Sets, Sequences, Relations and Functions
Mathematical Structures for CS (CSCI 3030)

Prof. Harley Eades (heades@gru.edu).

Read chapter 2.1 - 2.5

In computer science and mathematics we more often than not study collections of objects. For example, the collection of all real numbers or the collection of all computers on a network. In addition grouping objects together into collections we often need to relate one collection to another. In this lecture we mathematically define the notion of a collection and the notions need to relate collections to one another.

1 Mathematical Collections: Sets

In this section we give the formal definition of what we have been calling a "collection."

Definition 1. *A **set** is an unordered collection of objects called elements or members. Given elements $a, b, c, d, e, f, \ldots$ we denote the set containing these elements by $\{a, b, c, d, e, f, \ldots\}$. We say a set contains its elements, and when given a set, S, and an element, x, we write $x \in S$ if and only if the element x is a member of S, and we write $x \notin S$ otherwise. We often denote a set using a capital letter, and its elements using lowercase letters.*

There are many ways to define a set. The most basic way is to simply list all of its elements between curly braces. This is known as the roster method.

Example 2. *The following are several sets:*

- *The set of all integers is $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$,*
- *The set of all natural numbers is $\mathbb{N} = \{0, 1, 2, 3, 4, 5, 6, \ldots\}$,*
- *The set of boolean values is $\mathbb{B} = \{True, False\}$,*
- *A set of three colors is $C = \{Red, Green, Blue\}$,*
- *The set of propositional logical connectives is $P_{op} = \{\wedge, \vee, \Rightarrow, \neg\}$, and*
- *The set of four digit binary numbers is*

$$\mathsf{Bin}_4 = \{0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111\}.$$

Definition 3. *There is a special set called the **empty set** denoted $\emptyset$ or $\{\}$. This set has no elements.*

A second, and more powerful way to define sets is by the **set builder** or **set comprehension** method. Consider an example. Suppose $\mathsf{isEven(x)}$ is a predicate that is true when its argument, x, is an even integer, then we can define the following set of even integers:

$$\mathsf{Even} = \{i \mid i \in \mathbb{Z} \text{ and } \mathsf{isEven}(i)\}$$

This notation gives a pattern for the elements using variables, in the above this is i, and a predicate on i, in this case it is $i \in \mathbb{Z}$ and $\mathsf{isEven}(i)$, that when true for a particular i adds that integer to the set Even and leaves the integer out if not. Thus, the set

$$\mathsf{Even} = \{i \mid i \in \mathbb{Z} \text{ and } \mathsf{isEven}(i)\}$$

can also be defined by

$$i \in \mathsf{Even} \text{ if and only if } i \in \mathbb{Z} \text{ and } \mathsf{isEven}(i).$$

Therefore, we know that $\mathsf{Even} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$ because all of its elements are integers and even. We have arrived at the following definition:

Definition 4. *A set defined by set builder notation is denoted as follows:*

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

where P is some predicate on the set T. Thus, $x \in S$ if and only if $x \in T$ and $P(x)$ holds.

Thus, set builder or set comprehensions combine the power of logic with the power of sets. The following are a few more examples:

- $\mathbb{N}_{<10} = \{n \in \mathbb{N} \mid n < 10\}$,
- $\mathbb{N}^{+} = \{n \in \mathbb{N} \mid n > 0\}$, and
- $\mathsf{Win}_7 = \{c \in \mathsf{GRUNet} \mid c \text{ runs Windows 7}\}$, where GruNet is the set of all computers on the GRU network.

Sets can be related to one another if they have elements in common.

Definition 5. *A set A is a **subset** of a set B if and only if $\forall x \in A.x \in B$. We denote this relationship by $A \subseteq B$. If $\exists y \in B.y \notin A$, then we say A is a **proper subset** of B and denote this by $A \subset B$.*

To prove that $A \subseteq B$ show if $x \in A$ then $x \in B$ for arbitrary x. To prove that $A \not\subseteq B$ show that there exists some element $x \in A$ such that $x \notin B$. The previous definition implies the following:

Lemma 6. *Suppose A is a set. Then $A \subseteq A$ and $A \not\subset A$.*

Proof. Suppose A is a set. Then we must show that $A \subseteq A$ which is equivalent by definition to $\forall x \in A.x \in A$, but this is equivalent to $\forall x.x \in A \Rightarrow x \in A$, which easily follows.

We must now show that $A \not\subset A$, but this is equivalent to showing that $\neg(\exists y \in A.y \notin A)$. The latter is equivalent to $\neg(\exists y.y \in A \wedge y \notin A)$ if and only if $\forall y.y \notin A \vee y \in A$ which is equivalent to LEM, and thus holds. □

Lemma 7. *Suppose A is a set. Then $\emptyset \subseteq A$.*

Proof. Suppose A is a set. Then we must show that $\emptyset \subseteq A$ which is equivalent to $\forall x \in \emptyset.x \in A$, but this is equivalent to $\forall x.x \in \emptyset \Rightarrow x \in A$. The latter is always true, because $x \in \emptyset$ is always false for any x. □

Using the subset operation we can define when two sets are equivalent.

Definition 8. *We say two sets A and B are **equivalent** if and only if $A \subseteq B$ and $B \subseteq A$.*

The previous definition implies that two sets are equivalent if and only if they have exactly the same members. Thus, two sets A and B are equivalent if and only if $\forall x.(x \in A \Leftrightarrow x \in B)$ holds. Note that this says nothing about the order of the elements. Thus, the two sets $\{1, 2, 3, 4\}$ and $\{4, 2, 3, 1\}$ are equivalent, because they have the same elements. Furthermore, it does not matter if elements appear more than once, that is, the sets $\{1\}$ and $\{1, 1, 1, 1, 1, 1\}$ are equivalent, and so are, $\{2, 3, 4, 3, 6\}$ and $\{2, 3, 4, 6\}$.

Sets have a size called their cardinality.

Definition 9. *Suppose A is a set. If A has $n \in \mathbb{N}$ distinct elements, then we say A is finite, and its **cardinality** is n. We denote the cardinality of a set A by $|A|$.*

Some examples of cardinality are $|\mathbb{N}_{<10}| = 10$ and $|\{1, 1, 2, 3, 5, 3, 6\}| = 5$. However, what happens when the number of elements of a set is infinite? Then we say that the cardinality of the set is infinite.

Definition 10. *The cardinality of a set that is not finite, is called infinite.*

There is nothing stopping a set from having other sets as members. For example,

- $\{\emptyset, \{'a', 'b'\}, \{'c', 'd'\}\}$, and
- $\{\{\emptyset\}\}$.

The elements of a set are left abstract and can be anything at all. The following operation is ubiquitous in computer science.

Definition 11. *Given a set A, the **power set** of A, denoted $\mathcal{P}(A)$, is the set of all subsets of A.*

Suppose $A = \{1, 2, 3\}$, then $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$. Later we will prove that if $|A| = n$, then $|\mathcal{P}(A)| = 2^n$. Exercises:

- What is $\mathcal{P}(\{\emptyset\})$? The set $\{\emptyset, \{\emptyset\}\}$.
- What is $\mathcal{P}(\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\})$? The set $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \{\emptyset, \{\emptyset\}\}, \{\{\emptyset\}, \{\{\emptyset\}\}\}, \{\emptyset, \{\{\emptyset\}\}\}, \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}\}$.

1.1 Operations on Sets

There are a number of set operations that allow us to construct other sets in terms of given sets.

Definition 12. *Suppose A and B are sets. Then the **union** of A and B is defined by $A \cup B = \{x \mid x \in A \vee x \in B\}$.*

Let $A = \{1, 2, 3\}$ and $B = \{4, 5, 6\}$, then $A \cup B = \{1, 2, 3, 4, 5, 6\}$. Suppose $A = \{1, 2, 3\}$ and $B = \{1, 5, 3\}$, then $A \cup B = \{1, 2, 3, 5\}$.

Note that union is defined in terms of disjunction, and this is important point to remember, because a lot of the same properties of disjunction extends to sets because of this.

Definition 13. *Suppose A and B are sets. Then the **intersection** of A and B is defined by $A \cap B = \{x \mid x \in A \wedge x \in B\}$.*

Let $A = \{1, 2, 3, 4\}$ and $B = \{3, 5, 1, 7\}$. Then $A \cap B = \{1, 3\}$. The set $\mathbb{N} \cap \{x \in \mathbb{Z} \mid x^2 < 100\} = \{x \in \mathbb{Z} \mid 0 \leq x \wedge x^2 < 100\}$.

Note that intersection is defined in terms of conjunction, and this is important point to remember, because a lot of the same properties of conjunction extends to sets because of this.

Definition 14. *Suppose A and B are sets. Then the* ***difference*** *of A and B is defined by $A - B = \{x \mid x \in A \wedge x \notin B\}$. Note that the difference operation is sometimes denoted by $A \backslash B$. The difference of A and B is sometimes called the complement of B with respect to A.*

If we fix a set U where all of our sets draw their elements from, then we can define the complement of a set. The set U is called the universal set or the universe of our sets. Thus, if U has been chosen, and we have a set A, then we know $A \subseteq U$.

Definition 15. *Let U be the universal set. Then the complement of a set A is defined by $\overline{A} = U - A$. Thus, the complement of a set A is the set of all elements that are not in A.*

If there is no universal set, then one can only speak about complements with respect to other sets which is the same as the set difference.

1.2 Set Theoretic Equivalences

Just as we saw in propositional logic there are a number of equivalences one can prove about sets. Note that all equivalences given in this section are with respect to equality of sets given above (Definition **??**). The following table lists a large number of set theoretic equivalences:

$A \cap U = A$ $A \cup \emptyset = A$	Identities
$A \cup U = U$ $A \cap \emptyset = \emptyset$	Domination laws
$A \cup A = A$ $A \cap A = A$	Idempotent laws
$\overline{(\overline{A})} = A$	Complementation law
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associativity laws
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributivity laws
$\overline{A \cup B} = \overline{A} \cap \overline{B}$ $\overline{A \cap B} = \overline{A} \cup \overline{B}$	De Morgan's laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption laws
$A \cup \overline{A} = U$ $A \cap \overline{A} = \emptyset$	Complement laws

We now prove a few of these. There are other example proofs in the book on page 130.

Lemma 16 (Complementation Law)**.** *Show that $\overline{(\overline{A})} = A$.*

Proof. Suppose A is an arbitrary set. Then we must show that $\overline{(\overline{A})} \subseteq A$ and that $A \subseteq \overline{(\overline{A})}$. Consider the former, then we must prove the following formula holds:

$$
\begin{array}{rcl}
\forall x \in \overline{(\overline{A})}.x \in A & \Leftrightarrow & \forall x \in \overline{U - A}.x \in A \\
& \Leftrightarrow & \forall x \in (U - (U - A)).x \in A \\
& \Leftrightarrow & \forall x \in \{y \in U \mid y \notin (U - A)\}.x \in A \\
& \Leftrightarrow & \forall x \in \{y \in U \mid y \notin \{z \in U \mid z \notin A\}\}.x \in A \\
& \Leftrightarrow & \forall x \in \{y \in U \mid \neg(y \in \{z \in U \mid z \notin A\})\}.x \in A \\
& \Leftrightarrow & \forall x \in \{y \in U \mid \neg(y \in U \wedge y \notin A)\}.x \in A \\
& \Leftrightarrow & \forall x \in \{y \in U \mid (y \notin U \vee \neg(y \notin A))\}.x \in A \\
& \Leftrightarrow & \forall x \in \{y \in U \mid (y \notin U \vee \neg(\neg(y \in A)))\}.x \in A \\
& \Leftrightarrow & \forall x \in \{y \in U \mid (y \notin U \vee \neg(\neg(y \in A)))\}.x \in A \\
& \Leftrightarrow & \forall x \in \{y \in U \mid (y \notin U \vee y \in A)\}.x \in A \\
& \Leftrightarrow & \forall x \in \{y \in U \mid y \in A\}.x \in A \\
& \Leftrightarrow & \forall x \in \{y \in U \mid y \in A\}.x \in A \\
& \Leftrightarrow & \forall x \in A.x \in A
\end{array}
$$

Thus, it is the case that $\overline{(\overline{A})} \subseteq A$. The other direction is similar and left to the reader. □

We could have also prove the previous lemma simply by the following reasoning:

Suppose A is an arbitrary set. Then

$$
\begin{array}{rcl}
\overline{(\overline{A})} & = & U - \overline{A} \\
& = & U - (U - A) \\
& = & \{y \in U \mid y \notin \{z \in U \mid z \notin A\}\} \\
& = & \{y \in U \mid y \notin \{z \mid z \in U \wedge z \notin A\}\} \\
& = & \{y \in U \mid y \notin U \vee \neg(y \notin A)\} \\
& = & \{y \in U \mid y \notin U \vee \neg\neg(y \in A)\} \\
& = & \{y \in U \mid y \notin U \vee y \in A\} \\
& = & \{y \in U \mid y \in A\} \\
& = & A
\end{array}
$$

However, make sure the when an informal proof is complete that each step is trivial to follow. This makes sure that the proof is easy to understand and there are no errors.

We can give yet another proof of the previous fact.

> Suppose $x \in \overline{(\overline{A})}$. Then we must show that $x \in A$. We know by definition that if $x \in \overline{(\overline{A})}$, then $x \notin \overline{A}$. The latter is equivalent to $\neg(x \in \overline{A})$ which is equivalent to $\neg(x \notin A)$, but this is also equivalent to $\neg(\neg(x \in A))$. Thus, by the law of double negation we know that $\neg(\neg(x \in A))$ is equivalent to $x \in A$.
>
> Now suppose $x \in A$. Then we must show that $x \in \overline{(\overline{A})}$. We know by the law of double negation that $x \in A$ if and only if $\neg(\neg(x \in A))$. Now the latter yields:
>
> $$
> \begin{array}{rcl}
> \neg(\neg(x \in A)) & \text{iff} & \neg(x \notin A) \\
> & \text{iff} & \neg(x \in \overline{A}) \\
> & \text{iff} & x \notin \overline{A} \\
> & \text{iff} & x \in \overline{(\overline{A})}
> \end{array}
> $$
>
> Therefore, $\overline{(\overline{A})} = A$.

The previous two are the most common types of proofs of these problems. The book has a nice membership table notation that is very helpful as well. See the book for other example proofs of some of the other laws.

1.3 Generalized Union and Intersection

Suppose we have a series of sets $A_1, \ldots, A_n$ for some $n \in \mathbb{N}$. How could we union together all of these sets? For small n,say $n = 3$, we could just write down $A_1 \cup A_2 \cup A_3$, but what if n is very large? There happens to be a special notation:

Definition 17. *Suppose I is a set, and for each $i \in I$ we have a set A_i. Then the* ***generalized union*** *of all the sets A_i is defined as follows:*

$$\bigcup_{i \in I} A_i = \{x \mid \exists i \in I . x \in A_i\}$$

Note that this definition works for even an infinite series of sets. When we have a series of sets A_i for each $i \in I$ we say that sets A_i are **indexed** over the set I. We call I the **index set**.

We can do the same for intersection.

Definition 18. *Suppose I is a set, and for each $i \in I$ we have a set A_i. Then the* ***generalized intersection*** *of all the sets A_i is defined as follows:*

$$\bigcap_{i \in I} A_i = \{x \mid \forall i \in I . x \in A_i\}$$

Suppose $A_i = \{i, i+1, \cdots\}$ for some $i \in \mathbb{N}$. Then consider the following:

i. $\bigcup_{i \in \mathbb{N}} A_i = \mathbb{N}$

ii. $\bigcap_{i \in \mathbb{N}} A_i = \emptyset$

We prove the following lemmata:

Lemma 19. *Suppose $I = \{1, 2, \ldots, n\}$ is a finite indexed set where $n \in \mathbb{N}$ and A_i is a series of sets for each $i \in I$. Then*

$$\bigcup_{i \in I} A_i = A_1 \cup \cdots \cup A_n$$

Proof. Suppose $I = \{1, 2, \ldots, n\}$ is a finite indexed set where $n \in \mathbb{N}$ and A_i is a series of sets for each $i \in I$. Then we know the following by the definition of union:

$$A_1 \cup \cdots \cup A_n = \{x \mid x \in A_1 \vee \cdots \vee x \in A_n\}$$

If the proposition $x \in A_1 \vee \cdots \vee x \in A_n$ is true, then there must exist at least one set A_i for some $i \in I$ such that $x \in A_i$. Thus, the proposition $x \in A_1 \vee \cdots \vee x \in A_n$ is equivalent to the proposition $\exists i \in I . x \in A_i$. Thus, we know

$$\begin{aligned} A_1 \cup \cdots \cup A_n &= \{x \mid x \in A_1 \vee \cdots \vee x \in A_n\} \\ &= \{x \mid \exists i \in I . x \in A_i\} \\ &= \textstyle\bigcup_{i \in I} A_i. \end{aligned}$$

Therefore, $\bigcup_{i \in I} A_i = A_1 \cup \cdots \cup A_n$. □

Lemma 20. *Suppose $I = \{1, 2, \ldots, n\}$ is a finite indexed set where $n \in \mathbb{N}$ and A_i is a series of sets for each $i \in I$. Then*

$$\bigcap_{i \in I} A_i = A_1 \cap \cdots \cap A_n$$

Proof. Suppose $I = \{1, 2, \ldots, n\}$ is a finite indexed set where $n \in \mathbb{N}$ and A_i is a series of sets for each $i \in I$. Then we know the following by the definition of union:

$$A_1 \cap \cdots \cap A_n = \{x \mid x \in A_1 \wedge \cdots \wedge x \in A_n\}$$

If the proposition $x \in A_1 \wedge \cdots \wedge x \in A_n$ is true, then there for every set $i \in I$, $x \in A_i$. Thus, the proposition $x \in A_1 \wedge \cdots \wedge x \in A_n$ is equivalent to the proposition $\forall i \in I . x \in A_i$. Thus, we know

$$\begin{aligned} A_1 \cap \cdots \cap A_n &= \{x \mid x \in A_1 \wedge \cdots \wedge x \in A_n\} \\ &= \{x \mid \forall i \in I . x \in A_i\} \\ &= \textstyle\bigcap_{i \in I} A_i. \end{aligned}$$

Therefore, $\bigcap_{i \in I} A_i = A_1 \cap \cdots \cap A_n$. □

2 Tuples and Cartesian Product

In this section we define the notion of a tuple, and a new set theoretic operation called cartesian product which can be used to construct sets of tuples from other sets. Consider the following version of a truth table:

	1	2	3	4
p	$False$	$False$	$True$	$True$
q	$False$	$True$	$False$	$True$
$p \wedge q$	$False$	$False$	$False$	$True$

This truth table has each row labeled by a formula, instead of the columns, and then the columns consist of a particular value assignment to the variables. For example, column one represents assigning the value $False$ to p, and $False$ to q, and thus, $p \wedge q$ is assigned $False$. How would we model these types of truth tables using set theory?

We need a way to relate the rows to the columns and then those to the particular assignment. For example, we can see by the table that at row p and column 3 the assignment is $True$. Sets relate objects with a particular property and so one might first try cleverly constructing a set of sets to model the table where we model each coordinate in the table by a set. For example, the coordinate mentioned above would be modeled by the set $\{p, 3, True\}$, which means, choose row p, and then column 3, and the value at the coordinate is $True$. Another example might be $\{q, 2, False\}$.

Is this a good model? The answer is no, and the reason is that given a coordinate at a set we really do not have a way of determining which of the elements are the row, the column, and the value, because sets are unordered. That is, the coordinate $\{p, 3, True\} = \{3, p, False\}$. So we need a way to enforce an order on the set, and we can do this using a device called a tuple.

Definition 21. *A n-**tuple**, or sometimes just a tuple, is an ordered sequence of objects denoted $(a_1, \ldots, a_n)$. We call 2-tuples **pairs** or **coordinates**.*

Note that the syntax for tuples works in Haskell directly. The definition of n-tuple enforces an ordering on the objects. The object a_1 is considered first, and always first, and the object a_n is last. Thus, the pair $(1, 2) \neq (2, 1)$ which is not true about the sets $\{1, 2\} = \{2, 1\}$. Furthermore, sequences can have repeated objects, for example, $(1, 2, 3, 3) \neq (1, 2, 3)$.

Definition 22. *Suppose $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ are two n-tuples. Then we say they are equivalent if and only if $a_1 = b_1$, $a_2 = b_2$, $\ldots$, $a_n = b_n$. We denote this by $(a_1, \ldots, a_n) = (b_1, \ldots, b_n)$. This is known as **point wise** equivalence of tuples.*

Getting back to our example we now have a way to enforce a relationship between objects with an ordering. So we can model the coordinates of our example truth table from above using tuples. For example, $(p, 3, True)$ is the location in the table at row p, column 3, which has a value of $True$. Then we simply collect all of these coordinates into a tuple. The following tuple models the table given above:

$$((p,1,False),(p,2,False),(p,3,True),(p,4,True),$$
$$(q,1,False),(q,2,True),(q,3,False),(q,4,True),$$
$$(p \wedge q,1,False),(p \wedge q,2,False),(p \wedge q,3,False),$$
$$(p \wedge q,4,True))$$

Therefore, tuples are used to enforce a relationship between a sequence of objects that rely on a particular order. In fact, we can think of the above set as a primitive database. Note that the set above is the set theoretic version of association lists from Haskell.

Given two sets A and B it is possible to define all the possible pairs of objects from A and B.

Definition 23. *Suppose A and B are two sets. Then the **cartesian product** of A and B is defined as follows:*

$$A \times B = \{(a,b) \mid a \in A \text{ and } b \in B\}$$

We now give several examples.
Example 24.

i. $\{0,1\} \times \{a,b\} = \{(0,a),(0,b),(1,a),(1,b)\}$

ii. $\emptyset \times \{1\} = \emptyset$

iii. $\{1\} \times \emptyset = \emptyset$

iv. $(\{1,0\} \times \{a,b\}) \times \{c\} = \{(0,a),(0,b),(1,a),(1,b)\} \times \{c\} = \{((0,a),c),((0,b),c),((1,a),c),((1,b),c)\}$

3 Relations

The cartesian product allows for the definition of one of the most important and highly used structures in computer science.

Definition 25. *A **binary relation** on the sets A and B is a subset $r \subseteq A \times B$ of the cartesian product of A and B.*

The intuition of a relation is to relate the objects of A to the objects of B just as we did in the previous section modeling truth tables. There the relationship was propositional formulas to truth values. The definition above defines binary relations, but relations relating more than two sets can be constructed, but we only consider the binary case here.

The definition of binary relation is with respect to two sets A and B which may be distinct. However, it is more common in computer science that A and B are actually the same set.

Definition 26. *A **binary relation over** A is a binary relation $r \subseteq A \times A$.*

Binary relations over a set A are the most common, and we will restrict our attention to these types of binary relations for the remainder of this section.

Example 27.

- *The game rock-paper-scissors-lizard-spock:*

$$\mathcal{G} = \{(ROCK, SCISSORS),(ROCK, LIZARD),$$
$$(PAPER, ROCK),(PAPER, SPOCK),$$
$$(SCISSORS, PAPER),(SCISSORS, LIZARD),$$
$$(LIZARD, PAPER),(LIZARD, SPOCK),$$
$$(SPOCK, ROCK),(SPOCK, SCISSORS)\}$$

- *Zombie Athletes. A **speeder zombie** – the scariest zombie one can think of – is a zombie with the following abilities:*
  - *Have all their limbs,*
  - *fast runner,*
  - *can climb, and*
  - *can jump high.*

  Suppose S is the set of all speeder zombies, and Z is the set of zombies with arms and legs that were track and field athletes when they were human. Clearly, $Z \subset S$.

  Now we can define the following relation:

  $$\mathsf{SameTeam} \subseteq Z \times Z$$
  $$\mathsf{SameTeam} = \{(z_1, z_2) \mid z_1 \text{ was on the same team as } z_2\}$$

It is very common to denote the fact that $(a, b) \in R$ for some binary relation R over A by aRb that is read "a is related to b with respect to R." This is called **infix** notation. Sometimes we also denote the same relation by $R(a, b)$ which is called **prefix** notation. For example, we can state that Spock beats rock by SPOCK $\mathcal{G}$ ROCK or by $\mathcal{G}$ (SPOCK, ROCK).

Depending on the relationship one wishes to make a relation may need to satisfy different properties. For example, the less-than-or-equal-to relation over the set of natural numbers has the property that for any $n \in \mathbb{N}$, $n \leq n$. However, the strictly less than relation over the natural numbers does not satisfy that property. We now state all of the most important properties of binary relations:

i. **Reflexivity**. A binary relation R over A is **reflexive** if and only if for any $a \in A$, aRa.

ii. **Symmetry**. A binary relation R over A is **symmetric** if and only if for any $a, b \in A$, aRb implies bRa.

iii. **Transitivity**. A binary relation R over A is **transitive** if and only if for any $a, b, c \in A$, aRb and bRc implies aRc.

iv. **Antisymmetry**. A binary relation R over A is **antisymmetric** if and only if for any $a, b \in A$, aRb and bRa implies $a = b$.

There are many example relations that one can come up with that have some of the above properties or even none.

Example 28.

i. Suppose $A = \{a, b, c\}$. Then the relation R over A defined as $R = \{(a, b), (b, c), (c, c), (c, a)\}$ is not reflexive, transitive, symmetric or even antisymmetric.

ii. Suppose $A = \{a, b, c\}$. Then the relation R over A defined as $R = \{(a, a), (b, c), (a, b), (b, c), (c, c), (c, a)\}$ is reflexive, but not transitive, symmetric or antisymmetric.

iii. Suppose $A = \{a, b, c\}$. Then the relation R over A defined as $R = \{(a, b), (b, a), (b, c), (c, b), (c, c), (a, c)(c, a)\}$ is not reflexive, transitive, or antisymmetric, but it is symmetric.

iv. Suppose $A = \{a, b, c\}$. Then the relation R over A defined as $R = \{(a, b), (b, c), (a, c), (c, c)\}$ is not reflexive, symmetric or antisymmetric, but it is transitive.

v. The relation $isMarriedTo$ over the set of all people is symmetric, but not antisymmetric.

Now we consider a few proofs.

Lemma 29. *Show that the strictly less-than relation on the natural numbers is transitive.*

Proof. We must prove that $\forall l, n, m \in \mathbb{N}$, if $l < n$ and $n < m$, then $l < m$. Suppose $n, m \in \mathbb{N}$, and that $l < n$ and $n < m$. Then there must exist non-zero natural numbers $k_1, k_2 \in \mathbb{N}$ such that $n = l + k_1$ and $m = n + k_2$. This then implies that $l = n - k_1$. Since we know $k_1 > 0$ and $k_2 > 0$ by assumption we know that $n - k_1 < n + k_2$ which is equivalent to $l < m$. Therefore, the strictly less-than relation over the natural numbers is transitive. □

Lemma 30. *Show that the strictly less-than relation on the natural numbers is anti-symmetric.*

Proof. We must prove that $\forall n, m \in \mathbb{N}$, if $n < m$ and $m < n$, then $n = m$. We use proof by contradiction. Suppose $n, m \in \mathbb{N}$, $n < m$, $m < n$, and $n \neq m$. We know that $n < m$ and $m < n$, thus there must exist non-zero natural numbers $k_1, k_2 \in \mathbb{N}$ such that $m = n + k_1$ and $n = m + k_2$. This implies that $m = n - k_2$. Now using substitution we may conclude that $n - k_2 = n + k_1$ which implies that $n = n + k_1 + k_2$ which is impossible because $k_1 > 0$ and $k_2 > 0$; a contradiction. Therefore, the strictly less-than relation over the natural numbers is anti-symmetric. □

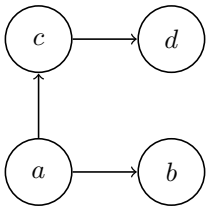
There are a special class of binary relations that capture the notion of being equivalent.

Definition 31. *A binary relation R over A is an **equivalence relation** if and only if R is reflexive, symmetric, and transitive.*

Example 32. *Notice that the subset operator on sets is a binary relation over the collection of all sets. That is, a set A is related to B if and only if $A \subseteq B$. We can define a new relation on sets, $R = \{(A, B) \mid A \subseteq B \wedge B \subseteq A\}$. The relation R is an equivalence relation. In fact, it is by definition the equality for sets.*

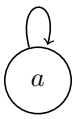
Exercise: Prove that R is an equivalence relation.

Relations have a nice graphical presentation. Consider the relation $R = \{(a, b), (c, d), (a, c)\}$. We can present this relation as follows:

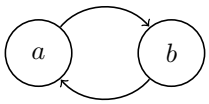


This style of digram is called the **graph** of the relation. Each element of the set the relation is over becomes a label in a circle called a **node**, and then if aRb holds, then there is an arrow connecting the node labeled by a to the node labeled by b.

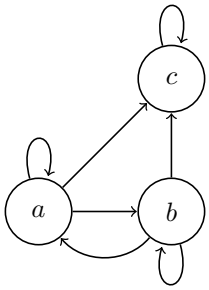
Consider the trivial relation $R = \{(a, a)\}$ then this can be represented by the diagram:



The graph of the relation $R = \{(a, b), (b, a)\}$ is as follows:



The graph of the relation $R = \{(a,a),(a,b),(b,a)(b,b),(c,c),(b,c),(a,c)\}$ is as follows:



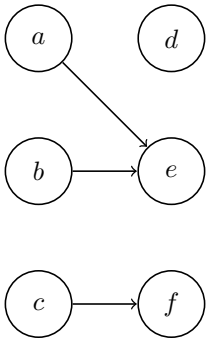
The biggest down fall of the graph representation is that the anti-symmetric property does not have a nice graphical representation.

Graphs have lots of applications in computer science. For example, they can be used to compute the shortest path between two points; see `http://en.wikipedia.org/wiki/Dijkstra's_algorithm`. For more example applications of graphs see `http://www.cs.xu.edu/csci390/12s/IJEST10-02-09-124.pdf`. Graphs will be heavily used in CSCI:3500 to model computation and modern day computational devices.

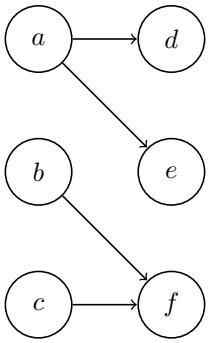
4 Functions

READ CHAPTER 2.3

Suppose we have the relation $R \subseteq A \times B$ for some set $A = \{a,b,c\}$ and $B = \{d,e,f\}$. Furthermore, assume that for any $a \in A$ there exists exactly one $b \in B$ such that aRb. For example, the relation defined by the following graph adheres to this property:



However, the following relation does not adhere to this property:



Notice that the property, for any $a \in A$ there exists exactly one $b \in B$ such that aRb, enforces that every element of A must be related to something in B, but not every element of B must be related to. Furthermore, no element of A can be related to two elements of B. Does this property sound familiar?

The property we have been describing is the property of a mathematical function.

Definition 33. *A **function**, $f : A \to B$, is a relation $f \subseteq A \times B$ with the property that for any $a \in A$ there exists exactly one $b \in B$ such that $(a, b) \in f$. We denote the latter by $f(a) = b$. The sets A and B are called the **domain** and **codomain** of f respectively. When $f(a) = b$ we say that f **maps** a to b, and call b the **image** of a and a the **preimage** of b.*

Every Haskell program written during this course is an example of a function. See the book for other examples Section 2.3.

There are a few properties of functions that are important.

Definition 34. *The **image** of $S \subseteq A$ under $f : A \to B$ is the set*

$$f(S) = \{t \in B \mid \exists s \in S.f(s) = t\}$$

For example, suppose $f(x) = x^2$ is a function from the natural numbers to itself, and $S = \{3, 5, 7\}$. Then $f(S) = \{9, 25, 49\}$. Notice that computing the image of a subset of A under some function, f, is essentially equivalent of mapping f across S when we represent sets using lists in Haskell.

Definition 35. *A function $f : A \to B$ is **injective** (or one-to-one) iff for all $a_1, a_2 \in A$, $f(a_1) = f(a_2)$ implies $a_1 = a_2$.*

An injective function is one in which every element of the codomain is mapped to exactly one element of the domain.

Example 36. *Consider the function $f = \{(a, 1), (b, 3), (c, 2)\}$. As we can see every element of the codomain is mapped to by exactly one element of the domain. Thus, f is injective.*

The function $f : \mathbb{N} \to \mathbb{N}$ defined by $f(x) = x^2$ is injective. Suppose $n, m \in \mathbb{N}$ and that $f(n) = f(m)$. Then $n^2 = m^2$ which implies that $n = m$ by taking the square root of both sides.

Now suppose that $f : \mathbb{R} \to \mathbb{R}$ and is defined as above. Then it turns out that f is no longer injective, because $f(3) = f(-3)$, but $3 \neq -3$.

Definition 37. *A function $f : A \to B$ is **surjective** (or onto) iff for all $b \in B$, there exists at least one $a \in A$ such that $f(a) = b$.*

A surjective function is one in which every element of the codomain is mapped to by at least one element of the domain.

Example 38. *Consider the function* $f = \{(a,1),(b,3),(c,2),(d,2),(e,1)\}$ *whose domain is* $\{a,b,c,d,e\}$ *and codomain is* $\{1,2,3\}$. *As we can see every element of the codomain is mapped to by at least one element of the domain. Thus,* f *is surjective.*

Consider the function $f = \{(a,1),(b,3),(c,3),(d,1),(e,1)\}$ *whose domain is* $\{a,b,c,d,e\}$ *and codomain is* $\{1,2,3\}$. *Then this function does not map anything to the element* 2 *in the codomain. Thus, this function is not surjective.*

Proving that a function is injective is usually easier than proving that a function is surjective, because the latter requires one to start with an arbitrary element of the codomain and then find an element of the domain. Existence proofs like these are usually non-trivial.

Definition 39. *A function* $f : A \to B$ *is called a* ***bijection*** *iff it is injective and surjective.*

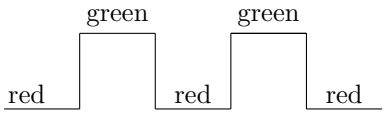
A bijection is a function where every element of the codomain is mapped to by exactly one element of the codomain. Thus, every element of the codomain is used in the definition of the function.

Definition 40. *Suppose* $f : A \to B$ *and* $g : B \to C$ *are two functions. Then we can define a new function denoted by* $g \circ f : A \to C$ *define by* $(g \circ f)(x) = g(f(x))$ *called the* ***composition*** *of* f *and* g. *The notation* $g \circ f$ *is often read as "*f *before* g*" or "* f *composed with* g*".*

Example 41. *Suppose that* f *and* g *are two functions from* $\mathbb{N}$ *to* $\mathbb{N}$ *defined by* $f(x) = x^2$ *and* $g(x) = x + \pi$. *Then* $(g \circ f)(x) = g(f(x)) = x^2 + \pi$.

5 Sequences and Summations

Sequences are ubiquitous in computer science. As an example consider modern day subway trains. Signals are placed a particular spots along the track to guide train conductors. If a signal is green then the train is free to pass, but if the signal is red then on coming traffic is coming and the train must halt. Suppose we need to model such a signaling network and verify that it always works, then how do model the signal? Let us assume that the signal is always on, and hence, electricity is always flowing. Furthermore, we assume that the signal is default red, and then when the electricity increases it switches to green. Thus, we can model the operational behavior by a constant flow of electricity. When the electricity is low then the signal will be red, and when the electricity is high, then the signal will be green. This situation is depicted by the following diagram:



We can model this situation by using what is called a sequence. A sequence can be thought of as an infinite tuple of objects written as follows:

$$a_1, a_2, \ldots, a_n, \ldots$$

The signal can now be modeled by a sequence of zeros and ones. When the signal is low the sequence is all zeros, and when the signal is high then the sequence is all ones:

$$\underbrace{0,0,0,0,0,0}_{red},\underbrace{1,1,1,1,1,1,1}_{green},\underbrace{0,0,0,0,0,0,0}_{red},\underbrace{1,1,1}_{green},\underbrace{0,0,0,0}_{red},\ldots$$

Now we give the formal definition of a sequence.

Definition 42. *A* ***sequence*** *is a function* $s : \mathbb{N} \to A$ *where* A *is the set of elements of the sequence. We often denote the nth element of the sequence as* $s_n = s(n)$.

We cannot denote a sequence by a tuple, because there may be an infinite number of elements in the sequence. A function makes this possible.

Sequences are also found in mathematics. Consider the following recursively defined function:

$$\begin{aligned} f(0) &= 1 \\ f(1) &= 1 \\ f(n) &= f(n-1) + f(n-2) \end{aligned}$$

This sequence defines what is called the Fibonacci sequence and it amounts to the following:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots$$

The Fibonacci sequence has many applications and has even been found to arise in nature – see `http://en.wikipedia.org/wiki/Fibonacci_number`. Sequences such as f above are sometimes written as follows:

$$\begin{aligned} F_0 &= 1 \\ F_1 &= 1 \\ F_2 &= F_{n-1} + F_{n-2} \end{aligned}$$

Consider a second example. Suppose we have the sequence defined by $b_n = (-1)^n$. This sequence looks like the following:

$$1, -1, 1, -1, 1, -1, 1, -1, 1, -1, \ldots$$

Given a prefix of an sequence sometimes one must find the general pattern. This is a very common logic problem. However, it can be exceedingly difficult. Suppose one is given the following prefix:

$$\begin{aligned} F_0 &= 2 \\ F_1 &= 2 \\ F_2 &= 5 \\ F_3 &= 19 \\ F_4 &= 85 \end{aligned}$$

Find F_5. There could be an infinite number of sequences with this prefix and so finding the general formula is very difficult. It turns out that the general formula is the following:

$$\begin{aligned} F_0 &= 2 \\ F_n &= nF_{n-1} + (n-1)^2 \end{aligned}$$

The rest of the sequence is then:

$$2, 2, 5, 19, 85, 441, 2671, 18733, 149913, \ldots$$

There two very common sequences that we define next.

Definition 43. *Given real numbers a and r, called the initial term and common ratio respectively, we define a **geometric progression** as follows:*

$$a, ar, ar^2, \ldots, ar^n, \ldots$$

As an example the sequence $b_n = (-1)^n$ is a geometric progression where $a = 1$ and $r = -1$. Another example is the sequence $b_n = 6 * (1/3)^n$ where $a = 6$ and $r = 1/3$.

Definition 44. *An **arithmetic progression** is a sequence of the form*

$$a, a + d, a + 2d, \ldots, a + nd, \ldots$$

An example is the sequence $F_n = 42 + 7n$, and the sequence $F_n = 72 - 9n$.

5.1 Summations

It is very common to take the sum of a sequence. Suppose

$$a_m, \ldots, a_n, \ldots$$

is a sequence. Then its sum is denoted $\sum_{j=m}^{n} a_j = a_m + \cdots + a_n$. The variable j is called the **index** of the sum and the variable m is called the **upper bound**. The sum is said to start at the **lower limit** of the sequence, here m, and progress to the **upper limit** of the sequence, here n.

All of the usual laws of addition hold for summations and they can be given direct proofs. For example, the distributive law for addition holds: $\sum_{j=0}^{n}(ax_j + by_j) = a\sum_{j=0}^{n} x_j + b\sum_{j=0}^{n} y_j$. We will prove these below, but we first must introduce a new proof technique called mathematical induction.

Many summations are equivalent to what are called **closed formulas** which are formulas for the sum of the sequence without any summation symbols. Consider the summation $\sum_{j=1}^{n} j = 1 + 2 + 3 + \ldots + n$ what closed formula does this summation equal? First, consider the arbitrary sequence:

$$a_1, a_2, a_3, a_4, \ldots, a_{n-3}, a_{n-2}, a_{n-1}, a_n$$

there are exactly n elements in this sequence. How many elements are in the following sequence:

$$(a_1, a_n), (a_2, a_{n-1}), (a_3, a_{n-2}), (a_4, a_{n-3}), \ldots$$

There are exactly half of the number elements in this sequence than in the original sequence. Thus, there are exactly $n/2$ elements in this sequence. Now using this intuition we can simplify the following equation:

$$\begin{aligned}
&\textstyle\sum_{j=1}^{n} j \\
&= 1 + 2 + 3 + 4 + \cdots + (n-3) + (n-2) + (n-1) + n \\
&= (1 + n) + (2 + (n-1)) + (3 + (n-2)) + (4 + (n-3)) + \ldots \\
&= (n+1) + (n+1) + (n+1) + (n+1) + \ldots \\
&= (n/2)(n+1)
\end{aligned}$$

Therefore, $\sum_{j=1}^{n} = \frac{n(n+1)}{2}$. There are lots of other common equations like these see Table 2 on page 166 of the book.

6 Mathematical Induction

The proof that $\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$ was only a sketch and we would like it to be more rigors. To make it more rigorous we need a new proof technique that is very powerful called mathematical induction. This proof technique allows one to prove formulas of the form $\forall n.P(n)$, for example, $n! \leq n^n$ for every natural number n.

Proofs using mathematical induction have two parts: i. the base case where we prove the formula holds for 1, and ii. the step case where we assume the formula holds for the case of n and prove that the formula holds for $n + 1$ using the fact that we have assumed that it holds for n. Suppose we wanted to prove that $\forall n.P(n)$ holds by mathematical induction. Then we would first prove that $P(1)$ holds, we prove that $\forall k.P(k) \Rightarrow P(k+1)$ holds, and if both of these hold, then $\forall n.P(n)$ holds by mathematical induction. In fact, we can formulate an inference rule for mathematical induction as follows:

$$\frac{P(1) \qquad \forall k.(P(k) \Rightarrow P(k+1))}{\forall n.P(n)}\ \text{IN}$$

At this point we give an intuitive way of understanding mathematical induction. Suppose we have an infinite ladder and we want to prove that we can reach any step on the ladder where we only know these two facts:

1. We can reach the first step of the ladder.
2. If we can reach a particular step of the ladder, then we can reach the next step.

Can we now conclude that we can reach every step? Can we reach the first step? Yes, because by the first fact we know we can reach the first step. How about the second step? Well, since we know we can reach step one, we can use fact two to conclude that we can reach the second step. How about step three? Since we know we can reach step two, we can use the second fact to conclude that we can reach step three. Using reasoning like this we can prove that we can reach any step. The two facts above capture exactly the base case (fact one) and the step case (fact two) of a mathematical inductive argument.

We now give several examples using mathematical induction.

Theorem 45. *Show that for any $n \in \mathbb{N}$, $\Sigma_{j=1}^{n} j = \frac{n(n+1)}{2}$.*

Proof. This is a proof by mathematical induction on n.

Base Case. We must show the following:

$$\Sigma_{j=1}^{1} = \frac{1(1+1)}{2} = \frac{2}{2}$$

Clearly, it is the case that $\Sigma_{j=1}^{1} = 1 = \frac{2}{2}$.

Step Case. We now must state the induction hypothesis which is the assumption that $\Sigma_{j=1}^{n} j = \frac{n(n+1)}{2}$ holds for some $n \in \mathbb{N}$. Then it suffices to show that

$$\Sigma_{j=1}^{n+1} j = \frac{(n+1)((n+1)+1)}{2} = \frac{(n+1)(n+2)}{2}$$

holds using the induction hypothesis. This follows from the following reasoning:

$$\begin{array}{rcll} \Sigma_{j=1}^{n+1} j & = & 1+2+3+\cdots+n+(n+1) & \text{(Def. of Summation)} \\ & = & (1+2+3+\cdots+n)+(n+1) & \text{(Associativity of Addition)} \\ & = & \Sigma_{j=1}^{n} j + (n+1) & \text{(Def. of Summation)} \\ & = & \frac{n(n+1)}{2} + (n+1) & \text{(Induction Hypothesis)} \\ & = & \frac{n(n+1)+2(n+1)}{2} & \text{(Basic Algebra)} \\ & = & \frac{(n+1)(n+2)}{2} & \text{(Basic Algebra)} \end{array}$$

□

Theorem 46. *Show that for any $n \in \mathbb{N}$, $\Sigma_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}$.*

Proof. This is a proof by mathematical induction on n.

Base Case. We must show the following:

$$\Sigma_{j=1}^{1} j^2 = \frac{1(1+1)(2(1)+1)}{6} = \frac{6}{6} = 1$$

Clearly, $\Sigma_{j=1}^{1} j^2 = 1^2 = 1$.

Step Case. We now must state the induction hypothesis which is the assumption that

$$\Sigma_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6} \quad \text{(IH)}$$

holds for some $n \in \mathbb{N}$. Then it suffices to show that

$$\Sigma_{j=1}^{n+1} j^2 = \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6} = \frac{(n+1)(n+2)(2n+3)}{6}$$

holds using the induction hypothesis. This follows from the following reasoning:

$$\begin{array}{lll}
\Sigma_{j=1}^{n+1} j^2 & = & 1^2 + 2^2 + 3^2 + \cdots + n^2 + (n+1)^2 \quad \text{(Def. of Summation)} \\
& = & \Sigma_{j=1}^{n} j^2 + (n+1)^2 \quad \text{(Def. of Summation)} \\
& = & \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \quad \text{(Induction Hypothesis)} \\
& = & \frac{n(n+1)(2n+1)+6(n+1)^2}{6} \quad \text{(Basic Algebra)} \\
& = & \frac{(n+1)(n(2n+1)+6(n+1))}{6} \quad \text{(Basic Algebra)} \\
& = & \frac{(n+1)(2n^2+n+6n+6))}{6} \quad \text{(Basic Algebra)} \\
& = & \frac{(n+1)(2n^2+7n+6))}{6} \quad \text{(Basic Algebra)} \\
& = & \frac{(n+1)(n(2n)+3n+4n+2(3))}{6} \quad \text{(Basic Algebra)} \\
& = & \frac{(n+1)(n+2)(2n+3)}{6} \quad \text{(Basic Algebra)}
\end{array}$$

□

Theorem 47. *Show that for any lists* `l1` *and* `l2`, `length(l1 ++ l2)` = `length(l1)` + `length(l2)`.

Proof. The is a proof by mathematical induction on `l1`. We keep `l2` constant throughout the proof.

Base Case. We must show that the result holds for `l` = `[]`:

$$\begin{array}{lll}
\texttt{length([] ++ l')} & = & \texttt{length(l')} \\
& = & 0 + \texttt{length(l')} \\
& = & \texttt{length([])} + \texttt{length(l')}
\end{array}$$

Step Case. We assume the inductive hypothesis:

$$\texttt{length(l1 ++ l2)} = \texttt{length(l1)} + \texttt{length(l2)} \quad \text{(IH)}$$

for some `l1`. Then we must show the following using the inductive hypothesis:

$$\texttt{length((x:l1) ++ l2)} = \texttt{length(x:l1) ++ length(l2)}$$

This follows from the following reasoning:

$$\begin{array}{lll}
\texttt{length((x:l1) ++ l2)} & = & \texttt{length(x:(l1 ++ l2))} \\
& = & 1 + \texttt{length(l1 ++ l2)} \\
& = & 1 + \texttt{length(l1) ++ length(l2)} \\
& = & (1 + \texttt{length(l1)}) \texttt{ ++ length(l2)} \\
& = & \texttt{length(x:l1) ++ length(l2)}
\end{array}$$

□