
- Notation: $A_1 \cap A_2 \cap \ldots \cap A_n = \bigcap_{i=1}^{n} A_i$
- Example: $A = \{0, 2, 4\}, B = \{0, 1, 2\}, C = \{0, 3, 6\}$
- Example: $A_i = \{i, i+1, i+2, \ldots\}$,

$$\bigcup_{i=1}^{n} A_i, \bigcap_{i=1}^{n} A_i, \bigcup_{i=1}^{\infty} A_i, \bigcap_{i=1}^{\infty} A_i$$

Logic and bit operations

- Computers represent information using bits. A bit is a symbol with two possible values.
- Computer bit operations correspond to the logical connectives. There are operators $\wedge, \vee, \bigoplus$, or denoted by AND, OR, XOR
- A bit string is a sequence of zero or more bits. The length of this string is the number of bits in the string.
- We can extend bit operations to bit strings: bitwise AND, OR, XOR

Computer representation of sets

- There are various ways to represent sets using a computer.
- One way is to store the elements of the set.
- Then it would be time-consuming to compute the union, intersection, or difference of sets, since a large amount of searching is required.
- Assume that the universal set U is finite and of reasonable size (so that the size is not larger than the memory size)
- Specify an arbitrary ordering of elements of U, say $a_1, a_2, \ldots, a_n$
- A set A is represented by a bit string of length n, where the ith bit is 1 iff $a_i \in A$
- Then it is easy to compute unions, intersections, or differences

An example

- Let $U = \{1, 2, \ldots, 10\}$
- The bit string for $O = \{1, 3, 5, 7, 9\}$, $F = \{1, 2, 3, 4, 5\}$
- What is the bit string for $\overline{O}$
- What are the bit strings for $O \cup F$ and $O \cap F$