Session Objectives

- Describe the role of formal methods in Computer Science
- Define sets and the main set operations
- Use Venn diagrams and compute with set algebra

Formal Methods

- Formal methods are the way in which mathematicians reason about the very foundations of mathematics: logic, how mathematical arguments are constructed, and set theory, how mathematical objects are put together.
- While mathematicians use set and logic notation a lot, they don't use formal proofs very often. Formal methods are very time consuming and bulky to use for proofs of any reasonable size.
- If you want a computer to reason (draw logical deductions, manipulate sets) you either have to program it to work as rigorously as a mathematician in an informal way (which is very difficult) or you have to program it to apply the rules of logic (which is relatively easy).
- Indeed, computers have been used to check formal proofs, as they are better at doing it than people.

Set Theory

- Set theory provides the foundation for all of mathematics.
- There is no formal definition of sets; this is unavoidable, since in any logical structure we must start with some basic concepts that cannot be defined in terms of other concepts.
- In fact, in formal set theory, sets are defined in terms of what are called classes, but classes themselves are undefined
- For our purposes, a set is a collection of items, no two of which are the same.
- If x is a member (also known as an element) of a set S, we write $x \in S$; we generally use upper case letters to denote sets and lower case letters to denote elements.

Definition in Extension

- We can define a set by displaying all of its elements enclosed in braces (curly brackets). This is called definition in extension. For example, the set of English vowels is {a, e, i, o, u, y}.
- Two sets A and B are equal if and only if they contain exactly the same elements. There is no notion of ordering, so

$$\{a, e, i, o, u, y\} = \{e, o, y, u, i, a\}.$$

- For larger sets, for which it is too time-consuming to list all of the elements, we may use dots, ..., to indicate elements left out of the list.
- The problem with this is that there may well be ambiguity over exactly what set is intended.

Definition in Comprehension

- We can define a set unambiguously in comprehension.
- We use a predicate $P(x)$, which is an expression that is true or false for any element x and a set A.
- Then there is a set whose elements are those members of A which satisfy the predicate P (i.e., elements x for which $P(x)$ is true).
- We denote this set by $\{x \in A \mid P(x)\}$ or by $\{x \in A : P(x)\}$.

Examples

1. Let $P(x)$ be the predicate 'x lives in Birmingham' and H the set of all living human beings. Then $\{x \in H \mid P(x)\}$ is the set of all human inhabitants of Birmingham.
2. Let $\mathbb{R}$ be the set of real numbers, and let the predicate $Q(y)$ be $y > 0$. Then
$$\mathbb{R}^+ = \{y \in \mathbb{R} \mid Q(y)\} = \{y \in \mathbb{R} \mid y > 0\}$$
is the set of positive real numbers.

Note that the definition of a set is in no way unique. For example, the following three sets are the same:

$$A = \{0, 1\} \qquad B = \{x \in \mathbb{R} \mid x^2 - x = 0\} \qquad C = \{y \in \mathbb{N} \mid y < 2\} \tag{1}$$

The Empty and the Universal Set

- The special set which has no members is called the empty set, written $\emptyset$.
- This often plays a similar role to 0 in set algebra.
- However, it is not the same as $\{0\}$, which is a set with a single element (equal to the number zero).
- With care, in any particular application we may define a set of all elements we are interested in, which is often called the universal set (for that particular application). We shall write such a set as U.

Exercise

Define the following sets $\{x \in A \mid P(x)\}$ explicitly (in extension):

1. $\{x \in \mathbb{N} \mid x < 5\} =$
2. A is the days of the week and $P(x)$ is 'x is after Thursday and before Sunday'.
3. $\{x \in \mathbb{R} \mid x^2 < 0\} =$

Solution

1. $\{x \in \mathbb{N} \mid x < 5\} = \{0, 1, 2, 3, 4\}$
2. A is the days of the week and $P(x)$ is 'x is after Thursday and before Sunday'.

$$A = \{\text{Friday}, \text{Saturday}\}.$$

3. $\{x \in \mathbb{R} \mid x^2 < 0\} = \emptyset$

Subsets

- A set A is said to be a subset of B, or A is contained in B, if every element of A is also an element of B. That is, whenever $x \in A$ then $x \in B$. This is written $A \subseteq B$.
- For example, if $A = \{1, 2, 3\}$ and $B = \{1, 2, 3, 6, 7\}$, then $A \subseteq B$.
- We say that A is a proper subset of B, or A is strictly contained in B, if A is a subset of B but is not equal to B. So, in the above example $A \subset B$.

Set Hierarchies

- We must distinguish sets and their members. For example $3 \in \{1, 2, 3\}$ but $\{3\} \notin \{1, 2, 3\}$. Here $\{3\}$ is a set whose only member is 3, so it is s subset of $\{1, 2, 3\}$, but not a member.
- A set may have other sets as its elements. This arises often in hierarchies.
- The set C of all BSc Computer Science students at Aston has four members: the first year, second year, placement year, and final year. So

$$C = \{CS1, CS2, CSP, CSF\}. \tag{2}$$

But each of the elements of C is itself a set, consisting of the students in the corresponding year. For example,

$$CS1 = \{\text{Adam Aardvark}, \text{Prunella Armstrong}, \ldots, \text{Minesh Zanzibar}\}. \tag{3}$$

Intersection

- If A and B are sets then their intersection $A \cap B$ is the set of all elements that belong to both A and B:

$$A \cap B = \{z \mid z \in A \quad \text{and} \quad z \in B\}. \tag{4}$$

  This is a subset of both A and B.

- $$\{n \in \mathbb{N} \mid n \text{ even}\} \cap \{n \in \mathbb{N} \mid n \text{ a multiple of } 3\}$$
$$= \{n \in \mathbb{N} \mid n \text{ is a multiple of } 6\}.$$

- We say that A and B are disjoint if their intersection is the empty set. The sets $\{1, 3, 5\}$ and $\{2, 4, 6\}$ are disjoint.

Union

- If A and B are sets then their union $A \cup B$ is the set of all elements that belong to either A or B:

$$A \cup B = \{z \mid z \in A \quad \text{or} \quad z \in B\}. \tag{5}$$

- Both A and B are subsets of $A \cup B$. For example,

$$\{a, b, c, d, e\} \cup \{b, d, f\} = \{a, b, c, d, e, f\}.$$

Difference and Complement

- If A and B are sets then their difference $A \setminus B$ (sometimes written $A - B$) is the set of elements of A which are not in B:

$$A \setminus B = \{z \mid z \in A \quad \text{and} \quad z \notin B\}. \tag{6}$$

For example:

$$\{a, b, c, d, e\} \setminus \{b, d, f\} = \{a, c, e\}.$$

- If A is a set and U is a universal set, then the complement A' of A is the set of elements of U that are not in A (so A' is equivalent to $U \setminus A$):

$$A' = U \setminus A = \{x \in U \mid x \notin A\}. \tag{7}$$

Cardinality

- The number of members of a set A is called the cardinality of A and is written $|A|$ or sometimes $\#A$.
- Although this seems only to make sense if A is finite, in mathematical set theory it is possible to define the cardinality of infinite sets. Although this cardinality is well-defined, it has some counter-intuitive properties.
- One important result is the $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$ are all countably infinite.
- They all have the same cardinality, even though $\mathbb{Z}$ seems to contain twice as many elements as $\mathbb{N}$. I did say that infinite cardinals were counter-intuitive!
- $\mathbb{R}$ is uncountably infinite and has more elements than the other sets.

Power Set

- The set of all subsets of a set A is called its power set, and is written $\mathcal{P}(A)$.
- For example, if $A = \{1, 2, 3\}$ then

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

- The subsets have been listed in order of the number of elements they contain: one subset with 0 elements, 3 with 1 element, 3 with 2 elements and one with 3 elements.
- We note that the cardinality of $\mathcal{P}(A)$ is $2^3 = 8$ elements.
- In general, if A contains n elements, then $\mathcal{P}(A)$ contains 2^n elements.

Exercise

1. Let U be the set of natural numbers from 0 up to 10 inclusive. Let $A = \{1, 4, 6, 8, 9\}$ and $B = \{0, 2, 3, 6, 7, 9\}$. Find $A \cup B$, $A \cap B$, $A \setminus B$, $B \setminus A$ and A'.

2. Let U be the set of natural numbers, A the set of even integers and B the set of odd integers. Find $A \cup B$, $A \cap B$, A' and B'. Are A and B disjoint?

Solution

1. $U = \{n \in \mathbb{N} \mid n \leq 10\}$, $A = \{1, 4, 6, 8, 9\}$ and $B = \{0, 2, 3, 6, 7, 9\}$.

$$A \cup B = \{0, 1, 2, 3, 4, 6, 7, 8, 9\}.$$

$$A \cap B = \{6, 9\} \qquad A' = \{0, 2, 3, 5, 7, 10\}$$

$$A \setminus B = \{1, 4, 8\} \qquad B \setminus A = \{0, 2, 3, 7\}$$

2. $U = \mathbb{N}$, $A = \{n \in \mathbb{N} \mid n = 2m, m \in \mathbb{N}\}$ and
$B = \{n \in \mathbb{N} \mid n = 2m + 1, m \in \mathbb{N}\}$.

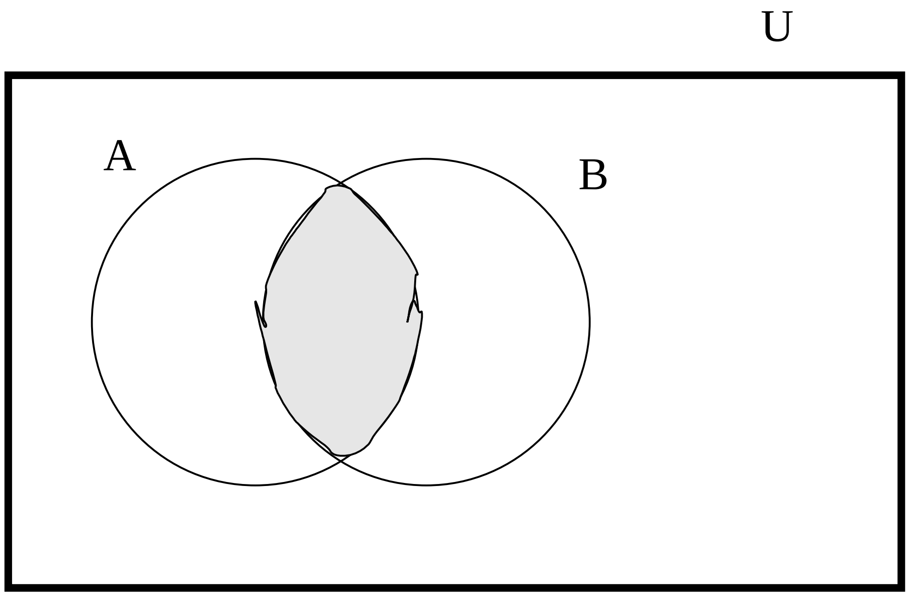
$$A \cup B = \mathbb{N} \qquad A' = B$$

$$A \cap B = \emptyset \qquad B' = A$$

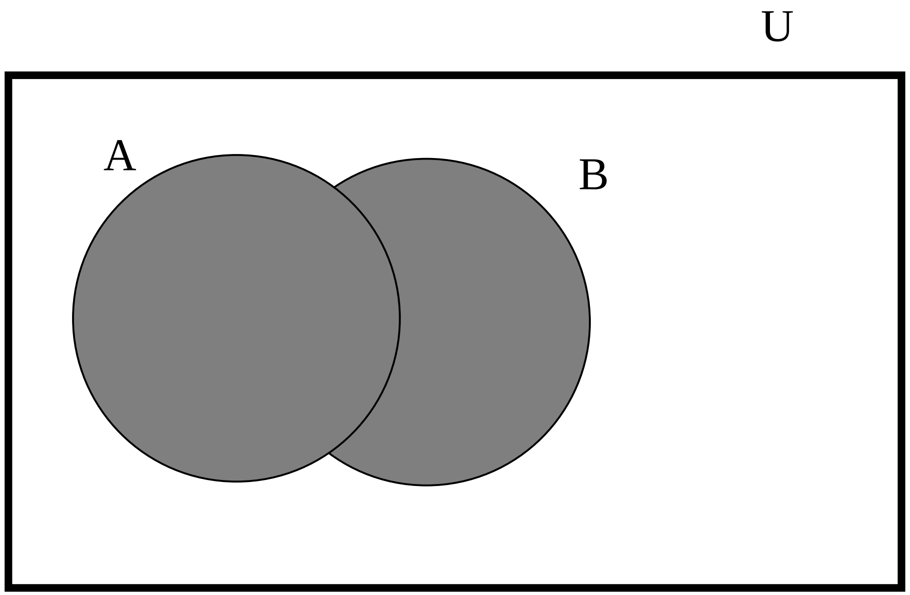
A and B are disjoint.

Venn Diagrams

Venn diagrams are not a substitute for formal proofs but are an aid to understanding.



Intersection



Union

Exercise

Draw Venn diagrams of

1. $A \setminus B$,
2. $A \subseteq B$.

Operator Properties

Commutative This means that the order of arguments to operators can be reversed.

$$A \cap B = B \cap A \qquad A \cup B = B \cup A. \tag{8}$$

Associative This means that the order of computing multiple operators is immaterial.

$$A \cap (B \cap C) = (A \cap B) \cap C \qquad A \cup (B \cup C) = (A \cup B) \cup C. \tag{9}$$

Distributive This means that we can expand out mixed brackets (compare with multiplication and addition of numbers).

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \qquad A \cup (B \cap C) = (A \cup B) \cap (A \cup C). \tag{10}$$

De Morgan's Laws These relate intersection, union and set difference.

$$A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C) \qquad (B \cap C)' = B' \cup C' \tag{11}$$

$$A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C) \qquad (B \cup C)' = B' \cap C' \tag{12}$$

Summary

1. A set is a collection of items, no two of which are the same.
2. Sets may be defined in extension (by listing the elements) or by comprehension (by giving a predicate that the elements satisfy).
3. The empty set $\emptyset$ has no members.
4. Set algebra defines intersection, union, set difference, complement, cardinality and the power set.
5. Venn diagrams help clarify relations between sets, but are not a substitute for proof.
6. Set operators may satisfy rules such as commutativity, associativity, distributivity, and De Morgan's laws.

Session Objectives

- Describe the role of formal methods in Computer Science
- Define sets and the main set operations
- Use Venn diagrams and compute with set algebra