Sets

Sets are a basic data structure of mathematics.

Informally a set is simply a (well-defined) collection of objects.

Well-known examples of sets from mathematics include the set of integers, the set of rational numbers, the set of real numbers, etc. In computer science one often needs to deal with sets of (finite-length) strings, e.g., bitstrings, or sets of expressions that are well-formed according to certain syntax rules.

While the concept of sets is deceptively simple, all mathematical objects can, in principle at least, be described or defined in terms of sets. In that sense sets are the basic building blocks for constructing mathematical (i.e., formal, abstract) objects.

We will discuss key components of the theory of sets and later on explore various applications of sets to computing.

Sets and Elements

Two basic concepts of set theory are the notion of a *set* and the *element relationship*.

We use the symbol $\in$ to denote the element relation and write

$$x \in A$$

to denote the proposition that x *is an element of* A (which may be true or false for specific choices of x and A).

It is customary to denote sets by capital letters, such as A, B, and C, and elements by small letters, such as x, y, and z. But this can sometimes be confusing, for as we shall see sets can themselves be elements of other sets!

Description of Sets

A *finite* set can (in principle) be described by listing its elements. For instance, we write

$$\{x_1, \ldots, x_n\}$$

to denote the set consisting of elements $x_1, \ldots, x_n$.

For example, the set

$$A = \{a, \{1\}, b, 1\}$$

has four elements and the statements

$$a \in A, \{1\} \in A, b \in A, \text{ and } 1 \in A$$

are all true.

Note that

1. sets can be elements of other sets: the set $\{1\}$ is an element of A; and

2. the set $\{A\}$ contains *one* element (whereas A has four elements), so that $A \in \{A\}$ and $A \neq \{A\}$.

A similar notation as above is often used for *infinite sets* as well, e.g., when one denotes describes the set of natural numbers by

$$\mathbf{N} = \{0, 1, 2, 3, \ldots\}$$

or the set of odd natural numbers by

$$\{1, 3, 5, \ldots\}.$$

But the use of ellipsis imparts a certain degree of vagueness, and we will discuss a more formal way of defining the set of natural numbers in set theory.

Equality

Two sets A and B are said to be *equal*, written $A = B$, if, and only if, they have the same elements.

More formally this can be expressed by:

$$(A = B) \iff \forall x\,(x \in A \iff x \in B).$$

Examples.

$$\begin{aligned} \{1,2\} &= \{2,1\}? \\ \{1,2\} &= \{1,1,2,2,2\}? \\ \{1,2,3\} &= \{1,1,1,3\}? \end{aligned}$$

Note that sets are *unordered* collections of objects, where the *multiplicities* of elements *don't matter*.

If A and B are finite sets containing a different number of elements, then they are obviously not equal.

Comprehension

The description of a (finite) set via an explicit listing of its elements is a relatively crude specification formalism. One often obtains more intuitive descriptions of sets by characterizing elements via a logical property.

Let A be a set and $P(x)$ be a formula in one variable. Then by

$$\{x \in A : P(x)\}$$

we denote the set that consists of all elements x of A for which $P(x)$ is true.

Remark. In formal set theory one has to introduce an axiom, called the *Principle of Comprehension*, which states that

> *for every set A and formula P there exists a set B, such that*
>
> $$\forall x\,[x \in B \iff (x \in A \wedge P(x))].$$

Subsets

A set A is said to be a *subset* of another set B, written $A \subseteq B$, if, and only if, every element of A is also an element of B.

Examples.

$$\begin{aligned} \{1,2\} &\subseteq \{1,2,3\}? \\ \{1,1,2,2\} &\subseteq \{1,2\}? \\ \{1\} &\subseteq \{2,3,5,7\}? \end{aligned}$$

Note that A is a subset of B if the following formula is true:

$$\forall x\,[x \in A \rightarrow x \in B].$$

Lemma. If $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Proof. If $A \subseteq B$ and $B \subseteq A$, then by the definition of the subset relation, every element of A is an element of B and every element of B is an element of A. This means that A and B have the same elements, hence are equal.
∎

Proper subsets

We say that A is a *proper subset* of B, written $A \subset B$, if A is a subset of B, but not equal to A:

$$A \subset B \iff (A \subseteq B \wedge A \neq B).$$

Example.

$$\{1,2\} \subset \{1,1,2,2\}?$$

Be careful about the distinction between the element relation and the subset relation.

Examples.

$$\begin{aligned} 2 &\in \{1,2,3\}? \\ \{2\} &\in \{1,2,3\}? \\ 2 &\subseteq \{1,2,3\}? \\ \{2\} &\subseteq \{1,2,3\}? \\ \{2\} &\subseteq \{\{1\},\{2\}\}? \\ \{2\} &\in \{\{1\},\{2\}\}? \end{aligned}$$

The Empty Set

Let A be any set. How many elements are there in the set $\{x \in A : x \neq x\}$?

A set with no elements is called an *empty set*.

Theorem. If $\emptyset$ is an empty set, then $\emptyset \subseteq A$, for all sets A.

Proof. It is vacuously true that every element of an empty set is an element of every other set A. ∎

Corollary. There is at most one empty set.

Proof. Suppose A and B are both empty sets. By the theorem above we have $A \subseteq B$ and $B \subseteq A$, and hence $A = B$. ∎

Another postulate of formal set theory, the *Existence Axiom*, asserts that

> *there exists a set*,

which by the above considerations implies that there is an (unique) empty set.

We use the symbol $\emptyset$, or sometimes $\{\}$, to denote the empty set.

Examples of Sets

The (finite) set of integers between -2 and 5:

$$\{n \in \mathbf{Z} \mid -2 < n < 5\}$$

The (open) interval of real numbers between -2 and 5:

$$\{x \in \mathbf{R} \mid -2 < x < 5\}$$

The (infinite) set of even integers:

$$\{n \in \mathbf{Z} \mid \exists k\,(n = 2k)\}$$

From a general description it may not always be obvious what the elements of the set are:

$$\{(x, y, z) \in \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z} \mid \exists n (n > 2 \wedge x^n + y^n = z^n)\}.$$

Powersets

There are various operations that allow one to construct new sets from given ones.

If A is a set, we denote by $\mathcal{P}(A)$ the set whose elements are the subsets of A.

Example. If A is the set $\{1, 2, 3\}$, then

$$\begin{aligned}\mathcal{P}(A) \;=\; \{&\emptyset,\\ &\{1\}, \{2\}, \{3\},\\ &\{1,2\}, \{1,3\}, \{2,3\},\\ &\{1,2,3\}\\ \}&\end{aligned}$$

Do we have $1 \in \mathcal{P}(A)$, or $2 \in \mathcal{P}(A)$, or $3 \in \mathcal{P}(A)$?

No, because $1 \neq \{1\}$, etc.

In formal set theory, the existence of these sets requires another axiom, the *Powerset Axiom*:

For every set A there exists a set B, such that

$$\forall x\,(x \in B \iff x \subseteq A).$$

The Size of Powersets

If $A = \emptyset$, then

$$\mathcal{P}(A) = \{\emptyset\} \neq \emptyset.$$

Observation.

> $\mathcal{P}(A) \neq \emptyset$, for all sets A.

If $A = \{x\}$, then $\mathcal{P}(A) = \{\emptyset, A\}$.

If $A = \{x, y\}$, then $\mathcal{P}(A) = \{\emptyset, \{x\}, \{y\}, A\}$.

If A has n elements, how many elements are there in its powerset?

Lemma.

> If A is a set with n elements, then $\mathcal{P}(A)$ has 2^n elements.

Proof. By mathematical induction on the number of elements in A.

Further Set Operations

Other operations for constructing sets include

- *set union*
- *set intersection*
- *relative complementation* (or *set difference*)
- *complementation*

They are defined as follows.

Let A and B be subsets of some set S. We define:

$$\begin{array}{rcl} A \cup B & = & \{x \in S \,|\, x \in A \vee x \in B\} \\ A \cap B & = & \{x \in S \,|\, x \in A \wedge x \in B\} \\ B - A & = & \{x \in S \,|\, x \in B \wedge x \notin A\} \\ A^c & = & \{x \in S \,|\, x \notin A\} \end{array}$$

For example, let

S be the set of real numbers,
A the set $\{x \in \mathbf{R} \,|\, -1 < x \leq 0\}$,
B the set $\{x \in \mathbf{R} \,|\, 0 \leq x < 1\}$.

What are $A \cup B$, $A \cap B$, $B - A$, and A^c?

Note that set difference can be defined as follows:

$$A - B = A \cap B^c.$$

Properties of Set Operations

Theorem.

1. $A \cap B \subseteq A$ and $A \cap B \subseteq B$
2. $A \subseteq A \cup B$ and $B \subseteq A \cup B$
3. If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof (of first property).

Let A and B be arbitrary sets. We prove that $A \cap B$ is a subset of A. By the definition of the subset relation, it suffices to show that every element of $A \cap B$ is an element of A. Let x be an arbitrary element of $A \cap B$. By the definition of intersection, we have $x \in A$ and $x \in B$. Thus x is an element of A. ∎

Set Identities

Review the following identities between sets and observe their similarity to equivalences in propositional logic.

1. Set union and intersection are commutative.
2. Set union and intersection are associative.
3. Distributivity: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
4. Double complement: $(A^c)^c = A$.
5. Idempotency: $A \cap A = A \cup A = A$.
6. De Morgan's Laws:
$$(A \cup B)^c = A^c \cap B^c$$
and
$$(A \cap B)^c = A^c \cup B^c.$$
7. Absorption: $A \cup (A \cap B) = A$ and $A \cap (A \cup B) = A$.

Distributivity

Theorem. For all sets A, B, and C,

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

Proof. Let A, B, and C be arbitrary sets. We show that the two sets $A \cap (B \cup C)$ and $(A \cap B) \cup (A \cap C)$ have the same elements:

$$\begin{array}{ll} x \in A \cap (B \cup C) & \\ \quad \text{iff} & x \in A \text{ and } x \in B \cup C \\ \quad \text{iff} & x \in A \text{ and } (x \in B \text{ or } x \in C) \\ \quad \text{iff} & (x \in A \text{ and } x \in B) \\ & \qquad \text{or } (x \in A \text{ and } x \in C) \\ \quad \text{iff} & x \in A \cap B \text{ or } x \in A \cap C \\ \quad \text{iff} & x \in (A \cap B) \cup (A \cap C) \end{array}$$

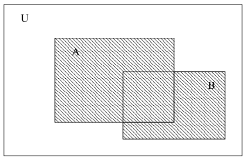
∎

Note the close connection between the "algebra of sets" and the "algebra of propositions" (Boolean algebra).

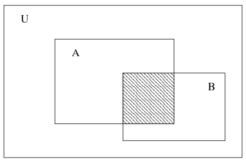
Venn Diagrams

Sets can often be conveniently represented by *Venn diagrams*.

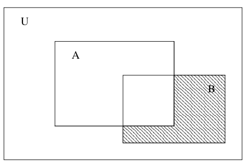
The union $A \cup B$ of A and B is represented by:



The intersection $A \cap B$ is represented by:



The set difference $B - A$ is represented by:



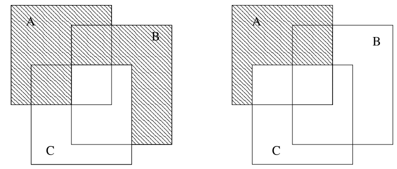
Counterexamples for Set Identities

Claim. For all sets A, B, and C,

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

Is this claim true?

Consider the two Venn Diagrams:



The diagram on the left represents $(A - B) \cup (B - C)$, the one on the right, $A - C$.

The difference in the diagrams suggests a counterexample to the claim.

Take $A = \{x, y\}$, $B = \{y, z\}$, and $C = \{x, w\}$. Then $(A - B) \cup (B - C) = \{x, y, z\}$, whereas $A - C = \{y\}$.

Encoding the Natural Numbers in Set Theory

If A is a set, then the set $A \cup \{A\}$ is called the *successor set* of A. Sometimes the successor set of A is denoted by A'.

The natural numbers can be encoded via successor sets:

$$\begin{array}{rclclcl}
0 & = & & & \emptyset & & \\
1 & = & 0' & = & \{\emptyset\} & = & \{0\} \\
2 & = & 1' & = & \{\emptyset, \{\emptyset\}\} & = & \{0, 1\} \\
3 & = & 2' & = & \ldots & = & \{0, 1, 2\} \\
\vdots & & & & & & \\
n + 1 & = & n' & = & \ldots & = & \{0, 1, \ldots, n\}
\end{array}$$

In other words, we can view each natural number as an abbreviation for a certain set!

One of the postulates of formal set theory asserts that there exists a set that contains the empty set and also contains the successor of each of its elements. That is, the existence of the set of natural numbers is assumed as an axiom.

Ordered Pairs and Tuples

Sets are *unordered* collections of elements.

Pairs, or more generally *tuples*, are *ordered* collections of elements.

Examples.

$$\begin{array}{rcl}
(1, 2) & \neq & (2, 1) \\
\{1, 2, 3\} & = & \{1, 3, 2\} \\
(1, 2, 3) & \neq & (1, 3, 2) \\
\{1, 2\} & = & \{1, 2, 2\} \\
(1, 2) & \neq & (1, 2, 2)
\end{array}$$

Surprisingly, (ordered) pairs can be defined in terms of (unordered) sets.

In set theory, an ordered pair (x, y) is taken as an abbreviation for the set $\{\{x\}, \{x, y\}\}$.

With this definition, do we indeed have

$$(x, y) = \{\{x\}, \{x, y\}\} \neq \{\{y\}, \{y, x\}\} = (y, x)?$$

What if $x = y$?

Tuples can be thought of as "nested" pairs. For example, we may regard $(1, 2, 3, 4, 5)$ as an abbreviation for $(1, (2, (3, (4, 5))))$ or $((((1, 2), 3), 4), 5)$.

Tuples of different length are never the same.

Number Sets

Common sets of numbers, such as the integers or the rational numbers, can be defined in terms of the natural numbers.

For instance, *integers* can be formally defined as pairs (σ, n) of a sign σ and a natural number n. There are two signs, usually written as $+$ and $-$ (and formally represented by two different sets, say $\emptyset$ and $\{\emptyset\}$).

These pairs are usually written as $+n$ (or simply n) and $-n$. There is only one 0, that is, $+0$ and -0 are considered equal.

The set of all integers is denoted by $\mathbf{Z}$.

The set of *rational numbers* can be defined by

$$\mathbf{Q} = \{(m,n) \,:\, m \in \mathbf{Z}, n \in \mathbf{Z}, \text{ and } m \neq 0\}.$$

Rational numbers are usually written as $\frac{m}{n}$ or m/n.

Integers can be identified with rational numbers of the form $\frac{k}{1}$.

Cartesian Products

Pairs and tuples provide us with a way of constructing new sets from given ones. This will be useful when we define "functions" and "relations."

If A and B are sets, then by $A \times B$ (read "A cross B"), we denote the set of all ordered pairs (a, b), where $a \in A$ and $b \in B$.

More formally,

$$A \times B = \{(a,b) \,|\, a \in A \wedge b \in B\}.$$

The set $A \times B$ is also called the *Cartesian* (or *cross*) *product* of A and B.

For example, if $A = \{1,2\}$ and $B = \{4,5\}$, then

$$A \times B = \{(1,4),(1,5),(2,4),(2,5)\}.$$

Note that A and B may be the same set.

For instance, if $A = \{1,3\}$, then

$$A \times A = \{(1,1),(1,3),(3,1),(3,3)\}.$$

If A contains m elements and B contains n elements, how many elements are there in $A \times B$?

Properties of Cartesian Products

Lemma.

> If A is a set of m elements and B a set of n elements, then $A \times B$ contains $m * n$ elements.

If $A = B$, then $A \times B = B \times A = A \times A$.

But if $A \neq B$, then $A \times B \neq B \times A$.

For example, let A be the set $\{1\}$ and B the set $\{2\}$. Then $A \times B = \{(1,2)\}$ and $B \times A = \{(2,1)\}$.

Also note that

$$A \times \emptyset = \emptyset \times A = \emptyset.$$

Lemma. For all sets A, B, and C we have

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

Proof. We need to show that $A \times (B \cup C)$ and $(A \times B) \cup (A \times C)$ have the same elements.

$$\begin{aligned} & (x,y) \in A \times (B \cup C) \\ \text{iff} \quad & x \in A \wedge y \in B \cup C \\ \text{iff} \quad & x \in A \wedge (y \in B \vee y \in C) \\ \text{iff} \quad & (x \in A \wedge y \in B) \vee (x \in A \wedge y \in C) \\ \text{iff} \quad & (x,y) \in A \times B \vee (x,y) \in A \times C \\ \text{iff} \quad & (x,y) \in (A \times B) \cup (A \times C) \end{aligned}$$

∎

Disjoint Sets

Two sets A and B are said to be *disjoint* if they have no elements in common, i.e., $A \cap B = \emptyset$.

Examples.

> Is $\{\emptyset, \{\emptyset\}\} \cap \{\emptyset\} = \emptyset$?
> *No*, $\{\emptyset, \{\emptyset\}\} \cap \{\emptyset\} = \{\emptyset\}$.
>
> Is $\{\emptyset, \{\emptyset\}\} \cap \emptyset = \emptyset$?
> *Yes*, the intersection $A \cap \emptyset$ of any set with the empty set is the empty set.

A *partition* of a set A is a collection of pairwise disjoint nonempty sets $A_1, \ldots, A_n$, such that

$$A = A_1 \cup A_2 \cup \cdots \cup A_n.$$

For example, at the end of the semester I will partition the class into subsets with grades of A, $A-$, etc. It will be a partition, since each student gets one, and only one, grade.

Partitions are closely related to equivalence relations, which we will discuss later in the semester.

Russell's Paradox

The barber of a small town agreed, for a handsome fee, to shave all the (male) inhabitants of the town who did not shave themselves, and never shave any inhabitant who did shave himself. The fee was to be paid at the end of each year.

When the barber tried to collect the fee at the end of the first year the mayor refused to make any payment, pointing out that the barber had shaved himself and therefore violated the rule of never shaving any inhabitant who did shave himself.

Therefore the next year the barber did not shave himself. But at year-end the mayor turned him down again, pointing out that time he had failed to shave someone who did not shave himself.

This paradox illuminates a difficulty in setting up a formal theory of sets: Allowing set operations that are too general may result in inconsistencies or contradictions in the theory.

A Set Paradox

Consider the set of all sets that are not elements of themselves:

$$S = \{A \mid A \notin A\}.$$

Is S an element of itself?

We have

$$S \in S \text{ if and only if } S \notin S,$$

which is a contradiction!

But note that the above definition of S is not covered by the Comprehension Principle. By this principle we can only define, for *some given set* U, the set

$$S = \{A \in U \mid A \notin A\}.$$

Now, if $S \in S$, then by the (new) definition of S, we get $S \notin S$, which would of course be a contradiction.

Therefore we may conclude that $S \notin S$, in which case we may *also infer* $S \notin U$. We obtain no contradiction, though.

In short, contradictions are avoided by the additional condition $A \in U$ required by comprehension.