

CITS2211 DISCRETE STRUCTURES

1. Sets and counting

Reference: Sections 3.1–3.3 of Gersting.

Set notation

- A **set** is an unordered collection of objects with no duplicates
- The set is one of the fundamental concepts in Mathematics
 - set language is used widely to describe (collections of) objects
 - it is integral to describing and modeling systems

- We will use capital letters to denote sets
- $a \in A$ means that the object a is a member of the set A
 - $a \notin A = \text{not } (a \in A)$
- $A = B$ means that A and B have the same members
 - $A = B \leftrightarrow (\forall x)(x \in A \leftrightarrow x \in B)$
- The lack of an ordering means that $\{1, 2, 3\} = \{2, 3, 1\} = \{3, 2, 1\} = \dots$
 - note that this distinguishes a set from a sequence
- The absence of duplicates means that $\{1, 2\} = \{1, 2, 1\} = \{1, 2, 2\} = \{1, 2, 1, 2\} = \dots$
 - this also distinguishes a set from a sequence

- The **cardinality** of A is the number of members of A , denoted by $|A|$
- The empty set or **null set** has no members and is denoted by \emptyset or $\{\}$

Specifying a set

- There are four common ways of specifying a set A
 - e.g. the set of positive even integers

- List the members of A
 - $A = \{2, 4, 6, 8, \dots\}$
 - note that an infinite (or large) set can be specified with an ellipsis, as long as the pattern is clear

- Give a recursive definition
 - $2 \in A \wedge (\forall x)(x \in A \rightarrow x + 2 \in A)$

- Describe a property that characterises the members of A
 - $A = \{x \mid x \text{ is a positive even integer}\}$
 - this is called an **absolute set abstraction**
 - $A = \{x \mid P(x)\} \leftrightarrow (\forall x)(x \in A \leftrightarrow P(x))$

- Define the members of A relative to another set
 - $A = \{2x \mid x \in \mathbb{N}^+\}$
 - this is called a **relative set abstraction**
 - \mathbb{N}^+ is the set of positive integers
 - membership of A can also be limited with a condition
 - $A = \{x \mid x \in \mathbb{N}^+ \wedge x \bmod 2 = 0\}$

Subsets and power sets

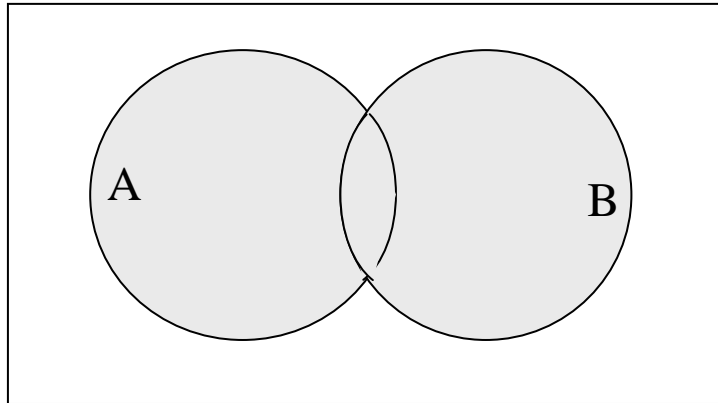
- $A \subseteq B$ means that A is a **subset** of B
 - all of the members of A are also members of B
 - $A \subseteq B \leftrightarrow (\forall x)(x \in A \rightarrow x \in B)$
- $A \subset B$ means that A is a **proper subset** of B
 - all of the members of A are members of B *and* there is at least one member of B that isn't a member of A
 - $A \subset B \leftrightarrow (\forall x)(x \in A \rightarrow x \in B) \wedge (\exists y)(y \in B \wedge y \notin A)$
- If A is a subset of B , then B is a **superset** of A , i.e. $B \supseteq A$

- Note that
 - $\emptyset \subseteq A$
 - $A \subseteq A$
 - $A = B \leftrightarrow (A \subseteq B \wedge B \subseteq A)$
 - $A = \{x \mid P(x)\} \wedge B = \{x \mid P(x) \wedge Q(x)\} \rightarrow A \supseteq B$
 - $A = \{x \mid P(x)\} \wedge B = \{x \mid P(x) \vee Q(x)\} \rightarrow A \subseteq B$

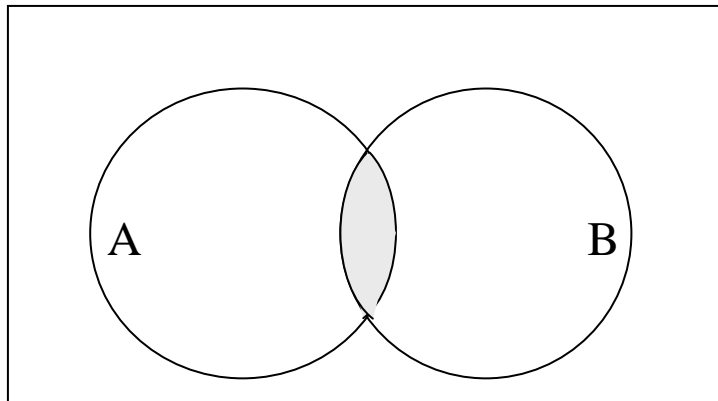
- The **power set** of A is the set containing all of the subsets of A , denoted by $\wp(A)$
 - $\wp(A) = \{B \mid B \subseteq A\}$
 - e.g. $\wp(\{4, 5\}) = \{\emptyset, \{4\}, \{5\}, \{4, 5\}\}$
- $|\wp(A)| = 2^n$, where $n = |A|$
 - for each $a \in A$ and $B \subseteq A$, either a is in B or it isn't

Combining sets

- Set operations and relationships can be visualised using Venn diagrams
- $A \cup B$ is the **union** of A and B
 - $A \cup B = \{x \mid x \in A \vee x \in B\}$

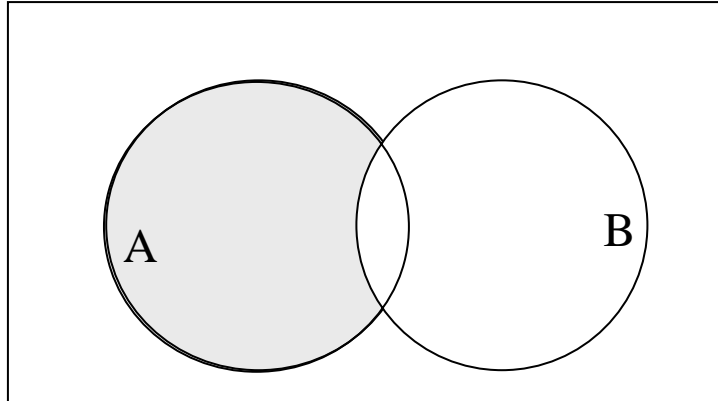


- $A \cap B$ is the **intersection** of A and B
 - $A \cap B = \{x \mid x \in A \wedge x \in B\}$
 - if $A \cap B = \phi$, A and B have no members in common and are said to be **disjoint**

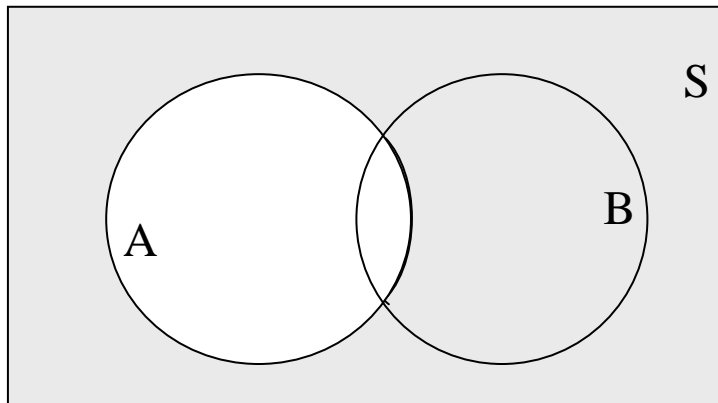


Combining sets

- $A - B$ is the **difference** between A and B
 - $A - B = \{x \mid x \in A \wedge x \notin B\}$



- Given $A \subseteq S$, A' is the **complement** of A relative to S
 - $A \subseteq S \rightarrow A' = \{x \mid x \in S \wedge x \notin A\} = S - A$



- $A \times B$ is the **Cartesian product** (or cross product) of A and B
 - $A \times B = \{(x, y) \mid x \in A \wedge y \in B\}$
 - e.g. $A = \{1, 2\}$, $B = \{3, 4\}$,
 $A \times B = \{(1, 3), (1, 4), (2, 3), (2, 4)\}$
 - note that (x, y) is an ordered pair
 - $(x, y) = (a, b) \leftrightarrow (x = a \wedge y = b)$
- $A^2 = A \times A$
 - this notation can be extended to A^n , $n > 0$

Set identities

- We can define many equivalences that hold for the set operations

1a. $A \cup B = B \cup A$ Commutativity

1b. $A \cap B = B \cap A$

2a. $(A \cup B) \cup C = A \cup (B \cup C)$ Associativity

2b. $(A \cap B) \cap C = A \cap (B \cap C)$

3a. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ Distributivity

3b. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

4a. $A \cup \phi = A$ Identity

4b. $A \cap S = A$

5a. $A \cup A' = S$ Complementarity

5b. $A \cap A' = \phi$

6a. $A \cup S = S$ Zero

6b. $A \cap \phi = \phi$

- Set equivalences have duals in the same way that equivalences in Boolean logic have duals
- replace \cup with \cap , and ϕ with S
 - or vice versa

Set equality

- There are two common ways of proving that two sets A and B are equal
 - indirectly, by proving $A \subseteq B \wedge B \subseteq A$
 - directly, using the set equivalences
- e.g. prove that $A \cup (A \cap B) = A$

□ Indirectly:

- to show $A \cup (A \cap B) \subseteq A$
 let $x \in A \cup (A \cap B)$
 $\therefore x \in A \vee x \in A \cap B$ Defn. of \cup
 $= x \in A \vee (x \in A \wedge x \in B)$ Defn. of \cap
 $= (x \in A \wedge \text{true}) \vee (x \in A \wedge x \in B)$ Identity of \wedge
 $= x \in A \wedge (\text{true} \vee x \in B)$ Distributivity
 $= x \in A \wedge \text{true}$ Zero of \vee
 $= x \in A$ Identity of \wedge
- to show $A \subseteq A \cup (A \cap B)$, reverse the above argument

□ Directly:

$$\begin{aligned}
 - \quad A \cup (A \cap B) &= (A \cap S) \cup (A \cap B) && (4b) \\
 &= A \cap (S \cup B) && (3b) \\
 &= A \cap (B \cup S) && (1a) \\
 &= A \cap S && (6a) \\
 &= A && (4b)
 \end{aligned}$$

Countable and uncountable sets

- A set is either finite or infinite
- An infinite set is either countably infinite (denumerable) or uncountably infinite
- An infinite set A is **countable** if we can define a mapping between the natural numbers and the members of A
 - this is called an **enumeration** of A

- Example: the set of even integers is countable
 - $f: \text{Nat} \rightarrow A$
 $f(n) = n, \text{ if } n \text{ is even}$
 $= -(n + 1), \text{ if } n \text{ is odd}$

- Example: the set of rational numbers is countable
 - assume that a rational number is a ratio of two positive integers m and n
 - $g: A \rightarrow \text{Nat}$
 $g(m/n) = ((m + n)^2 - (m + n)) / 2 - n$
 - Gersting has a more descriptive version of this proof

Countable and uncountable sets

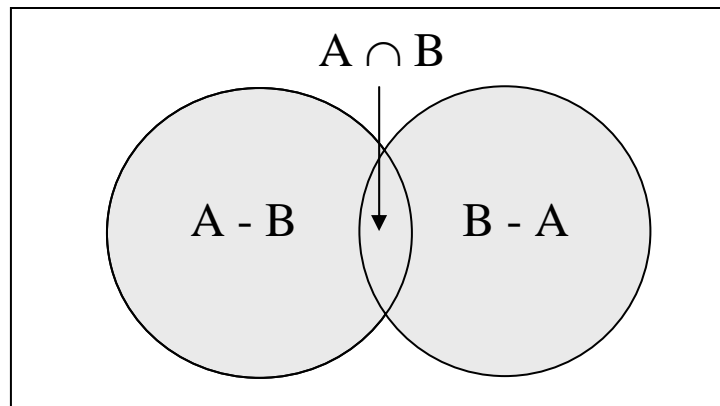
- Example: the set of real numbers in the interval $(0, 1)$ is **uncountable**
 - there is a famous proof by contradiction using Cantor's diagonalisation method
 - assume that the set is complete and countable and that the i^{th} element of the enumeration, d_i , can be written uniquely in the form $0.d_{i1}d_{i2}d_{i3}\dots$
 - construct a new number $p = 0.p_1p_2p_3\dots$ as follows
$$p_i = 5, \text{ if } d_{ii} \neq 5$$
$$= 6, \text{ if } d_{ii} = 5$$
 - $0 < p < 1 \wedge (\forall i)(p \text{ is different from } d_i)$
 - therefore p is not in the set: a contradiction!

Counting: the multiplication and addition principles

- We often want to count the members of a finite set
 - we have several principles that we can use to reduce the problem of counting a complex set into the problem of counting simpler sets
- If there are n_1 possible outcomes for an event A and n_2 possible outcomes for an event B , there are $n_1 n_2$ possible outcomes for the sequence of the events $A B$
 - this is known as the **multiplication principle**
- By the multiplication principle,
 $|A \times B| = |A| |B|$
 $|A^n| = |A|^n$
- If there are n_1 possible outcomes for an event A and n_2 possible outcomes for an event B that is disjoint with A , there are $n_1 + n_2$ possible outcomes for the event A or B
 - this is known as the **addition principle**
- By the addition principle,
 A, B disjoint $\rightarrow |A \cup B| = |A| + |B|$
- Both of these principles can be extended using induction to m events, $m \geq 2$
- Instances of these principles can be illustrated with **decision trees**
 - e.g. how many four-digit binary strings are there?
- Decision trees can also account for the situation where choices depend on previous choices
 - e.g. how many four-digit binary strings are there if we disallow consecutive 1s?

Counting: the principle of inclusion and exclusion

- Consider the Venn diagram for $A \cup B$
 - $A \cup B = (A - B) \cup (A \cap B) \cup (B - A)$
 - $A - B$, $A \cap B$, and $B - A$ are pairwise disjoint
 - $\therefore |A \cup B| = |A - B| + |A \cap B| + |B - A|$



- But $A = (A - B) \cup (A \cap B)$
 - $\therefore |A| = |A - B| + |A \cap B|$
 - $\therefore |A - B| = |A| - |A \cap B|$
and $|B - A| = |B| - |B \cap A|$
- $\therefore |A \cup B| = |A - B| + |A \cap B| + |B - A|$
 $= |A| + |B| - |A \cap B|$
 - this is known as the **principle of inclusion and exclusion**

- This can be extended to n sets, $n \geq 2$
- For three sets:
$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$
- For n sets, see Gersting

Counting: the pigeonhole principle

- If we place n items into k bins, $n > k$, at least one bin will contain more than one item
 - this is known as the **pigeonhole principle**

- e.g. how many times must a die be rolled to guarantee getting the same number twice?
 - the 6 possibilities on each roll correspond to 6 bins, therefore we need a minimum of 7 rolls

- e.g. prove that two people living in Perth have the same (non-zero!) number of hairs on their head
 - a person can have up to 500,000 hairs on their head, corresponding to 500,000 bins. 1,400,000 people live in Perth, therefore ...

- e.g. prove that if four distinct numbers are chosen from the set $\{1, 2, 3, 4, 5, 6\}$, at least one pair must add up to 7
 - there are three pairs that add up to 7, corresponding to three bins. $4 > 3$, therefore we must choose at least one complete pair

A short primer on propositional logic

- Atomic statements are denoted by capitals A, B, C , etc
- The set of **well-formed formulas (wffs)** is defined recursively by
 - every atomic statement is a wff
 - if P and Q are wffs, then the following are also wffs

P'	negation (not)
$P \wedge Q$	conjunction (and)
$P \vee Q$	disjunction (or)
$P \rightarrow Q$	implication (necessity/sufficiency, if)
$P \leftrightarrow Q$	equivalence (equals, iff)
(P)	parenthesis

- the operators given above are in descending order of syntactic precedence

A short primer on predicate logic

- A **predicate** is essentially a Boolean-valued function
- The set of **predicate well-formed formulas (predicate wffs)** is again defined recursively
- A simple statement is an application of a predicate

e.g. $P(x, y, z)$

- A compound statement is an application of a logical operator

pls_1'	negation (not)
$pls_1 \wedge pls_2$	conjunction (and)
$pls_1 \vee pls_2$	disjunction (or)
$pls_1 \rightarrow pls_2$	implication (necessity/sufficiency, if)
$pls_1 \leftrightarrow pls_2$	equivalence (equals, iff)

- The operators are in descending order of precedence
- A quantified statement is an application of a quantifier

$(\forall x)(pls_1)$	for all x , pls_1 is true
$(\exists y)(pls_1)$	there exists at least one y for which pls_1 is true

- A parenthesised statement is a statement in brackets

(pls_1)

- pls_1 and pls_2 are any predicate wffs