CS170: Discrete Methods in Computer Science
Summer 2023
Sets and Friends

Instructor: Shaddin Dughmi[1]

[1] These slides adapt some content from similar slides by Aaron Cote.

Outline

Definition

A set is an unordered collection of distinct objects, which we call it's members.

Examples: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$, $\emptyset$, even integers, prime numbers, students in this class, runtime functions that are $O(n)$

Definition

A set is an unordered collection of distinct objects, which we call it's members.

Examples: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$, $\emptyset$, even integers, prime numbers, students in this class, runtime functions that are $O(n)$

Notation

- $\emptyset$ is the empty set
- $\{1, 2, 3\}$: The set which includes the three number $1, 2, 3$
- Even $= \{x \in \mathbb{N} : \exists k \in \mathbb{N}\ x = 2k\}$
- $x \in A$ denotes membership. E.g. $4 \in$ Even
- $x \notin A$ denotes non-membership. E.g. $3 \notin$ Even

Note

Order and repetition don't matter!

- E.g. $\{1, 2, 3\} = \{3, 2, 1\} = \{2, 2, 1, 3, 3, 3\}$

Relationships between sets

- Subset: $A \subseteq B$ means every element of A is in B
  - E.g. $\{1,2\} \subseteq \{1,2,3\}$, $\mathbb{N} \subseteq \mathbb{Z}$, 170 students $\subseteq$ USC students
  - The empty set $\emptyset$ is a subset of every set
  - Every set is a subset of itself: e.g. $\{1,2,3\} \subseteq \{1,2,3\}$.
- Equality: $A = B$ if both $A \subseteq B$ and $B \subseteq A$.
- Proper subset: $A \subset B$ or $A \subsetneq B$ means $A \subseteq B$ but $A \neq B$.
  - E.g. 170 students $\subset$ USC students, $\mathbb{N} \subset \mathbb{Z}$
- Superset: $A \supseteq B$ means $B \subseteq A$.
- Proper Superset: $A \supset B$ or $A \supsetneq B$ means $B \subseteq A$ and $B \neq A$.
- We say A and B are disjoint if they have no elements in common
  - E.g. The set of Even numbers and the set of Odd numbers are disjoint

Sets of Sets

- Sets can include other sets as members. For example
  - $\{\{1\}, \{1, 2, 3\}, \emptyset\}$
  - Set of communities in a social network
  - $\left\{A \subseteq \mathbb{N} : \sum_{i \in A} i \leq 3\right\} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}\}$
  - $\{\emptyset, \{\emptyset\}, \mathbb{N}, \{\mathbb{N}, \mathbb{Q}\}\}$
- Powerset of A, denoted by $\mathcal{P}(A)$ or 2^A, is set of all subsets of A
  - E.g. $\mathcal{P}(\{1, 2, 3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$
  - E.g. $\mathcal{P}(\emptyset) = \{\emptyset\}$, and $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$

Cardinality of Sets

- The cardinality of a set A, denoted $|A|$, is the number of elements in it. May be finite or infinite. For example:
  - $|\{1,2,3\}| = 3$ and $|\emptyset| = 0$
  - $|\mathcal{P}(\{1,2,3\})| = 8$, $|\{\emptyset\}| = 1$, $|\mathcal{P}(\mathcal{P}(\emptyset))| = 2$
  - $|\mathbb{Z}|$ and $|\mathbb{R}|$ are ∞ (but not the same ∞!!)
  - $|\{\mathbb{Z}, \mathbb{R}\}| = 2$
- $|\mathcal{P}(A)| = 2^{|A|}$ for finite sets A (why?)

Cardinality of Sets

- The cardinality of a set A, denoted $|A|$, is the number of elements in it. May be finite or infinite. For example:
  - $|\{1,2,3\}| = 3$ and $|\emptyset| = 0$
  - $|\mathcal{P}(\{1,2,3\})| = 8$, $|\{\emptyset\}| = 1$, $|\mathcal{P}(\mathcal{P}(\emptyset))| = 2$
  - $|\mathbb{Z}|$ and $|\mathbb{R}|$ are ∞ (but not the same ∞!!)
  - $|\{\mathbb{Z}, \mathbb{R}\}| = 2$
- $|\mathcal{P}(A)| = 2^{|A|}$ for finite sets A (why?)

Interesting Fact

Comparing sizes of infinite sets is very interesting and relevant to CS! You will see that cardinality of set of computer programs is a smaller infinity than the cardinality of the set of problems you might want to solve, therefore there are problems that are not computable!

Operations on Sets and Venn Diagrams

- Intersection: $A \bigcap B$ contains elements that are in both A and B
- Union: $A \bigcup B$ contains elements that are in A or in B (or both)
- Difference: $A - B$ or $A \setminus B$ contains elements that are in A but not in B
- Complement: $\overline{A}$ contains elements that are not in A
  - Defined relative to a universe $\mathbb{U}$, which should clear from context.
  - $\overline{A} = \mathbb{U} - A$
- These operations are often visualized using Venn Diagrams (on board)

Operations on Sets and Venn Diagrams

- Intersection: $A \bigcap B$ contains elements that are in both A and B
- Union: $A \bigcup B$ contains elements that are in A or in B (or both)
- Difference: $A - B$ or $A \setminus B$ contains elements that are in A but not in B
- Complement: $\overline{A}$ contains elements that are not in A
  - Defined relative to a universe $\mathbb{U}$, which should clear from context.
  - $\overline{A} = \mathbb{U} - A$
- These operations are often visualized using Venn Diagrams (on board)

Some Examples

- Even $= \mathbb{Z} -$ Odd, which is $\overline{\text{Odd}}$ if universe is $\mathbb{Z}$
- Even $\bigcap$ Odd $= \emptyset$ (they are disjoint)
- Even $\bigcup$ Odd $= \mathbb{Z}$
- Multiples-of-3 $\bigcap$ Multiples-of-2 $=$ Multiples-of-6
- $\mathbb{Z} \bigcup \mathbb{R} = \mathbb{R}$
- $\emptyset \bigcup A = A$ and $\emptyset \bigcap A = \emptyset$ for any set A

Generalized Union and Intersection

Can union or intersect many sets all at once with following shorthand

$$\bigcup_{i=1}^{n} S_i = S_1 \bigcup S_2 \bigcup \ldots \bigcup S_n$$

$$\bigcap_{i=1}^{n} S_i = S_1 \bigcap S_2 \bigcap \ldots \bigcap S_n$$

Can also take infinite union / intersection. For example:

$$\mathbb{N} = \bigcup_{i=1}^{\infty} \{i\}$$

$$A = \bigcap_{x \notin A} (\mathbb{U} - \{x\})$$

Properties of Set operations

Commutative

$$A \bigcup B = B \bigcup A$$

$$A \bigcap B = B \bigcap A$$

Distributive

$$A \bigcup (B \bigcap C) = (A \bigcup B) \bigcap (A \bigcup C)$$

$$A \bigcap (B \bigcup C) = (A \bigcap B) \bigcup (A \bigcap C)$$

Properties of Set operations

Commutative

$$A \bigcup B = B \bigcup A$$

$$A \bigcap B = B \bigcap A$$

Distributive

$$A \bigcup (B \bigcap C) = (A \bigcup B) \bigcap (A \bigcup C)$$

$$A \bigcap (B \bigcup C) = (A \bigcap B) \bigcup (A \bigcap C)$$

Should remind you of commutative and distributive from propositional logic

Outline

Tuples

- An n-tuple is an ordered list of n elements (basically, an array of n elements)
  - Written using $()$ or $<>$, unlike sets which are written using $\{\}$
  - E.g. $(1, 2, 3)$, $(3, 2, 1)$, $(1, 2, 2)$, $(1, 2)$, $(2, 1, 2)$ are all different tuples
  - When $n = 2$ often called an "ordered pair"
- You often see tuples constructed from sets using Cartesian products
- The cartesian product of sets A and B, denoted $A \times B$, is the set of all ordered pairs (a, b) with $a \in A$ and $b \in B$.
  - E.g. $\{1, 2\} \times \{1, 3, 4\} = \{(1, 1), (1, 3), (1, 4), (2, 1), (2, 3), (2, 4)\}$
  - E.g. USC Students $\times$ USC Courses = Set of possible class enrollments
- Note: $|A \times B| = |A||B|$

Sequences

- Intuitively: A sequence is essentially a countably infinite tuple
  - Formally, it is a function from $\mathbb{N}$ to elements
- E.g. Fibonacci Sequence: $0, 1, 1, 2, 3, 5, 8, \ldots$
- E.g. The sequence $T(n)$ of worst-case runtimes
- A sequence is called a recurrence relation if it is defined recursively
  - E.g. Fibonacci, worst case runtime of Mergesort
- A closed form expression for a sequence is an elementary mathematical expression for the nth element of a sequence
  - We found a closed form expression for the runtime of Mergesort
  - There also is one for the Fibonacci sequence (look it up)
  - Not every sequence has a closed-form expression
  - “closed form” depends on what you allow in your expression

Outline

Relations

Definition

A Relation between sets A and B is some $R \subseteq A \times B$.

Example

- A is the set of USC Students
- B is the set of USC Courses
- $R = \{(a, b) \in A \times B$: student a is enrolled in class $b\}$

Functions

A function f from set A to set B takes as input a member of a, and outputs a member of b.

Formally

f is a relation between A and B where each $a \in A$ is related to exactly one $b \in B$.

- In other words, each $a \in A$ shows up exactly once in the relation.
- We use $f(a)$ to denote the output of f on a (i.e., the unique member of B which is related to a)
- When $b = f(a)$, we say b is the image of a under f.
- We say f is a map or mapping from A to B.
- We call A the domain and B the co-domain of f.
- The range of f is the set of possible outputs, which may or may not be the entire co-domain
    - range$(f) = \{f(a) : a \in A\}$.

Important Kinds of Functions

A function $f : A \to B$ is

- injective (a.k.a. one-to-one) if different inputs map to different outputs
  - Formally: $\forall x, y \in A \ \ (x \neq y \Rightarrow f(x) \neq f(y))$
  - In other words: Every $b \in B$ is the output of f on at most one $a \in A$.
- surjective (a.k.a. onto) if every allowed output is produced from some input
  - Formally: $\forall b \in B \ \exists a \in A \ \ f(a) = b$
  - In other words: Every $b \in B$ is the output of f on at least one $a \in A$.
  - In other words still: range = codomain
- bijective (a.k.a. one-to-one correspondance) if it is both injective and surjective
  - In other words: Every $b \in B$ is the output of f on exactly one $a \in A$.

Examples

- The function mapping USC students to their ID #s is injective, but not surjective onto the co-domain of 10 digit numbers
- $f : \mathbb{R} \to \mathbb{Z}$ defined by $f(x) = \lfloor x \rfloor$ is surjective but not injective
- The identity function on A, defined by $f(a) = a$, is bijective for any set A.
- The function $f : \mathbb{Z} \to Even$ defined by $f(x) = 2x$ is bijective

Composition

Definition

If $f : A \to B$ and $g : B \to C$ are functions, then their composition is the function $g \circ f : A \to C$ is the function mapping $a \in A$ to $g(f(a)) \in C$.

- In other words: Apply f first, then apply g to its output.
- Associative: $h \circ (g \circ f) = (h \circ g) \circ f$
  - Proof: $h((g \circ f)(x)) = h(g(f(x))) = (h \circ g)(f(x))$
  - So we omit the parenthesis and write $h \circ g \circ f$
- NOT usually commutative: $f(g(x)) \neq g(f(x))$
  - First of all, this doesn't even type check if $A \neq C$
  - But even when $A = B = C$ this isn't true: $(x+1)^2 \neq x^2 + 1$

Inverse of a Function

- If $f : A \to B$ is a bijection, then it has an inverse $f^{-1} : B \to A$.
  - $f^{-1}(b)$ is defined as the unique $a \in A$ such that $f(a) = b$.
- $f^{-1}(f(a)) = a$ for all $a \in A$, and $f(f^{-1}(b)) = b$ for all $b \in B$.
  - IOW: $f^{-1} \circ f$ is the identity function on A, and $f \circ f^{-1}$ is the identity function on B.

Inverse of a Function

- If $f : A \to B$ is a bijection, then it has an inverse $f^{-1} : B \to A$.
  - $f^{-1}(b)$ is defined as the unique $a \in A$ such that $f(a) = b$.
- $f^{-1}(f(a)) = a$ for all $a \in A$, and $f(f^{-1}(b)) = b$ for all $b \in B$.
  - IOW: $f^{-1} \circ f$ is the identity function on A, and $f \circ f^{-1}$ is the identity function on B.
- When $f : A \to B$ is just injective but not surjective, it is common to define f^{-1} : range$(f) \to A$ by first restricting the co-domain to the range (to make it surjective) then taking the inverse of that.

Outline

Single-Set Relations

Recall:

Definition

A Relation between sets A and B is some $R \subseteq A \times B$.

Single-Set Relations

Recall:

Definition

A Relation between sets A and B is some $R \subseteq A \times B$.

- We now look more closely at the special case when $A = B$. We call these Single-set Relations.
  - A single set relation on A is some $R \subseteq A \times A$
- Many relations you have encountered, and will continue to encounter, are on the same set
- We will look at order relations (e.g. $\leq, <, \subseteq, \subset$, big-$O$) and equivalence relations (e.g. $=$, $\equiv$, big-Θ)

Single-Set Relations

Recall:

Definition

A Relation between sets A and B is some $R \subseteq A \times B$.

- We now look more closely at the special case when $A = B$. We call these Single-set Relations.
  - A single set relation on A is some $R \subseteq A \times A$
- Many relations you have encountered, and will continue to encounter, are on the same set
- We will look at order relations (e.g. $\leq, <, \subseteq, \subset$, big-$O$) and equivalence relations (e.g. $=$, $\equiv$, big-Θ)

Infix Notation

Often it is convenient to use infix notation.

$$a \; R \; b \text{ means } (a, b) \in R$$

e.g. $a \leq b$, $a = b$

Properties of Single-set Relations

Here are some properties that a single-set relation R on A may or may not have:

- Reflexive: Every element is related to itself. Formally, $(x, x) \in R$ for all $x \in A$.
- Irreflexive: No element is related to itself. Formally, $(x, x) \notin R$ for all $x \in A$.

Properties of Single-set Relations

Here are some properties that a single-set relation R on A may or may not have:

- Reflexive: Every element is related to itself. Formally, $(x, x) \in R$ for all $x \in A$.
- Irreflexive: No element is related to itself. Formally, $(x, x) \notin R$ for all $x \in A$.
- Symmetric: All relationships are mutual. Formally, $(x, y) \in R \iff (y, x) \in R$ for all $a, b \in A$.
- Antisymmetric: No relationship between distinct elements is mutual. Formally, $(x, y) \in R \Rightarrow (y, x) \notin R$ for all $x, y \in A$ with $x \neq y$.

Properties of Single-set Relations

Here are some properties that a single-set relation R on A may or may not have:

- Reflexive: Every element is related to itself. Formally, $(x, x) \in R$ for all $x \in A$.
- Irreflexive: No element is related to itself. Formally, $(x, x) \notin R$ for all $x \in A$.
- Symmetric: All relationships are mutual. Formally, $(x, y) \in R \iff (y, x) \in R$ for all $a, b \in A$.
- Antisymmetric: No relationship between distinct elements is mutual. Formally, $(x, y) \in R \Rightarrow (y, x) \notin R$ for all $x, y \in A$ with $x \neq y$.
- Transitive: If x is related to y and y is related to z then x is also related to z. Formally, $(x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R$.

Properties of Single-set Relations

Here are some properties that a single-set relation R on A may or may not have:

- Reflexive: Every element is related to itself. Formally, $(x, x) \in R$ for all $x \in A$.
- Irreflexive: No element is related to itself. Formally, $(x, x) \notin R$ for all $x \in A$.
- Symmetric: All relationships are mutual. Formally, $(x, y) \in R \iff (y, x) \in R$ for all $a, b \in A$.
- Antisymmetric: No relationship between distinct elements is mutual. Formally, $(x, y) \in R \Rightarrow (y, x) \notin R$ for all $x, y \in A$ with $x \neq y$.
- Transitive: If x is related to y and y is related to z then x is also related to z. Formally, $(x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R$.
- Total: Every distinct pair of elements is related in at least one direction. Formally, $(x, y) \in R \vee (y, x) \in R$ for all $x, y \in A$ with $x \neq y$.

Order Relations

- A partial order is a single-set relation which is reflexive, antisymmetric, and transitive
  - E.g. $\leq$ on numbers, $\subseteq$ on sets, divisibility $|$ on integers
  - Sometimes calles weak partial order

Order Relations

- A partial order is a single-set relation which is reflexive, antisymmetric, and transitive
  - E.g. $\leq$ on numbers, $\subseteq$ on sets, divisibility $|$ on integers
  - Sometimes calles weak partial order
- A strict partial order is a single-set relation which is irreflexive, antisymmetric, and transitive
  - E.g. $<$ on numbers, $\subset$ on sets, little-o on functions, prerequisite on courses
  - Note: can be converted to partial order by adding all self-relations, and vice versa

Order Relations

- A partial order is a single-set relation which is reflexive, antisymmetric, and transitive
  - E.g. $\leq$ on numbers, $\subseteq$ on sets, divisibility $|$ on integers
  - Sometimes calles weak partial order
- A strict partial order is a single-set relation which is irreflexive, antisymmetric, and transitive
  - E.g. $<$ on numbers, $\subset$ on sets, little-o on functions, prerequisite on courses
  - Note: can be converted to partial order by adding all self-relations, and vice versa

Can be visualized by a directed acyclic graph (DAG)!

Order Relations

- A total order is a partial order which is also total.
  - Every pair of elements is comparable
  - e.g. $\leq$ on numbers, lexicographic (dictionary) order on strings, temporal order of events
  - Sometimes also called a weak total order

Order Relations

- A total order is a partial order which is also total.
  - Every pair of elements is comparable
  - e.g. $\leq$ on numbers, lexicographic (dictionary) order on strings, temporal order of events
  - Sometimes also called a weak total order
- A strict total order is a strict partial order which is also total.
  - Every pair of distinct elements is comparable
  - e.g. $<$ on numbers
  - Can be converted to weak total order by adding all self relations, and vice versa

Order Relations

- A total order is a partial order which is also total.
  - Every pair of elements is comparable
  - e.g. $\leq$ on numbers, lexicographic (dictionary) order on strings, temporal order of events
  - Sometimes also called a weak total order
- A strict total order is a strict partial order which is also total.
  - Every pair of distinct elements is comparable
  - e.g. $<$ on numbers
  - Can be converted to weak total order by adding all self relations, and vice versa

Can be visualized on a line.

Order Relations

- A total order is a partial order which is also total.
  - Every pair of elements is comparable
  - e.g. $\leq$ on numbers, lexicographic (dictionary) order on strings, temporal order of events
  - Sometimes also called a weak total order
- A strict total order is a strict partial order which is also total.
  - Every pair of distinct elements is comparable
  - e.g. $<$ on numbers
  - Can be converted to weak total order by adding all self relations, and vice versa

Can be visualized on a line.

Topological Ordering

A partial order (weak or strict) can be completed to a total order. For example, the order in which you take your classes, respecting pre-requisites, is a topological ordering of the prerequisite relation.

Equivalence Relations

Definition

An Equivalence Relation is a single-set relation which is reflexive, symmetric, and transitive.

These capture various notions of "equality"

Examples

- $=$ on numbers, sets, ...
- Getting the same grade in 170
- big-Θ on functions
- $\equiv$ on logical formulas
- Reachability in an undirected graph
- Congruence modulo k, on integers. Written $a \equiv b \pmod{k}$.
  - $a \equiv b \pmod{k}$ iff $k | (a - b)$

Equivalence Relations

Useful Fact

An equivalence relation $\approx$ on a set A partitions the set into equivalence classes, where $a \approx b$ iff they are in the same class.

Equivalence Relations

Useful Fact

An equivalence relation $\approx$ on a set A partitions the set into equivalence classes, where $a \approx b$ iff they are in the same class.

What are the equivalence classes in these examples?

Examples

- $=$ on numbers, sets, ...
- Getting the same grade in 170
- big-Θ on functions
- $\equiv$ on logical formulas
- Reachability in an undirected graph
- Congruence modulo k, on integers. Written $a \equiv b \pmod{k}$.
  - $a \equiv b \pmod{k}$ iff $k | (a - b)$