Lecture 8: Sets

In past lectures, we have already talked about sets. Today, we make this more formal.

Why Sets?

A set is the mathematician's answer whenever you have a question that can have zero, one, or more than one correct answers. Imagine you are writing an equation-solving procedure in a program, depending on your programming language this might also be called a method, or a function. For example, if your procedure gets $2x - 1 = 5$ as input then you might think the answer should be 3. If your programming language has types, you might think the return value of your procedure should be some kind of number.

The problem is that not all equations have a single solution. For example, $(x - 1)(x - 2) = 0$ has exactly two solutions; $x = x + 1$ has none at all, and $x = x$ has infinitely many. You might think your return type should be something like 'list of numbers' but this does not get you the exact abstraction you need, since for example a list can contain the same number more than once.

A set (of numbers) is exactly what you need here. Mathematically, a set is an object where, for any number (or more generally, any element) you can ask the question: is this element in the set? The only possible answers are yes and no.

Sets and Elements

We assume everyone agrees on some idea of basic elements (numbers, truth values, colours, people etc.). Elements do not need to have 'types'. A set is a collection of elements, for example the integers, or the real numbers, or the set containing the single element 5, or the empty set. Sets do not need to have 'types' either[1], so you can form a set containing the number 3, the colour red, and the King of England if you want to.

The basic thing you can do when you have an element and a set is ask, is this element in the set?

Definition 1 (sets and elements)**.** If x is an element and S is a set, then we write $x \in S$ if x is in[a] S, and $x \notin S$ otherwise. These are both formulas (that is, they have truth values).

For any element x and any set S, exactly one of the two cases $x \in S$ and $x \notin S$ is true, and the other is false (this is the law of excluded middle for set theory).

Sets can contain other sets, so all sets are also elements[b].

[a] You can also pronounce $x \in S$ as 'x is an element of S'.
[b] In more formal versions of set theory, actually all elements are also sets.

For simple enough sets, we can just list their elements:

Definition 2 (set notation)**.** We can write sets by listing their elements between curly braces, thus $S = \{2, 3\}$ is the set containing two elements $2, 3$ (so $2 \in S$ but $4 \notin S$).

Of course, some sets are important enough to get their own names, such as $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.

Sets are completely defined by their elements:

[1] In mathematics, at least. In many programming languages with types, you can make e.g. a `Set<X>` that only accepts elements of type X.

Definition 3 (set equality)**.** Sets are completely defined by their elements, that is, two sets are equal if and only if they contain the same elements. As a formula,

$$\forall X, Y : \text{sets} \,.\, (X = Y \leftrightarrow \forall a : \text{element} \,.\, (a \in X \leftrightarrow a \in Y))$$

So, for example,

- $\{2, 3\}$ and $\{3, 2\}$ are the same set written in different ways (just as $2/3$ and $4/6$ are the same number).
- $\{2, 2, 3\}$ is the same set as $\{2, 3\}$, a set cannot contain an element more than once. Writing a set with an element appearing more than once is legal but not fully reduced, just like $2/2$ is a legal but not reduced way of writing the value 1 — not fully reduced fractions and sets can both occur 'naturally' as part of doing calculations, but you should obviously reduce any answers you give to your exercises and exams if there is an obvious way to do this.
- However, $\{2, 3\}$ and $\{\{2\}, 3\}$ are not the same. The former is a set containing the numbers $2, 3$, and the latter is a set containing the number 3 and the set containing the number 2 as elements. The number 2 and the set $\{2\}$ are not the same thing.

The empty set also gets a special symbol.

Definition 4 (empty set)**.** The empty set is the set with no elements (we can say 'the' empty set because, by the previous definition, any other set with no elements would be equal). We write it either $\{\}$ or $\varnothing$. As a formula,

$$\forall a \,.\, a \notin \varnothing$$

Set Restriction and Subsets

If we have a set and a predicate, we can form another set with only the elements from the oroginal set that match the predicate.

Definition 5 (set restriction)**.** If S is a set and P is a predicate, then the expression

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

is called the restriction of S to P, pronounced 'the set of all x in S such that P [holds on x]'. This is again a set.

Warning, restriction can only make sets out of other sets, you have to start with something that is a set in the first place. Russell's paradox is an expression of the form 'the set of all sets such that …' which leads to a contradiction; it looks like it should be a set restriction but the problem is that 'all sets' is not a set itself, so this is not a valid term in the first place.

Set restriction allows us to link sets and logic, because we can use restrictions with logical formulas to form new sets as well as using logical formulas to reason about sets themselves.

Definition 6 (subset)**.** A set X is called a subset of a set Y, written $X \subseteq Y$, if every element of X is also an element of Y, or put another way

$$\forall a \,.\, (a \in X \to a \in Y)$$

Every set is a subset of itself (our definition is really 'subset-or-equal'), and two sets are equal

($X = Y$) if and only if $X \subseteq Y \wedge Y \subseteq X$.

The result of a set restriction $\{x \in S \mid P(x)\}$ is always a subset of the original set S.

The empty set is a subset of all sets: $\forall S : \text{set} \,.\, \varnothing \subseteq S$ since the implication $a \in \varnothing \to a \in S$ is always true, on account of the antecedent $a \in \varnothing$ being false for all elements a.

Set Operations

We can combine two sets to make a new one.

Definition 7 (Set Union and Intersection)**.** For two sets X, Y

- The union $X \cup Y$ is the set of all elements in either of the sets, or both; as a formula

$$\forall a \,.\, (a \in X \cup Y \leftrightarrow a \in X \vee a \in Y)$$

- The intersection $X \cap Y$ is the set of all elements in both sets, as a formula

$$\forall a \,.\, (a \in X \cap Y \leftrightarrow a \in X \wedge a \in Y)$$

- The difference $X \setminus Y$ is the set of elements in X that are not in Y, as a formula

$$\forall a \,.\, (a \in X \setminus Y \leftrightarrow a \in X \wedge a \notin Y)$$

The similarity in shapes between $\wedge$ and $\cap$, and between $\vee$ and $\cup$, is intentional. Some books write $X - Y$ for the set difference instead of $X \setminus Y$.

Further, if we fix a set $\mathcal{U}$ that in set theory we call a *universe*, such as the integers or real numbers, then we can define a set's complement $\overline{X} = \mathcal{U} \setminus X$. (Note that without a universe, $\{a \mid a \notin X\}$ is not a valid term as set restriction needs to start with a set, but $\{a \in \mathcal{U} \mid a \notin X\}$ is fine. Similarly, in a universe, we can define $X \cup Y = \{a \in \mathcal{U} \mid a \in X \vee a \in Y\}$ and the same idea for $\cap$ with $\wedge$.

The set operations obey the laws of logic from the expressions that define them:

- **Commutative laws**. $A \cap B = B \cap A$ and $A \cup B = B \cup A$.
- **Associative laws**. $(A \cap B) \cap C = A \cap (B \cap C)$ and the same for $\cup$.
- **DeMorgan's laws**. $\overline{A \cup B} = \overline{A} \cap \overline{B}$ and $\overline{A \cap B} = \overline{A} \cup \overline{B}$.
- **Distributive laws**. $A \cup (B \cap C) = (A \cup B) \cap (B \cup C)$ and the same with $\cap, \cup$ reversed.
- **Idempotent laws**. $A \cup A = A$ and $A \cap A = A$.
- **Law of the excluded middle**. $A \cup \overline{A} = \mathcal{U}$ and $A \cap \overline{A} = \varnothing$.
- **Elimination laws**. $A \cup \varnothing = A$ and $A \cap \varnothing = \varnothing$ and, in a universe $\mathcal{U}$, $A \cup \mathcal{U} = \mathcal{U}$ and $A \cap \mathcal{U} = A$.
- **Complement laws**. $\overline{\mathcal{U}} = \varnothing$ and $\overline{\varnothing} = \mathcal{U}$.
- **Double complement law**. $\overline{\overline{A}} = A$.

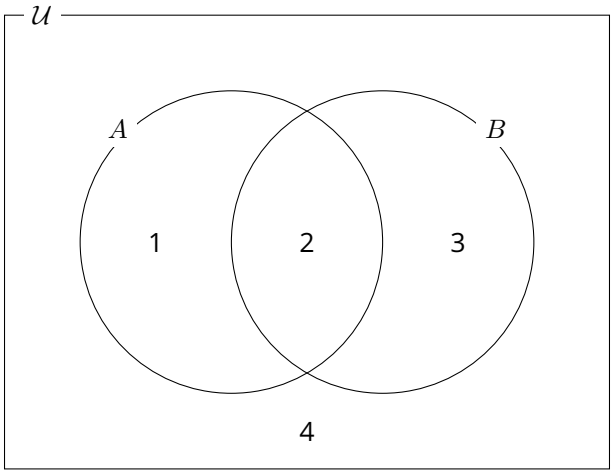
All these laws can be proven with logic, through the general approach of unpack, calculate, pack again. For example, the first DeMorgan's law:

Claim. $\overline{A \cup B} = \overline{A} \cap \overline{B}$ in a universe $\mathcal{U}$.
Proof. Pick $x \in \overline{A \cup B}$. This means that $x \notin (A \cup B)$ by unpacking the complement, and so $\neg(x \in (A \cup B))$. Unpacking the union, this means $\neg(x \in A \vee x \in B)$, to which we apply logical DeMorgan to get $(x \notin A) \wedge (x \notin B)$. Packing $x \notin A \equiv x \in \overline{A}$ and the same for B, we get $x \in \overline{A} \wedge x \in \overline{B}$, and packing the definition of $\cap$ this is $x \in (\overline{A} \cap \overline{B})$, which is one direction of what we wanted to prove namely $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$.

There are two ways in general to prove $X = Y$ for sets; the first is to start with $x \in X$ and calculate until you get $x \in Y$ which shows $X \subseteq Y$, and then show $Y \subseteq X$ separately; the second way is that if all steps in your first proof are reversible, then you have shown both directions at once. This is the case here.

Venn Diagrams

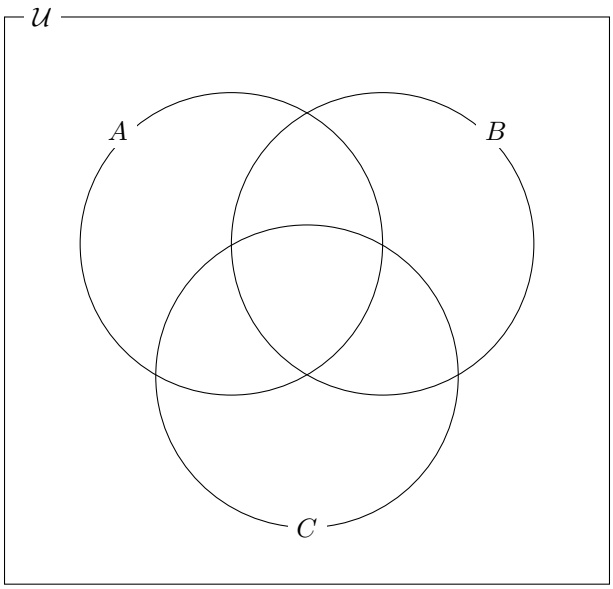
When we are working with two (or sometimes three) sets, it is helpful for the intuition to draw a picture:



The two circles divide the enclosing rectangle, representing the universe, into four areas. Elements in area 1 are in A but not in B; elements in area 2 are in both A and B; elements in area 3 are in B but not in A, and elements in area 4 are neither in A nor in B.

For example, if we called area 1 W, then we would have $\forall e \in W.e \in A \wedge e \notin B$. If we interpreted the numbers 1–4 as elements, then we would have $\mathcal{U} = \{1, 2, 3, 4\}$ and $A = \{1, 2\}$ and $B = \{2, 3\}$.

We can similarly draw a Venn diagram for three sets, giving 8 areas:



Operations on Multiple Sets

We can do set operations on more than two sets using a similar notation to Σ for sums. If $A_1, \ldots, A_n$ are sets, then $\cup_{i=1}^{n} A_i$ is the union $A_1 \cup \ldots \cup A_n$, or more formally,

$$\forall e.\ \left(e \in \bigcup_{i=1}^{n} A_i \leftrightarrow e \in A_1 \vee \ldots \vee e \in A_n \right)$$

Similarly, one defines $\cap_{i=1}^{n} A_i$ using $\wedge$. This is fine because both $\cup$ and $\cap$ are associative and commutative.

We can take this idea even further by using any set, instead of integers, for indexing. If I is a set of elements that we call indexes, and for any $i \in I$ there is a set A_i, then we call these A_i a collection of sets, or a family of sets. We can write $\{A_i\}_{i \in I}$ to mean a collection of sets A_i indexed by the set I.

For such a collection of sets, we can write $\bigcup_{i \in I} A_i$ for the union of all the sets A_i. For example, if $I = \{+, 0, -\}$ and we define $\mathbb{Z}_- = \{\ldots, -2, -1\}$ to be the negative integers, $\mathbb{Z}_+ = \{1, 2, \ldots\}$ to be the positive integers, and $\mathbb{Z}_0 = \{0\}$, then we could write $\mathbb{Z} = \bigcup_{i \in I} \mathbb{Z}_i$ which means $\mathbb{Z}_- \cup \mathbb{Z}_+ \cup \mathbb{Z}_0$.

A particularly useful thing you can do with indexes is partition a set in such a way that every element ends up in exactly one part.

Definition 8 (partition)**.** A partition of a non-empty set A is a collection of sets A_i (where $i \in I$ for some index set I) such that

1. $A = \bigcup_{i \in I} A_i$
2. $\forall i, j \in I.\ (i \neq j \rightarrow A_i \cap A_j = \varnothing)$

The first condition says that all the A_i together contain all the elements of A, but no extra elements that were not in A. The second condition says that no element of A can end up in more than one of the A_i. Thus, in a partition of sets, every $a \in A$ has exactly one associated $i \in I$ such that $a \in A_i$. We can, of course, think of a partition as a function $A \rightarrow I$ (which we will define formally in a later lecture).

For example, we could classify all integers by their remainder when dividing by 3. Thus, if $I = \{0, 1, 2\}$ is the set of possible remainders as our index set, then we could set $\mathbb{Z}_0 = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$, $\mathbb{Z}_1 = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$ and $\mathbb{Z}_2 = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$. Then $\{\mathbb{Z}_i\}_{i \in I}$ is a partition of the integers $\mathbb{Z}$. All the sets here except the index set are infinite, but that is not a problem.

One reason to do a partition of a set is to do a proof by case distinction. If you want to prove some predicate $p(a)$ for all $a \in A$, then you can sometimes find a way to partition A into A_1, A_2, A_3 for example so that you can easily prove the predicate p on each of the A_i individually. As long as the A_i are a partition of A, this proves the predicate for all $a \in A$.

Sets of Sets

Sets can contain other sets. Over the integers, consider the sets

$$A = \{1\}, \quad B = \{1, 2\}, \quad C = \{\{1\}, 1, 2\}, \quad D = \{\{1\}\}$$

- The set A contains one element, the integer 1.
- The set B contains two elements, namely the integers 1 and 2.
- The set C is a set of three elements, two of which are integers, and the third of which is another set (containing an integer). The set $\{1\}$ is not the same thing as the integer 1.
- The set D contains one element, which is itself a set containing one element which is an integer.

Comparing A and B, we have $A \subseteq B$ (A is a subset of B) because $\forall e.\ (e \in A \to e \in B)$: there is only one element 1 in A, and it is also in B.

We do not have $A \in B$. It is allowed to apply the predicate $\in$ to sets as well as elements, but the set B does not contain the set $\{1\}$ as an element, even though it does contain the integer 1 — but that is a different thing.

Comparing the other sets with C, we have both $A \subseteq C$ since $1 \in C$, and $A \in C$ since $\{1\} \in C$. However, although $B \subseteq C$, we do not have $B \in C$.

We have $A \in D$ as A is an element of D (in fact, the only element of D) but we do not have $A \subseteq D$ since A contains the element 1, but D does not. Thus, for any two sets X, Y, the predicates $X \in Y$ and $X \subseteq Y$ can be both true, both false, or one true and one false in both ways — all four possibilities exist.

As we know that two sets are equal if and only if they contain the same elements, we could say in the above example that $D = \{A\}$ or that $C = \{A, 1, 2\}$. Allowing sets to contain other sets increases the level of abstraction that one needs to think on to work with sets, and one must not confuse $\in$ and $\subseteq$.

The empty set can itself be an element in other sets, which we will need in a moment. For example, the following are all different sets:

- $\{\}$, the empty set, also written $\varnothing$. It contains 0 elements.
- $\{\{\}\}$, the set containing the empty set. It contains 1 element, and you could also write it $\{\varnothing\}$.
- $\{\{\{\}\}\}$, the set containing the set containing the empty set. You could write this $\{\{\varnothing\}\}$.

You can continue this as many times as you want, and even do it 'infinitely often' if you are very careful what you mean by this. For example, one formulation of the integers is the Peano Axioms, which say:

1. The element 0, defined as the empty set, is an integer.
2. For any integer (as a set) x, the successor $S(x) = x \cup \{x\}$ is also an integer.

So $1 = \{\varnothing, \{\varnothing\}\}$ (the set containing two elements, one being the empty set, and one being the set containing the empty set) and $2 = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$ and so on. No mathematician actually thinks of the integers like this, but this definition does give you the correct recursive structure over the integers (so you can do proofs by induction) using only definitions from set theory.

Whatever you do, although a set is always a subset of itself ($\forall A.\ (A \subseteq A)$), a set can never contain itself: ($\forall A.\ (A \notin A)$). Even the empty set is not an element of itself, since it contains no elements.

Set theory does in principle allow infinitely nested chains of sets (you need this to define the set of integers in Peano's theory, for example), but only under very specific rules as it is very easy to build a contradiction otherwise. Once again, there is no such thing as a 'set of all sets'.

Powersets

Starting with a set A, one can form the set of all of its subsets. This is called the powerset.

Definition 9 (powerset)**.** The powerset of a set A, written $\mathcal{P}(A)$, is the set of all subsets of A. As a formula, for any set T, we have $T \in \mathcal{P}(A) \leftrightarrow T \subseteq A$.

For example,

- If $A = \varnothing$ then $\mathcal{P}(A) = \{\varnothing\}$.
- If $A = \{1\}$ then $\mathcal{P}(A) = \{\varnothing, \{1\}\}$.
- If $A = \{1, 2\}$ then $\mathcal{P}(A) = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\}$.

Some facts about powersets:

- A powerset is never empty. Even the powerset of the empty set contains an element.
- The empty set is an element of every powerset. (The empty set is also a subset of every set, but it is not an element of every set.)
- A powerset always contains 'more' elements than the original set (but we will need to explain what we mean for infinite sets). For finite sets, the powerset of a set with n elements contains 2^n elements.

If a set contains n elements, then we can form 2^n subsets by making a truth table with n variables, one for each element. On each row of the table, if you take exactly the elements whose variable is set to true in this row, that gives you a subset. For example on a set with three elements $A = \{1, 2, 3\}$:

1	2	3	subset
F	F	F	$\varnothing$
F	F	T	$\{3\}$
F	T	F	$\{2\}$
F	T	T	$\{2, 3\}$
T	F	F	$\{1\}$
T	F	T	$\{1, 3\}$
T	T	F	$\{1, 2\}$
T	T	T	$\{1, 2, 3\}$

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

Cardinality

The cardinality of a finite set A is the number of elements that it contains, and we write this operation as $|A|$. One can define cardinality for infinite sets, but this is more complicated.

We can state some obvious rules for cardinality:

1. The cardinality of the empty set is zero: $|\varnothing| = 0$. In fact, the empty set is the only set of cardinality zero.
2. $|A \cup B| \leq |A| + |B|$, with equality if and only if $A \cap B = 0$.
3. $|A \cap B| \leq \min(|A|, |B|)$.
4. To be precise, $|A \cup B| = |A| + |B| - |A \cap B|$.
5. In a finite universe $\mathcal{U}$, $|\overline{A}| = |\mathcal{U}| - |A|$.

Set Projection

If we have one or more sets, and a function from their elements to a new set, then we can form the set projection (or set comprehension) such as

$$\{f(a) \mid a \in A\} \qquad \{g(a,b) \mid a \in A, b \in B\}$$

This uses similar notation to set restriction, but it is a very different thing. The vertical bar here is pronounced 'for' instead of 'such that', and the $\in$ symbols appear on the right, not the left, of the bar. The result of a set projection is not necessarily a subset of the sets on the right. For example, the set

$$\{\sqrt{x} \mid x \in \mathbb{N}\} = \{0, 1, \sqrt{2}, \sqrt{3}, 2, \sqrt{5}, \ldots\}$$

is a set projection starting in the integers, but some of its elements are not integers any more.

Cartesian Product

A pair (a, b) is a mathematical object with the property that two pairs are equal if and only if their elements in each position are equal: $(a, b) = (c, d) \Leftrightarrow a = c \wedge b = d$. Unlike sets, pairs can contain the same element twice, and the order matters: $(1, 2) \neq (2, 1)$.

Formally, one could define in set theory that the pair (a, b) is the set $\{a, \{a, b\}\}$ and derive all the usual properties from this, which works even if a, b are sets themselves. This definition buys us that we do not have to work with two separate 'data types' for sets and pairs, but it gives neither any intuition nor does it make any calculations any easier, so informally one can treat pairs as if they were their own kind of object.

For two sets A, B, we can define the set of pairs of their elements.

Definition 10 (Cartesian product)**.** The Cartesian product $A \times B$ of two sets A, B is the set $\{(a, b) \mid a \in A, b \in B\}$.

If either of the sets A, B is the empty set, then so is their Cartesian product.

As to cardinality, for finite sets we have $|A \times B| = |A| \cdot |B|$.

For example, if $A = \{\text{red}, \text{blue}\}$ and $B = \{\bigcirc, \triangle, \square\}$ then

$$A \times B = \{(\text{red}, \bigcirc), (\text{blue}, \bigcirc), (\text{red}, \triangle), (\text{blue}, \triangle), (\text{red}, \square), (\text{blue}, \square)\}$$

You can visualise the Cartesian product of two sets with m and n elements respectively as an $m \cdot n$ table with each entry being the pair of elements described by their row and column; the Cartesian product is then the set of all table entries. For the same sets A, B as above for example,

	$\bigcirc$	$\triangle$	$\square$
red	(red, $\bigcirc$)	(red, $\triangle$)	(red, $\square$)
blue	(blue, $\bigcirc$)	(blue, $\triangle$)	(blue, $\square$)

Note that $A \times B \neq B \times A$ in general: the former is a set of pairs with A-elements on the left, and the latter is a set of pairs with A-elements on the right. However, there is an obvious way to map from one set to the other, namely turn the pair (a, b) into the pair (b, a) or vice versa, so the two sets $A \times B$ and $B \times A$ can be considered equivalent for many purposes even if they are not equal (the mathematically exact term would be *isomorphic*).

We can take Cartesian products of more than two sets. If $A = \{1\}, B = \{2\}$ and $C = \{3\}$ then $(A \times B) \times C = \{((1, 2), 3)\}$ but $A \times (B \times C) = \{(1, (2, 3))\}$. The former is a set of one element, which is a pair, whose left element is again a pair; the latter is a set of one element, which is a pair, whose left element is an integer and whose right element is another pair.

But there is an obvious way again to map from one of these sets to the other, so in practice one defines the Cartesian product of sets $A_1 \times \ldots \times A_n$ without any brackets as the set of tuples $(a_1, \ldots, a_n)$ where $a_i \in A_i$ for $i \in \{1, \ldots, n\}$.