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.

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).*

e.g., $\{x \mid x$ is an integer where $x>0$ and $x<5\}$

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!
  - {a, b, c} = {a, a, b, a, b, c, c, c, c}.
  - This set contains at most 3 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 = {1, 2, 3, …} The **n**atural numbers.
  Z = {…, -2, -1, 0, 1, 2, …} The integers.
  R = The "**r**eal" numbers, such as 374.1828471929498181917281943125…
- Infinite sets come in different sizes!

Basic Set Relations:

- $x \in S$ ("x is in S") is the proposition that object x is an $\in$*element* 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 $\neg\exists x$: $x \in \varnothing$.
- There is at least one x

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 $S=T \Leftrightarrow S \subseteq T \wedge S \supseteq T$. 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 $S \supset T$.

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__
- We say S is *infinite* if it is not *finite*.
- What are some infinite sets we've seen?

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.* $P(\{a,b\}) = \{\varnothing, \{a\}, \{b\}, \{a,b\}\}$.
- Sometimes $P(S)$ is written $\mathbf{2}^S$.
  Note that for finite S, $|P(S)| = 2^{|S|}$.
- It turns out that $|P(\mathbf{N})| > |\mathbf{N}|$.
  There are different sizes of infinite sets!

Ordered *n*-tuples

- For $n \in \mathbf{N}$, an *ordered n-tuple* or a sequence of length n is written $(a_1, a_2, \ldots, a_n)$. The *first* element is a_1, *etc.*
- These are like sets, except that duplicates matter, and the order makes a difference.
- Note $(1, 2) \neq (2, 1) \neq (2, 1, 1)$.
- Empty sequence, singlets, pairs, triples, quadruples, quintuples, …, n-tuples.

Cartesian Products of Sets

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

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

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

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: $\{2,3,5\} \cup \{3,5,7\} = \{2,3,5,3,5,7\} = \{2,3,5,7\}$

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.
- $A - B :\equiv \{x \mid x \in A \wedge x \notin B\}$
  $= \{x \mid \neg(x \in A \rightarrow x \in B)\}$
- Also called: The complement of B with respect to A.

Set Difference Examples

- $\{1,2,3,4,5,6\} - \{2,3,5,7,9,11\} =$ ______1, 4,6______

- **Z** – W = {… , -1, 0, 1, 2, … } − {0, 1, … }
  = {x | x is an integer but not a ___}
  = {x | x is a negative integer}
  = {… , -3, -2, -1}

Set Complements

- The *universe of discourse* can itself be considered a set, call it U.
- The *complement* of A, written , is the complement of A w.r.t. U, *i.e.*, it is $U{-}A$.
- *E.g.*, If U=**W**, $\overline{\{3,5\}} = \{0,1,2,4,6,7,...\}$

Set Identities

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

TABLE 1 Set Identities.

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

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 logical equivalences.
- Use a *membership table*.

Method : 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 : 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

Generalized Union

- Binary union operator: $A \cup B$
- n-ary union:
  $A1 \cup A_2 \cup \ldots \cup A_n :\equiv ((\ldots((A_1 \cup A_2) \cup \ldots) \cup A_n)$
  (grouping & order is irrelevant)
- "Big U" notation: $\bigcup_{i=1}^{n} A_i$
- Or for infinite sets of sets: $\bigcup_{A \in X} A$

Generalized Intersection

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

Multisets

- Sometimes the number of times that an element occurs in an unordered collection matters.
- **Multisets** are unordered collections of elements where an element can occur as a member more than once.
- The notation $\{m1 \cdot a1, m2 \cdot a2, \ldots, mr \cdot ar\}$ denotes the multiset with element $a1$ occurring $m1$ times, element $a2$ occurring $m2$ times, and so on.
- The numbers mi , $i = 1, 2, \ldots, r$ are called the **multiplicities** of the elements ai , $i = 1, 2, \ldots, r$.
- The **union** ($P \cup Q$) of the multisets P and Q is the multiset where the multiplicity of an element is the maximum of its multiplicities in P and Q.
- The **intersection** **(**$P \cap Q$ **)** of P and Q is the multiset where the multiplicity of an element is the minimum of its multiplicities in P and Q.
- The **difference** **(**P -Q **)**of P and Q is the multiset where the multiplicity of an element is the multiplicity of the element in P less its multiplicity in Q unless this difference is negative, in which case the multiplicity is 0.
- The **sum** of P and Q is the multiset where the multiplicity of an element is the sum of multiplicities in P and Q.
- The union, intersection, and difference of P and Q are denoted by, and $P - Q$, respectively (where these operations should not be confused with the analogous operations for sets).
- The sum of P and Q is denoted by $P + Q$.
- EX.: Let A and B be the multisets $\{3 \cdot a, 2 \cdot b, 1 \cdot c\}$ and $\{2 \cdot a, 3 \cdot b, 4 \cdot d\}$, respectively.

Find **a)** $A \cup B$. **b)** $A \cap B$. **c)** $A - B$. **d)** $B - A$. **e)** $A + B$.

Fuzzy sets

- **Fuzzy sets** are used in artificial intelligence. Each element in the universal set U has a **degree of membership**, which is a real number between 0 and 1 (including 0 and 1), in a fuzzy set S.
- The fuzzy set S is denoted by listing the elements with their degrees of membership (elements with 0 degree of membership are not listed).
- *Let* R is the set of rich people with $R = \{$0.4 Alice, 0.8 Brian, 0.2 Fred, 0.9 Oscar, 0.7 Rita$\}$.
- For the set F (of famous people)= {0.6 Alice, 0.9 Brian, 0.4 Fred, 0.1 Oscar, 0.5 Rita}
- The **complement** of a fuzzy set S is the set S, with the degree of the membership of an element in S equal to 1 minus the degree of membership of this element in S.
- Find -F (the fuzzy set of people who are not famous) and -R (the fuzzy set of people who are not rich).
- The **union** of two fuzzy sets S and T is the fuzzy set $S \cup T$, where the degree of membership of an element in $S \cup T$ is the maximum of the degrees of membership of this element in S and in T.
- Find the fuzzy set $F \cup R$ of rich or famous people.
- The **intersection** of two fuzzy sets S and T is the fuzzy set $S \cap T$, where the degree of membership of an element in $S \cap T$ is the minimum of the degrees of membership of this element in S and in T.
- Find the fuzzy set $F \cap R$ of rich and famous people.

Functions

- Let A and B be **non**empty sets. A *function f* from A to B is an assignment of exactly one element of B to each element of A. We write $f(a) = b$ if b is the unique element of B assigned by the function f to the element a of A.
- If f is a function from A to B, we write $f : A \rightarrow B$.
- Functions are sometimes also called **mappings** or **transformations**.
- If f is a function from A to B, we say that A is the *domain* of f and B is the *codomain* of f.
- If $f(a) = b$, we say that b is the *image* of a and a is a *preimage* of b.
- The *range*, or *image*, of f is the set of all images of elements of A. Also, if f is a function from A to B, we say that *f maps* A to B.

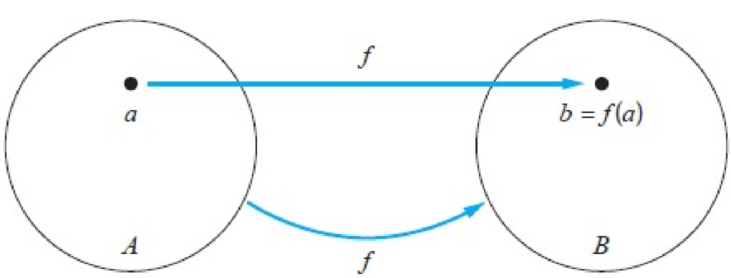
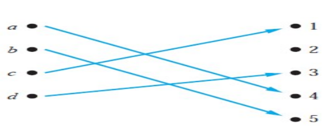


FIGURE The Function f Maps A to B.

- Let $f : \mathbf{Z} \rightarrow \mathbf{Z}$ assign the square of an integer to this integer. Then, $f(x) = x2$, where the domain of f is the set of all integers, the codomain of f is the set of all integers, and the range of f is the set of all integers that are perfect squares, namely, $\{0, 1, 4, 9, \ldots\}$.
- Let f be the function that assigns the last two bits of a bit string of length 2 or greater to that string. For example, $f(11010) = 10$. Then, the domain of f is the set of all bit strings of length 2 or greater, and both the codomain and range are the set $\{00, 01, 10, 11\}$.
- A function is called **real-valued** if its codomain is the set of real numbers, and it is called **integer-valued** if its codomain is the set of integers.
- Two real-valued functions or two integer valued functions with the same domain can be added, as well as multiplied.
- Let $f1$ and $f2$ be functions from A to $\mathbf{R}$. Then $f1 + f2$ and $f1\,f2$ are also functions from A to $\mathbf{R}$ defined for all $x \in A$ by
- $(f1 + f2)(x) = f1(x) + f2(x)$, $(f1\,f2)(x) = f1(x)\,f2(x)$.
- Let f be a function from A to B and let S be a subset of A. The *image* of S under the function f is the subset of B that consists of the images of the elements of S.
- We denote the image of S by $f(S)$, so
- $f(S) = \{t \mid \exists s \in S\ (t = f(s))\}$.
- We also use the shorthand $\{f(s) \mid s \in S\}$ to denote this set.
- Let $A = \{a, b, c, d, e\}$ and $B = \{1, 2, 3, 4\}$ with $f(a) = 2$, $f(b) = 1$, $f(c) = 4$, $f(d) = 1$, and $f(e) = 1$.
- The image of the subset $S = \{b, c, d\}$ is the set $f(S) = \{1, 4\}$.

One-to-One and Onto Functions

- A function f is said to be *one-to-one,* or an *injunction,* if and only if $f(a) = f(b)$ implies that $a = b$ for all a and b in the domain of f.
- A function is said to be *injective* if it is one-to-one.
- Ex. 

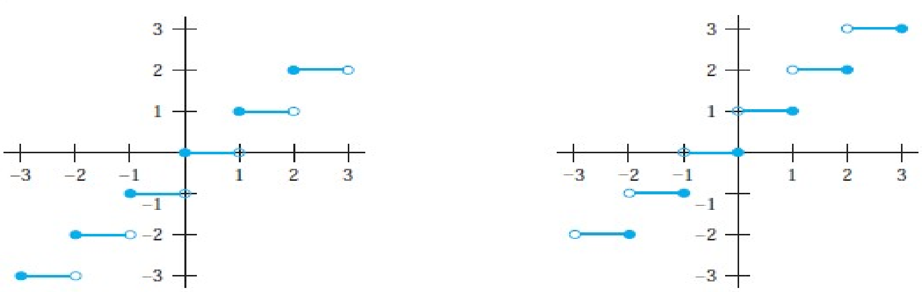
- Determine whether the function f from $\{a, b, c, d\}$ to $\{1, 2, 3, 4, 5\}$ with $f(a) = 4$, $f(b) = 5$, $f(c) = 1$, and $f(d) = 3$ is one-to-one.
- Determine whether the function $f(x) = x\text{^}2$ from the set of integers to the set of integers is one-to-one.
- Determine whether the function $f(x) = x + 1$ from the set of real numbers to itself is one-to one.

Onto Function

- A function f from A to B is called *onto,* or a *surjection,* if and only if for every element $b \in B$ there is an element $a \in A$ with $f(a) = b$.
- A function f is called *surjective* if it is onto.
- Let f be the function from $\{a, b, c, d\}$ to $\{1, 2, 3\}$ defined by $f(a) = 3$, $f(b) = 2$, $f(c) = 1$, and $f(d) = 3$. Is f an onto function?
- Is the function $f(x) = x$^2 from the set of integers to the set of integers onto?
- Is the function $f(x) = x + 1$ from the set of integers to the set of integers onto?
- The function f is a *one-to-one correspondence,* or a *bijection,* if it is both one-to-one and onto.
- We also say that such a function is *bijective*.
- Let f be a one-to-one correspondence from the set A to the set B. The ***inverse function*** of f is the function that assigns to an element b belonging to B the unique element a in A such that $f(a) = b$.
- The inverse function of f is denoted by f^(−1). Hence, f^(−1)$(b) = a$ when $f(a) = b$.
- Let g be a function from the set A to the set B and let f be a function from the set B to the set C. The ***composition*** of the functions f and g, denoted for all $a \in A$ by $f \circ g$, is defined by $(f \circ g)(a) = f(g(a))$.

The *floor function* assigns to the real number x the largest integer that is less than or equal to x. The value of the floor function at x is denoted by $\lfloor x \rfloor$. The *ceiling function* assigns to the real number x the smallest integer that is greater than or equal to x. The value of the ceiling function at x is denoted by $\lceil x \rceil$.

Remark: The floor function is often also called the *greatest integer function*. It is often denoted by $[x]$.



(a) $y = \lfloor x \rfloor$ (b) $y = \lceil x \rceil$

Data stored on a computer disk or transmitted over a data network are usually represented as a string of bytes. Each byte is made up of 8 bits. How many bytes are required to encode 100 bits of data?

Solution: To determine the number of bytes needed, we determine the smallest integer that is at least as large as the quotient when 100 is divided by 8, the number of bits in a byte. Consequently, $\lceil 100/8 \rceil = \lceil 12.5 \rceil = 13$ bytes are required. ◀

Computer Representation of Sets

- There are various ways to represent sets using a computer. One method is to store the elements of the set in an unordered fashion.
- However, if this is done, the operations of computing the union, intersection, or difference of two sets would be time-consuming, because each of these operations would require a large amount of searching for elements.
- A method for storing elements using an arbitrary ordering of the elements of the universal set is more efficient.
- Assume that the universal set U is finite (and of reasonable size so that the number of
- elements of U is not larger than the memory size of the computer being used).
- First, specify an arbitrary ordering of the elements of U, for instance $a1, a2, \ldots, an$. Represent a subset A of U with the bit string of length n, where the ith bit in this string is 1 if ai belongs to A and is 0 if ai does not belong to A.
- Example: The bit string for the set $\{1, 3, 5, 7, 9\}$ (with universal set $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$) is
- 10 1010 1010.
- What is the bit string for the complement of this set?