1 Introduction

As computer scientists we are familiar with the notion of *abstraction* at various levels. In particular, programming languages provide abstractions both of the physical processes of computation at the hardware level, and of the actual data and algorithms that they represent. In the theory of computing we want to be able to discuss and reason about computing itself without reference to any specific language so yet another level of abstraction is required.

Fortunately, mathematics provides a ready built set of abstract concepts that are ideal for this sort of reasoning. In the first few lectures of COSC 341 we will (re)introduce these concepts. We *are not* going to need a large body of mathematical knowledge – but we do need its notation, and the basic concepts of logic that allow us to write proofs.

2 Sets

A *set*, X, is just a collection of objects. It divides the universe into two parts: those things that belong to, or *are elements of* X, and those which do not. This is all it does so the elements of a set can also be thought of as an unordered collection without duplication. The easiest way to specify a set is by listing its elements explicitly:

$$\begin{aligned} X &= \{1, 2, 5\} \\ Y &= \{a, b, c, d, e\} \end{aligned}$$

The belonging relationship is denoted by the symbol $\in$. So:

$$1 \in X,\ 2 \in X,\ 3 \notin X,\ 4 \notin X,\ 5 \in X,\ \ldots$$

Two sets are equal if (and only if) they have exactly the same collection of elements. That is:

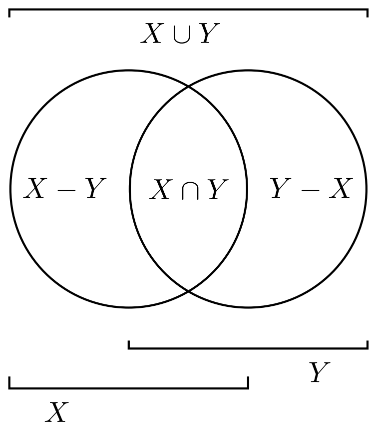
$$X = Y \iff \begin{array}{l} \text{for all } x \in X, x \in Y \\ \text{and, for all } y \in Y, y \in X \end{array}$$

If the first of these conditions holds then we say that X *is a subset of* Y and write $X \subseteq Y$.

The *empty set* is the unique set that has no elements and is denoted $\emptyset$.

3 Operations on sets

We can combine sets in various ways, summarized in the following diagram:



- $\cup$ is called *union*, $a \in X \cup Y$ if $a \in X$ or $a \in Y$;
- $\cap$ is called *intersection*, $a \in X \cap Y$ if $a \in X$ and $a \in Y$
- $-$ is called *difference* or *relative complement*, $a \in X - Y$ if $a \in X$ and $a \notin Y$;
- if our sets exist in some "universe", U, (e.g. the integers) then we also have a notion of *complement*, where $X^c = U - X$.

4 Partitions

A collection of sets $X_1, X_2, \ldots, X_k$ *partition* a set X if

- $X = X_1 \cup X_2 \cup \cdots \cup X_k$, and
- for $i \neq j$, X_i and X_j are *disjoint*, that is $X_i \cap X_j = \emptyset$.

5 Set builder notation

A second, and more common, way to represent a set is by defining explicitly the rule or formula that its elements must satisfy in order to belong to the set. We write:

$$X = \{x \mid \text{some property of } x \text{ holds}\}$$

which is to be read as "X is the set of those elements x such that some property of x holds". For instance, the set of perfect squares $\{0, 1, 4, 9, 16, \dots\}$ can be defined as

$$S = \{m \mid \text{for some } n \in \mathbb{N}, m = n^2\}.$$

Here and henceforth we use $\mathbb{N}$ as a symbol for the *natural numbers*, or non negative integers

$$\mathbb{N} = \{0, 1, 2, 3, \dots\}.$$

6 Ordered pairs and tuples

Given two sets A and B we can form *ordered pairs*, (a, b) whose first coordinate comes from A and second from B. The rule here is that:

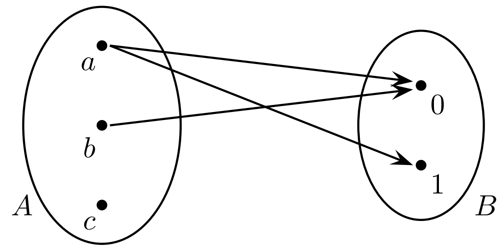
$$(a, b) = (a', b') \iff a = a' \text{ and } b = b'$$

i.e. two ordered pairs are equal if and only if their coordinates are equal and in the same order. The set of all ordered pairs whose first coordinate comes from A and second from B is called the *Cartesian product* of A and B and denoted $A \times B$.

More generally we can form *ordered tuples* of any fixed length and corresponding Cartesian products of sets A_1, A_2, …, A_k.

7 Relations

A *relation* from A to B (or between A and B) is just a subset of $A \times B$. Relations are often illustrated schematically by "potato and arrow" diagrams. For instance the relation from $\{a, b, c\}$ to $\{0, 1\}$ which is the set $\{(a, 0), (a, 1), (b, 0)\}$ could be drawn as follows:



8 Functions and partial functions

A *function* is a special sort of relation. In the potato and arrow diagram there must be exactly one arrow from each element of A to some element of B. In other words a function is like a procedure that takes elements of A as input and produces elements of B as output. A *partial function* is like a function except that some elements of A may not have arrows that start from them (the "procedure" is not fully defined, or crashes on some inputs). If we want to be completely clear we sometimes call functions which are defined for every element of A *total functions*.

If we have a function, f, and an element $a \in A$, then the element of B that is paired with it is generally denoted $f(a)$. That is:

$$f = \{(a, f(a)) \mid a \in A\}.$$

The set of all functions from A to B is denoted B^A.

A function is *one to one* or *injective* if no two arrows point to the same element (that is, different inputs give different outputs). A function is *onto* or *surjective* if every element of B has at least one arrow pointing to it. A function is a *one to one correspondence* or *bijection* if it is both injective and surjective.

9 Tutorial problems

1. Let $X = \{1, 2, 5\}$ and $Y = \{0, 2, 4, 6\}$. List the elements of:
   (a) $X \cup Y$ (the union of X and Y)
   (b) $X \cap Y$ (the intersection of X and Y)
   (c) $X - Y$ (the complement of Y relative to X)
   (d) $Y - X$ (the complement of X relative to Y)
   (e) $\mathcal{P}(X)$ (the power set of X, i.e. the set of all subsets of X)
2. Let $X = \{0, 1, 2\}$ and $Y = \{f, t\}$.
   (a) List all the members of $X \times Y$.
   (b) List all total functions from Y to X.
   (c) List all partial (but not total) functions from Y to X.
3. Let X be a set with 3 elements, and Y a set with 4 elements.
   (a) How many elements are there in $X \times Y$?
   (b) How many total functions are there from X to Y?
   (c) How many total functions are there from Y to X?
   (d) How many partial (possibly total) functions are there from X to Y?
4. Give examples of functions $f : \mathbb{N} \to \mathbb{N}$ that satisfy:
   (a) f is total and injective but not surjective,
   (b) f is total and surjective but not injective,
   (c) f is total, injective and surjective, but is not the identity,
   (d) f is not total, but is surjective.