Chapter 2

Sets and Logic

This chapter introduces sets. In it we study the structure on subsets of a set, operations on subsets, the relations of inclusion and equality on sets, and the close connection with propositional logic.

2.1 Sets

A *set* (or class) is an (unordered) collection of objects, called its *elements* or *members*. We write $a \in X$ when a is an element of the set X. We read $a \in X$ as "a is a member of X" or "a is an element of X" or "a belongs to X", or in some contexts as just "a in X". Sometimes we write *e.g.* $\{a, b, c, \cdots\}$ for the set of elements $a, b, c, \cdots$. Some important sets:

$\emptyset$ the empty set with no elements, sometimes written $\{\ \}$. (Contrast the empty set $\emptyset$ with the set $\{\emptyset\}$ which is a singleton set in the sense that it has a single element, *viz.* the empty set.)

$\mathbb{N}$ the set of natural numbers $\{1, 2, 3, \cdots\}$.

$\mathbb{N}_0$ the set of natural numbers with zero $\{0, 1, 2, 3, \cdots\}$. (This set is often called ω.)

$\mathbb{Z}$ the set of integers, both positive and negative, with zero.

$\mathbb{Q}$ the set of rational numbers.

$\mathbb{R}$ the set of real numbers.

In computer science we are often concerned with sets of strings of symbols from some alphabet, for example the set of strings accepted by a particular automaton.

A set X is said to be a *subset* of a set Y, written $X \subseteq Y$, iff every element of X is an element of Y, *i.e.*

$$X \subseteq Y \iff \forall z \in X.\ z \in Y.$$

Synonymously, then we also say that X is *included* in Y.

A set is determined solely by its elements in the sense that two sets are equal iff they have the same elements. So, sets X and Y are equal, written $X = Y$, iff every element of A is a element of B and *vice versa*. This furnishes a method for showing two sets X and Y are equal and, of course, is equivalent to showing $X \subseteq Y$ and $Y \subseteq X$.

Sets and properties

Sometimes a set is determined by a property, in the sense that the set has as elements precisely those which satisfy the property. Then we write

$$X = \{x \mid P(x)\},$$

meaning the set X has as elements precisely all those x for which the property $P(x)$ is true. If X is a set and $P(x)$ is a property, we can form the set

$$\{x \in X \mid P(x)\}$$

which is another way of writing

$$\{x \mid x \in X\ \&\ P(x)\}.$$

This is the subset of X consisting of all elements x of X which satisfy $P(x)$.

When we write $\{a_1, \cdots, a_n\}$ we can understand this as the set

$$\{x \mid x = a_1 \text{ or } \cdots \text{ or } x = a_n\} .$$

Exercise 2.1 This question is about strings built from the symbols a's and b's.
For example aab, $ababaaa$, etc. are strings, as is the empty string ε.

(i) Describe the set of strings x which satisfy

$$ax = xa .$$

Justify your answer.

(ii) Describe the set of strings x which satisfy

$$ax = xb .$$

Justify your answer. □

2.2 Set laws

2.2.1 The Boolean algebra of sets

Assume a set U. Subsets of U support operations closely related to those of logic. The key operations are

Union	$A \cup B = \{x \mid x \in A \text{ or } x \in B\}$
Intersection	$A \cap B = \{x \mid x \in A \ \& \ x \in B\}$
Complement	$A^c = \{x \in U \mid x \notin A\}$.

Notice that the complement operation makes sense only with respect to an understood 'universe' U. A well-known operation on sets is that of set difference $A \setminus B$ defined to be $\{a \in A \mid a \notin B\}$; in the case where A and B are subsets of U set difference $A \setminus B = A \cap B^c$. Two sets A and B are said to be *disjoint* when $A \cap B = \emptyset$, so they have no elements in common.

Exercise 2.2 Let $A = \{1, 3, 5\}$ and $B = \{2, 3\}$. Write down explicit sets for:

(i) $A \cup B$ and $A \cap B$.

(ii) $A \setminus B$ and $B \setminus A$.

(iii) $(A \cup B) \setminus B$ and $(A \setminus B) \cup B$. □

The operations $\cup$ and $\cap$ are reminiscent of sum and multiplication on numbers, though they don't satisfy quite the same laws, *e.g.* we have $A \cup A = A$ generally while $a + a = a$ only when a is zero. Just as the operations sum and multiplication on numbers form an algebra so do the above operations on subsets of U. The algebra on sets and its relation to logical reasoning were laid bare by George Boole (1815-1864) in his "Laws of thought," and are summarised below. The laws take the form of algebraic identities between set expressions. (An algebra with operations $\cup, \cap$, and $(-)^c$ satisfying these laws is called a *Boolean algebra*.) Notice the laws $A \cup \emptyset = A$ and $A \cap U = A$ saying that $\emptyset$ and U behave as units with respect to the operations of union and intersection respectively.

The Boolean identities for sets: Letting A, B, C range over subsets of U,

Associativity	$A \cup (B \cup C) = (A \cup B) \cup C$	$A \cap (B \cap C) = (A \cap B) \cap C$
Commutativity	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Idempotence	$A \cup A = A$	$A \cap A = A$
Empty set	$A \cup \emptyset = A$	$A \cap \emptyset = \emptyset$
Universal set	$A \cup U = U$	$A \cap U = A$
Distributivity	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Absorption	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$
Complements	$A \cup A^c = U$	$A \cap A^c = \emptyset$
	$(A^c)^c = A$	
De Morgan's laws	$(A \cup B)^c = A^c \cap B^c$	$(A \cap B)^c = A^c \cup B^c$.

To show such algebraic identities between set expressions, one shows that an element of the set on the left is an element of the set on the right, and *vice versa*. For instance suppose the task is to prove

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

for all sets A, B, C. We derive

$$\begin{aligned} x \in A \cap (B \cup C) &\iff x \in A \text{ and } (x \in B \cup C) \\ &\iff x \in A \text{ and } (x \in B \text{ or } x \in C) \\ &\iff (x \in A \text{ and } x \in B) \text{ or } (x \in A \text{ and } x \in C) \\ &\iff x \in A \cap B \text{ or } x \in A \cap C \\ &\iff x \in (A \cap B) \cup (A \cap C) \ . \end{aligned}$$

The 'dual' of the identity is

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

To prove this we can 'dualize' the proof just given by interchanging the symbols $\cup, \cap$ and the words 'or' and 'and.' There is a duality principle for sets, according to which any identity involving the operations $\cup, \cap$ remains valid if the symbols $\cup, \cap$ are interchanged throughout. We can also prove the dual of identities directly, just from the laws of sets, making especial use of the De Morgan laws. For example, once we know

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

for all sets A, B, C we can derive its dual in the following way. First deduce that

$$A^c \cap (B^c \cup C^c) = (A^c \cap B^c) \cup (A^c \cap C^c) \ ,$$

for sets A, B, C. Complementing both sides we obtain

$$(A^c \cap (B^c \cup C^c))^c = ((A^c \cap B^c) \cup (A^c \cap C^c))^c \ .$$

Now argue by De Morgan's laws and laws for complements that the left-hand-side is

$$\begin{aligned} (A^c \cap (B^c \cup C^c))^c &= (A^c)^c \cup ((B^c)^c \cap (C^c)^c) \\ &= A \cup (B \cap C) \ , \end{aligned}$$

while the right-hand-side is

$$\begin{aligned}((A^c \cap B^c) \cup (A^c \cap C^c))^c &= (A^c \cap B^c)^c \cap (A^c \cap C^c)^c \\ &= ((A^c)^c \cup (B^c)^c) \cap ((A^c)^c \cup (C^c)^c) \\ &= (A \cup B) \cap (A \cup C) \ .\end{aligned}$$

We have deduced the dual identity

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

Exercise 2.3 Prove the remaining set identities above. □

The set identities allow deductions like those of school algebra. For example, we can derive

$$U^c = \emptyset \qquad\qquad \emptyset^c = U \ .$$

To derive the former, using the Universal-set and Complements laws:

$$U^c = U^c \cap U = \emptyset \ ,$$

Then by Complements on this identity we obtain $\emptyset^c = U$.

Using the Distributive laws and De Morgan laws with the Idempotence and Complements laws we can derive standard forms for set expressions. Any set expression built up from basic sets can be transformed to a union of intersections of basic sets and their complements, or alternatively as an intersection of unions of basic sets and their complements, *e.g.*:

$$\cdots \cup (A_1^c \cap A_2 \cap \cdots \cap A_k) \cup \cdots$$
$$\cdots \cap (A_1^c \cup A_2 \cup \cdots \cup A_k) \cap \cdots$$

The method is to first use the De Morgan laws to push all occurrences of the complement operation inwards so it acts just on basic sets; then use the Distributive laws to bring unions (or alternatively intersections) to the top level. With the help of the Idempotence and Complements laws we can remove redundant occurrences of basic sets. The standard forms for set expressions reappear in propositional logic as *disjunctive* and *conjunctive normal forms* for propositions.

Exercise 2.4 Using the set laws transform $(A \cap B)^c \cap (A \cup C)$ to a standard form as a union of intersections. □

The Boolean identities hold no matter how we interpret the basic symbols as sets. In fact, any identity, true for all interpretations of the basic symbols as sets, can be deduced from Boole's identities using the laws you would expect of equality; in this sense the Boolean identities listed above are *complete*.

Although the Boolean identities concern the equality of sets, they can also be used to establish the inclusion of sets because of the following facts.

Proposition 2.5 *Let A and B be sets. Then,*

$$A \subseteq B \iff A \cap B = A \ .$$

Proof. *"only if"*: Suppose $A \subseteq B$. We have $A \cap B \subseteq A$ directly from the definition of intersection. To show equality we need the converse inclusion. Let $x \in A$. Then $x \in B$ as well, by supposition. Therefore $x \in A \cap B$. Hence, $A \subseteq A \cap B$. *"if"*: Suppose $A \cap B = A$. Then $A = A \cap B \subseteq B$. □

Exercise 2.6 Let A and B be sets. Prove $A \subseteq B \iff A \cup B = B$. □

Proposition 2.7 *Let $A, B \subseteq U$. Then,*

$$A \subseteq B \iff A^c \cup B = U \ .$$

Proof. Let $A, B \subseteq U$. Then,

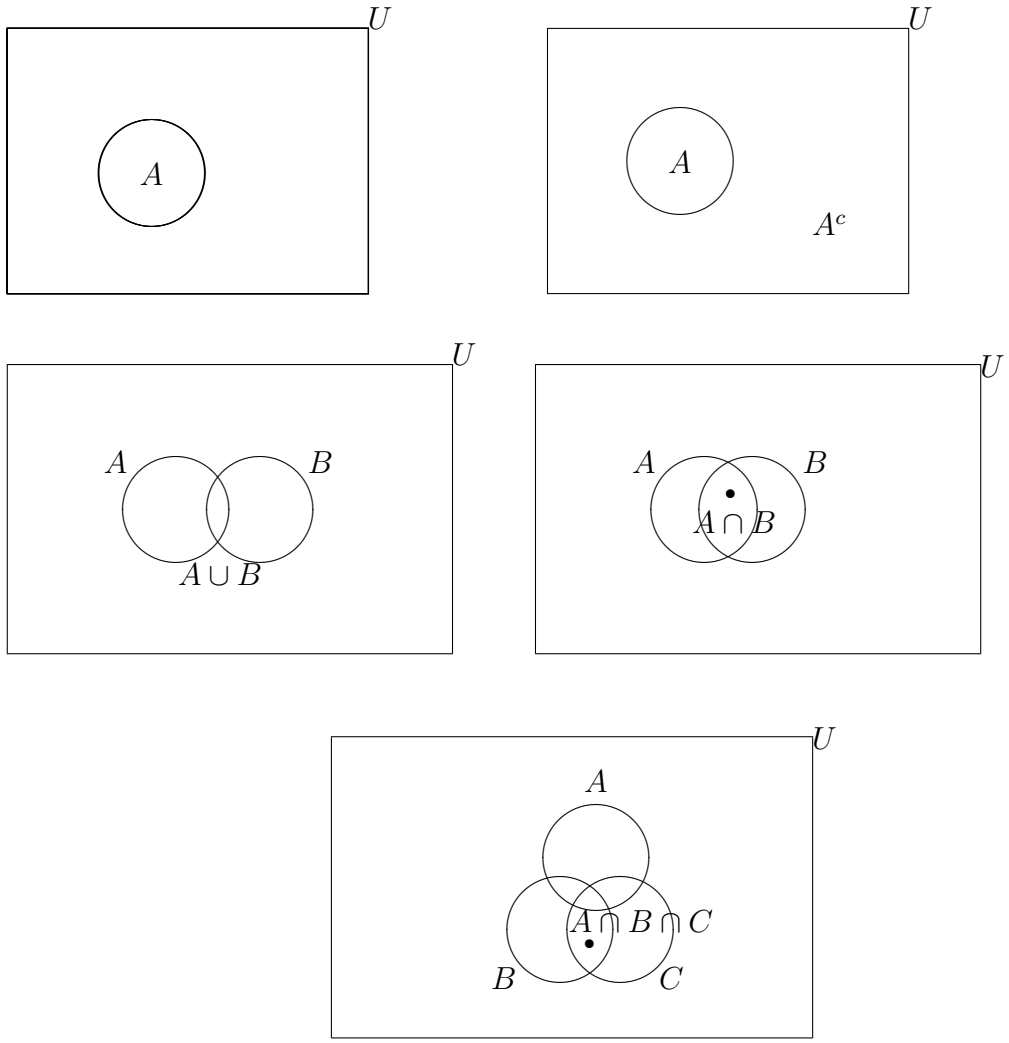
$$\begin{aligned}A \subseteq B &\iff \forall x \in U.\ x \in A \Rightarrow x \in B \\ &\iff \forall x \in U.\ x \notin A \text{ or } x \in B \\ &\iff \forall x \in U.\ x \in A^c \cup B \\ &\iff A^c \cup B = U \ .\end{aligned}$$

□

Exercise 2.8 Let $A, B \subseteq U$. Prove that $A \subseteq B \iff A \cap B^c = \emptyset$. □

2.2.2 Venn diagrams

When an expression describing a set is small it can be viewed pictorially as a *Venn diagram*[1] in which sets are represented as regions in the plane. In each diagram below the outer rectangle represents the universe U and the circles the sets A, B, C.



Exercise 2.9 Describe the set $A \cup B \cup C$ as a union of 7 disjoint sets (*i.e.*, so each pair of sets has empty intersection). □

Exercise 2.10 In a college of 100 students, 35 play football, 36 row and 24 play tiddlywinks. 13 play football and row, 2 play football and tiddlywinks but never row, 12 row and play tiddlywinks, while 4 practice all three activities. How many students participate in none of the activities of football, rowing and tiddlywinks? □

2.2.3 Boolean algebra and properties

A property $P(x)$ where $x \in U$ determines a subset of U, its *extension*, the set $\{x \in U \mid P(x)\}$. For instance U might be the set of integers $\mathbb{Z}$, when a suitable property could be "x is zero" or " x is a prime number"; the extension of the first property is the singleton set $\{0\}$, while the extension of the second is the set of primes. In many computer science applications U is a set of program states and then properties can specify the values stored in certain locations: for example "state x has value 3 in location Y and 5 in location Z." Alternatively U might consist of all the inhabitants of a country when properties of interest could be those of a census, specifying for example sex, age, household.

[1] After John Venn (1834-1923).

Logical operations on properties are paralleled by Boolean operations on their extensions as sets:

Property	Its extension as a set
$P(x)$	$\{x \in U \mid P(x)\}$
$Q(x)$ & $R(x)$	$\{x \in U \mid Q(x)\} \cap \{x \in U \mid R(x)\}$
$Q(x)$ or $R(x)$	$\{x \in U \mid Q(x)\} \cup \{x \in U \mid R(x)\}$
$\neg P(x)$	$\{x \in U \mid P(x)\}^c$
$Q(x) \Rightarrow R(x)$	$\{x \in U \mid Q(x)\}^c \cup \{x \in U \mid R(x)\}$

We can think of the meaning (or semantics) of a property as being the set which is its extension. Then logical operations on properties correspond to Boolean operations on sets. Two properties being equivalent corresponds to them having the same extension. The relation of entailment between properties corresponds to the relation of inclusion between sets. We can reason about properties by reasoning about sets.