ASILATA BAPAT AND ANAND DEOPURKAR

GAMES, GRAPHS, AND MACHINES

Contents

Some foundations

We begin by briefly introducing some language to talk about the objects we will encounter in this course. We will revisit this foundational material several times throughout the course in several contexts.

Sets

Informally, a *set* is an unordered collection of objects with no repetitions. This is the most basic object usually used to discuss almost every construction in mathematics. If T is a set and x is any object, we have the following dichotomy[1]: either x is an element of T, denoted $x \in T$, or x is not an element of T, denoted $x \notin T$. Two sets are equal if and only if they have the same elements. That is, every element of the first set is an element of the second set, and vice versa.

[1] A situation in which exactly one of two possible options is true.

The Zermelo–Fraenkel axioms can be used to develop this theory more formally, but we will not go into the details in this course.

We use the following notation for some standard sets of numbers:

1. $\mathbf{N}$ is the set of natural numbers $\{1, 2, 3, \dots, \}$.
2. $\mathbf{Z}$ is the set of integers $\{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$.
3. $\mathbf{Q}$ is the set of rational numbers.
4. $\mathbf{R}$ is the set of real numbers.
5. $\mathbf{C}$ is the set of complex numbers.

Sets are often denoted by capital letters such as S, T, and potential elements as small letters x, y[2]. If we are listing all the elements of a set, we put them in curly braces, for example $\{1, 2, 3, 4\}$. We can also specify a set by taking all elements of another set that satisfy a particular property, for example $\{x \in \mathbf{N} \mid x \text{ is even}\}$.

[2] This is just a convention. In fact, sets are often elements of other sets, so there is no clear distinction between sets and potential elements.

A set S is a *subset* of a set T, denoted $S \subset T$, if every element of S is also an element of T. A set U is a *superset* of a set T, denoted $U \supset T$, if every element of T is also an element of U. There is a unique set that contains no elements. It is called *the empty set* and is denoted $\emptyset$. The empty set is vacuously[3] a subset of every set.

[3] We say that a statement of type "if ... then ...", or equivalently "for every ... we have ..." is *vacuously true* if nothing satisfies the "if" or "for every" condition.

The *size* or *cardinality* of a set is the number of elements in the set. If the number of elements is infinite, then we say that the set is infinite, and its cardinality is ∞.

Here are some things we can do with sets.

Unions The union of S and T, denoted $S \cup T$, is the set such that each element of $S \cup T$ is either an element of S or of T, or both.

Intersections The intersection of S and T, denoted $S \cap T$, is the set such that each element of $S \cap T$ is both an element of S and an element of T.

Difference The difference denoted $S - T$ is the set such that an element of $S - T$ is an element of S but not an element of T.

Cartesian products The Cartesian product of S and T, denoted $S \times T$, is the set whose elements are *ordered pairs* (x, y), where x runs over all the elements of S, and y runs over all the elements of T. Note that if one of the two sets is empty, then the Cartesian product is also empty.

Power set The power set of S, denoted $\mathcal{P}(S)$, is the set whose elements are all the subsets of S.

Example 1.

1. $\{1,2\} \cup \{2,3\} = \{1,2,3\}$.
2. $\{1,2\} \cap \{2,3\} = \{2\}$.

Example 2.

1. $\mathcal{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$.
2. $\{1,2\} \times \{2,3\} = \{(1,2), (1,3), (2,2), (2,3)\}$.
3. $\{1,2\} \times \emptyset = \emptyset$.

Functions

A function f from a set S to a set T is a rule that takes elements of S as input and produces elements of T as output. We write $f : S \to T$ to say that f is a function from S to T. Usually, after writing $f : S \to T$, we specify the rule. For an input element $s \in S$, we denote by $f(s)$ the output (in T) produced by f for the input s. For f to be a valid function, the rule that defines it must be *unambiguous*, that is, for every input $s \in S$, it must produce a unique output $f(s)$. Furthermore, the rule cover all possible input values $s \in S$.

If we have a function $f : S \to T$, we say that S is the *source* or *domain* of f and T is the *target* or *co-domain* of f.

Example 3. *1. We have a function $f : \mathbf{N} \to \mathbf{N}$ defined by $f(s) = s^2$.*

2. *The rule $s \mapsto s/2$ does* not *define a function $f : \mathbf{N} \to \mathbf{N}$ because for inputs s that are odd numbers, the output $s/2$ is not an element of $\mathbf{N}$. However, it does define a function $f : \mathbf{N} \to \mathbf{Q}$.*

Relations

Informally, a relation is a specification that links objects of one set and objects of another set. If x is related to y under a relation R, we say that the ordered pair (x, y) satisfies R. For example, we may consider a relation called `is-factor-of`, on pairs of natural numbers, which specifies that (x, y) satisfies `is-factor-of` if and only if x is a factor of y. In this case, $(1, 3)$, $(3, 27)$, $(4, 24)$ are all examples of ordered pairs that satisfy the relation `is-factor-of`[4].

To model this mathematically, we formally define a relation as a subset $R \subset S \times T$, where S and T are two sets. In this case, the elements of R are precisely the ordered pairs that we think of as satisfying the relation R. In the previous example, we have $S = T = \mathbf{N}$. If we want R to model the relation `is-factor-of`, then

[4] In English, we might read one of these as "3 is a factor of 27".

we take R to be the subset of $\mathbf{N} \times \mathbf{N}$ consisting of exactly the pairs (x, y) where x is a factor of y.

As in the previous example, we often want S and T to be the same set. In this case, we say that a subset $R \subset S \times S$ is a (binary[5]) relation on S.

[5] This is a binary relation because we are looking at a subset of the product of two copies of S. An n-ary relation on S would just be a subset of the product of n copies of S.

A FUNCTION GIVES RISE TO A RELATION, which we can think of as the `input-output` relation of the function. Given a function $f\colon S \to T$, the *input-output relation* of f is the relation $R \subset S \times T$ defined by $R = \{(s, t) \in S \times T \mid t = f(s)\}$. In other words, we think of s and t as related if t is the output given by f for the input s.

The input-output relation R associated to a function f satisfies an important property. For every $s \in S$, there is a *unique* $t \in T$ such that $(s, t) \in R$. This is another way of saying that for every input, f produces a unique output. If a relation does not satisfy this property, then it cannot be the input-output relation of a function.

Example 4.

1. *The relation* $\{(a, b) \in \mathbf{N} \times \mathbf{N} \mid a + b \text{ is even } \}$ *is not the input-ouput relation of a function because, for example, for the element* $2 \in \mathbf{N}$*, we have two elements* 0 *and* 4 *of* $\mathbf{N}$ *such that* $(2, 0)$ *and* $(2, 4)$ *are related.*
2. *The relation* $\{(a, b) \in \mathbf{N} \times \mathbf{N} \mid b = a^2\}$ *is the input-output relation of a function. The function is* $f\colon \mathbf{N} \to \mathbf{N}$ *given by* $f(a) = a^2$*.*

Graphs

Graphs provide an extremely useful way to organise information about relations. For the moment we use them as powerful visual aids, but we will see later that graphs also lend themselves well to computational tools.

A *directed graph* consists of a *vertex set* V and an *edge set* E. We require that the edge set E is a relation on V, that is, $E \subset V \times V$. We will write this graph as (V, E). Visually, we draw the vertices as nodes and an edge (v, w) as an arrow from v to w.

We think of *undirected graph* as a directed graph with the extra property that the edge relation E is symmetric. That is, $(v, w) \in E$ if and only if $(w, v) \in E$. In this case, we draw the vertices as nodes, and we draw a single segment joining v and w for every corresponding pair of edges (v, w) and (w, v).

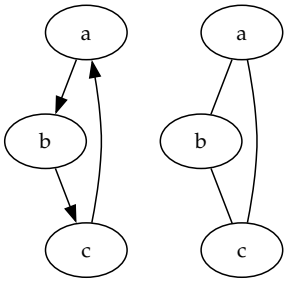


Figure 1: A directed and an undirected graph

Representing a relation on a set as a graph

Note that the definition of a graph is very similar to the definition of a relation on a single set — in fact, a directed graph is just another way of looking at a relation on a set. More precisely, let R be a relation on a set S. Then we can construct a directed graph whose vertex set is S and whose edge set is R. This point of view is useful in certain situations, as we will see later.

The adjacency matrix of a graph

Recall that a *matrix* is a rectangular array, usually filled with numbers. An $m \times n$ matrix M has m rows (numbered 1 through m) and n columns (numbered 1) through n). The entry in the ith row and jth column is denoted M_{ij}.

It is extremely useful to encode the data of a graph into a matrix, called an *adjacency matrix*.

Definition 5. *Suppose $G = (V, E)$ is a graph[6]. Choose an ordering on the elements of V, say the ordered tuple $(v_1, \ldots, v_n)$. The adjacency matrix of G with respect to the chose ordering is the $n \times n$ matrix A, defined by*

$$A_{ij} = \begin{cases} 1, & (i,j) \in E, \\ 0, & (i,j) \notin E \end{cases}.$$

[6] For simplicity we usually consider finite sets V when we construct adjacency matrices but in general V may be infinite.

The adjacency matrix is a matrix that only contains the elements 0 and 1. It encodes the entire information contained in the original graph, in a way that is highly adapted to calculations — we will see more of this soon.

Note that changing the ordering on the elements of V produces a different-looking adjacency matrix. It is related to the original adjacency matrix by a serious of simultaneous swaps of corresponding row and column numbers. For example, the adjacency matrix given by the ordering $(v_2, v_1, v_3, \ldots, v_n)$ can be obtained from A by swapping rows 1 and 2 and also swapping columns 1 and 2.

Example 6. *Let (V, E) be the directed graph shown in Figure 1, with the ordering on the vertices chosen to be (a, b, c). Then the adjacency matrix is*

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Now if we reorder the vertices as (c, b, a), the adjacency matrix becomes

$$A' = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Properties of relations

Sometimes, relations (on a single set) satisfy further special properties. Here are some common ones. Remember that a relation R is simply a subset of $S \times S$ for some set S. So the following properties are about R as a whole, as a subset of $S \times S$.

Reflexivity A relation R is *reflexive* if $(x, x) \in R$ for each $x \in S$.

Symmetry A relation R is *symmetric* if whenever we have $(x, y) \in R$, we also have $(y, x) \in R$.

Anti-symmetry A relation R is *anti-symmetric* if having both $(x, y) \in R$ and $(y, x) \in R$ implies that $x = y$.

Transitivity A relation R is *transitive* if whenever $(x, y) \in R$ and $(y, z) \in R$, we also have $(x, z) \in R$.

Note that the properties of being *symmetric* and *anti-symmetric* are almost but not quite complementary to each other: if a relation is both symmetric and anti-symmetric, it means that only pairs of the form (x, x) can be in the relation[7]. However, not all pairs of this form have to satisfy the relation (i.e. the relation need not be reflexive).

The adjacency matrix can be helpful in order to read off properties about the relation. For example, since a reflexive relation has all possible pairs (x, x) in it, all diagonal entries A_{ii} of the adjacency matrix must equal 1, and conversely if $A_{ii} = 1$ for each i, then the relation is reflexive.

Similarly, a relation is symmetric if $A_{ij} = A_{ji}$ for each i, j. That is, if the adjacency matrix is symmetric. A relation is anti-symmetric if whenever $i \neq j$ and $A_{ij} = 1$, we have $A_{ji} = 0$.

Example 7.

1. *The relation*

   $$R = \{(a, b) \in \mathbf{N} \times \mathbf{N} \mid a \text{ divides } b\}$$

   is reflexive, anti-symmetric, and transitive.

2. *The relation*

   $$R = \{(a, b) \in \mathbf{N} \times \mathbf{N} \mid a + b \text{ is odd}\}$$

   is symmetric but not reflexive or transitive.

[7] Convince yourself of this from the definitions!

What does it mean in terms of the adjacency matrix if a relation is transitive? The answer to this question is slightly more complicated, and we will get back to it later.

Closures of relations

If S is any set, then the entire cartesian product $S \times S$ is itself a relation on S. Note that certain properties are true for $S \times S$: for example, of the four properties discussed in the previous section, $S \times S$ has reflexivity, symmetry, and transitivity.

If R is any relation on S, it makes sense to ask about the *reflexive closure* (resp. symmetric or transitive closure) of R. In the following discussion we'll talk about the reflexive closure, but you can use the same definition for symmetric and transitive closures respectively.

Informally, we'd like the reflexive closure of R to be the smallest relation on S that contains R, and which is reflexive. If R is already reflexive, then it is its own reflexive closure. Otherwise, the reflexive closure will contain some more elements. But what does *smallest* mean in the above context[8]? To make this precise, we give the following definition.

[8] If S is a finite set, then we can say that that smallest means the one with the least number of elements, but we give a general definition because we don't want to be restricted to this case.

Definition 8. *A reflexive (resp. symmetric, transitive) closure of R is a set $\overline{R}$ with the following properties.*

1. $R \subset \overline{R} \subset S \times S$.
2. $\overline{R}$ *is reflexive (resp. symmetric, transitive).*
3. *If T is a subset of $S \times S$ such that $R \subset T \subsetneq \overline{R}$, then T is not reflexive (resp. symmetric, transitive).*

It can be shown that reflexive (resp. symmetric, transitive) closures always exist, and that they are unique[9]. We won't prove this formally, but instead we will just produce a construction of each.

[9] Think about when it makes sense to ask for the closure of a relation with respect to a property, and when you can expect it to exist uniquely. For example, it doesn't really make sense to ask for the anti-symmetric closure of a relation. Do you see why?

Let us first tackle the reflexive closure. To make a relation reflexive, we need to add in all pairs of the form $\{(x, x)\}$, where $x \in S$. So you can convince yourself that the reflexive closure is simply the set $R \cup \{(x, x) \mid x \in S\}$: not only is this new relation reflexive, but also if you take away any pair that is not already an element of R, you get something non-reflexive. In terms of adjacency matrices, the reflexive closure is the relation corresponding to the matrix obtained by changing all diagonal entries of the original adjacency matrix to 1.

Similarly, the *symmetric closure* of R is obtained by adding the flipped pair $\{(b, a)\}$ for every pair $(a, b) \in R$. This is the same thing as taking $R \cup \{(a, b) \mid (b, a) \in R\}$. In terms of the adjacency matrix, we obtain this by symmetrising the adjacency matrix[10]: whenever $A_{ij} = 1$, we also set $A_{ji} = 1$.

[10] This is the same as taking $\frac{1}{2}(A + A^t)$. Do you see why?

Once again, it is not so easy to describe how to construct the *transitive closure* of a relation R, but it can be done by developing some techniques for working with adjacency matrices. We will revisit this later once we have those techniques.

Equivalence relations

Recall that a relation R on a set S is just a subset of the product $S \times S$. We take a short tour through the theory of equivalence relations, which are extremely important in constructing all sorts of mathematical structures.

Definition 9. *A* equivalence relation *is a relation that is reflexive, symmetric, and transitive.*

Example 10. *Let R be the relation on $\mathbf{Z}$ defined as*

$$R = \{(a, b) \in \mathbf{Z} \times \mathbf{Z} \mid a - b \text{ is even}\}.$$

Usually, if we have an equivalence relation R on a set S, we say that $x \sim_R y$ if (x, y) is in R. If the context is clear, we will simply say $x \sim y$. The most important application is that having an equivalence relation on a set allows us to treat an object x as "being equivalent" to an object y if $x \sim y$: the equivalence relation gives us a new way of identifying various objects. We will capture this identification with the notion of *equivalence classes*[11].

[11] The idea is that we can treat all elements of one equivalence class as being interchangeable in some sense.

Definition 11. *Let R be an equivalence relation on a set S. For any $x \in S$, the* equivalence class *of x, denoted $[x]$, is the subset of S defined as follows:*

$$[x] = \{y \in S \mid x \sim_R y\}.$$

In Example 10, $a \sim b$ if and only if they have the same parity, so there are two equivalence classes of R on $\mathbf{Z}$, namely $[0]$ and $[1]$. Note that $[0]$ is the same as $[2]$ or $[-6]$, and $[1]$ is the same as $[-55]$ or $[7]$, but it's traditional to use the smallest non-negative values, which are $[0]$ and $[1]$.

The special properties that an equivalence relation satisfies guarantees the following proposition.

Proposition 12. *Let R be an equivalence relation on a set S.*

1. *Every element of S belongs to at least one equivalence class (its own!).*
2. *If $x, y \in S$ such that $y \in [x]$, then $[x] = [y]$. In other words, the set of equivalence classes of an equivalence relation partitions*[12] *the set S into disjoint subsets whose union is S.*

[12] If $S = S_1 \cup \cdots \cup S_n$, we say that it is a *partition* if $S_i \cap S_j = \emptyset$ for $i \neq j$. In this case we write $S = S_1 \sqcup \cdots \sqcup S_n$, or more concisely, $S = \bigsqcup_{i=1}^{n} S_i$.

Proof. Let x be any element of S. First note that $x \in [x]$ by reflexivity, which proves the first statement. To prove the second statement, suppose that $x, y \in S$ such that $y \in [x]$. To show that $[x] = [y]$, we need to show that for every $z \in S$, we have $z \in [x]$ if and only if $z \in [y]$.

Recall that $y \in [x]$ means that $x \sim_R y$. If $z \in [y]$, then we have $z \in [x]$ by transitivity: $x \sim_R y$ and $y \sim_R z$ implies $x \sim_R z$. On the

other hand, since we know that $y \in [x]$, we also have $x \in [y]$ by symmetry, and then by the previous argument we see that if $z \in [x]$ then $z \in [y]$ by transitivity. The proof is now complete. □

If $y \in [x]$, we say that y is a *representative* of $[x]$.

Often we can uncover new structures by working with the set of equivalence classes rather than the original set S, and it can even give rise to new structures. An important example of this technique is modular arithmetic.

Modular arithmetic

As an important application of equivalence classes, we briefly study modular arithmetic. First recall the relation from Example 10. We can observe that in the integers, the sum of two numbers is always even. The sum of an even with an odd is odd, and the sum of two odd numbers is always odd. But the set of even numbers has another name: $[0]$, and the set of odd numbers is also called $[1]$ with respect to this relation.

So we can express the above statements by writing down the following statements instead.

1. Whenever $a \in [0]$ and $b \in [0]$, we have $a + b \in [0]$.
2. Whenever $a \in [0]$ and $b \in [1]$, we have $a + b \in [1]$.
3. Whenever $a \in [1]$ and $b \in [0]$, we have $a + b \in [1]$.
4. Whenever $a \in [1]$ and $b \in [1]$, we have $a + b \in [0]$.

Let us instead express this by defining a *new addition operation* on the set[13] $\{[0], [1]\}$. We will simply define this addition using the four properties above, which can be written more concisely as

$$[a] + [b] \coloneqq [a + b] \text{ for each } a, b \in \mathbf{Z}.$$

[13] Note that this set is *not* equal to $\mathbf{Z}$! It is also not equal to the set $\{0, 1\}$. Instead this is a set with two elements, which are themselves subsets of $\mathbf{Z}$.

Because we know the properties we stated above about even/odd addition, we have effectively proven that it actually doesn't matter whic representative we take for each equivalence class. This is the idea behind modular arithmetic.

More generally, fix a *modulus* $d \in \mathbf{N}$. We say that $x \sim_d y$ if $x - y$ is divisible by d, which is also written as $d \mid x - y$. More traditionally, we write $x \equiv y \pmod{d}$. Note that if $x \sim_d y$, then there is some integer $m \in \mathbf{Z}$ such that $x - y = md$.

Exercise 13. *Check that $\sim_d$ is an equivalence relation.*

In this case, we have equivalence classes $[0], [1], \ldots, [d-1]$. Note that $[d] = [0]$ again. But if $0 \leq e, f < d$, how do we know for sure that $[e] \neq [f]$ when $e \neq f$? We know this by Euclid's algorithm, which guarantees that for every integer n and positive integer d, we can write a *unique* equation

$$n = qd + r, \quad 0 \leq r < d.$$

In our case, suppose that $e \geq f$. Since $0 \leq e - f < d$, the equation for $e - f$ has to be $e - f = 0 \cdot d + (e - f)$. On the other hand

if $[e] = [f]$ then we also have a valid equation that looks like $e - f = m \cdot d + 0$ for some m. Matching up the two, we see that $m = 0$ and $e = f$ is the only possibility.

Having established this, we now know that we have exactly d different equivalence classes, namely $[0], [1], \ldots, [d-1]$. Of course these can be represented by different integers. For example, $[1] = \{\ldots, 1-2d, 1-d, 1, 1+d, 1+2d, \ldots\}$, so any of these elements would do as a representative of $[1]$. We will write $\mathbf{Z}/d\mathbf{Z} = \{[0], \ldots, [d-1]\}$ to be the set of equivalence classes in this case.

Once again we define a *new addition operation*, this time on $\mathbf{Z}/d\mathbf{Z}$. The definition is the same: for any $[a], [b] \in \mathbf{Z}/d\mathbf{Z}$, set

$$[a] + [b] \coloneqq [a + b].$$

We now have to check whether this is *well-defined*[14] Suppose that $[p] = [a]$ and $[q] = [b]$. Then $p - a = md$ and $q - b = nd$ for some integers m, n. Adding these, we see that $(p+q) - (a+b) = (m+n)d$, and so $[p+q] = [a+b]$. Indeed, our operation is well-defined! This is called modular addition.

[14] This means that if $[p] = [a]$ and $[q] = [b]$, do we have $[p+q] = [a+b]$? If not, we don't have a good definition because it depends on the specific representative we had chosen!

Notice that this has properties similar to the addition in the integers, with some key differences. For example, we have the following.

similarity $[0] + [a] = [a] + [0] = [a]$

similarity $[a] + [b] = [b] + [a]$

difference! $[a] + [a] + \cdots + [a]$ can equal $[0]$ even if $[a] \neq 0$. For example, $[1] + [1] + [1] = [0]$ when $d = 3$.

What about multiplication? Can we define a modular multiplication? Let us try. We will attempt to define a multiplication operation by saying that

$$[a] \cdot [b] \text{ should b } [ab].$$

Again, we must check that this is well-defined. Suppose that $[p] = [a]$ and $[q] = [b]$. Then $p - a = md$ and $q - b = nd$ for some integers m, n. Note that $pq - aq = mqd$ and $aq - ab = nad$. Adding these, we see that $pq - ab = (mq + na)d$, so $[pq] = [ab]$, and this multiplication is well-defined! This is called modular multiplication.

Exercise 14. *What are some similarities and differences between modular multiplication and usual integer multiplication?*

Partial orders

In this section we study another important kind of relation, called *partial orders*. These are entirely different in flavour from equivalence relations, and very common.

Definition 15. *A relation R on a set P is a* partial ordering *or* partial order *if it is reflexive, anti-symmetric, and transitive.*

A set equipped with a partial order relation is called a *partially ordered set* or a *poset*. If R is a partial order on P, we usually write $x \preceq y$ if $(x, y) \in R$. We also often say that $(P, \preceq)$ is a poset, to mean that $\preceq$ is a partial order relation on the set P.

Here is an example of a non-numerical partial ordering.

Note that a partially ordered set P need not be a set of numbers, so the curly inequality sign denoting the partial order relation is not necessarily a numerical inequality.

Example 16. *Suppose that S is any set, and let $\mathcal{P}(S)$ be the power set of S, so that the elements of $\mathcal{P}(S)$ are all the subsets of S. We can define a partial ordering on $\mathcal{P}(S)$ by setting $A \preceq B$ whenever $A \subseteq B$. Let us check the three properties.*

1. *This relation is reflexive because any set A is a subset of itself.*

2. *It is anti-symmetric because if $A \subseteq B$ and $B \subseteq A$ both hold, then all elements of A are elements of B and all elements of B are elements of A, and so A and B must be equal.*

3. *It is transitive because whenever $A \subseteq B$ and $B \subseteq C$, we also have $A \subseteq C$.*

Suppose that $\preceq$ is a partial order on some set P.

Definition 18. *We say that two elements $a, b \in P$ are* comparable *if they are related in some order, that is, either $a \preceq b$ or $b \preceq a$.*

Let $\preceq$ be a partial order on a set P. We say that this partial order is *total* if any two elements a, b of P are comparable. That is, we either have $a \preceq b$ or $b \preceq a$.

Here are a couple of other important examples of partial orderings.

- The usual inequality ordering on $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, or $\mathbf{R}$, where $a \preceq b$ whenever $a \leq b$ as numbers. This is a total order because any two numbers are comparable.

- The division ordering on $\mathbf{N}$, where $a \preceq b$ whenever $a \mid b$, that is, a is a factor of b. This is not a total order, because (for example) 12 and 15 are incomparable.

Exercise 17. *Find examples to show that the partial order of Example 16 is not usually a total order.*

Exercise 19. *Check that the examples given satisfy the properties of being partial orders, and come up with some more of your own.*

Hasse diagrams

A Hasse diagram is a useful way to visualise a partial order. It is similar to drawing the graph of the partial order, but much less cluttered. Let us consider the example in Figure 2.

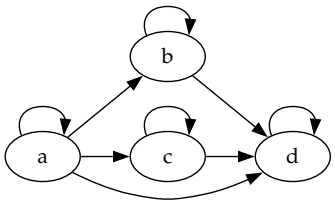


Figure 2: The graph of a partial order relation

This is the graph of the relation, which contains all the information about the relation. But it is also highly redundant: we already know that partial order relations are reflexive, so the self-loops are redundant. Similarly, we alreday know that the relation is transitive, so any "shortcuts", such as the one from the node a to the node d, are redundant.

So to convert the graph of a partial order relation into a Hasse diagram, we do the following:

- remove all self-loops,
- remove all edges implied by transitivity, and
- implicitly order all edges from bottom to top to get rid of the arrowheads.

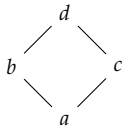


Figure 3: The Hasse diagram of the partial order relation from Figure 2.

The result can be seen in Figure 3.

Similarly, to convert from a Hasse diagram to the graph of the relation, we do the following:

- add arrowheads going from the bottom to the top,
- add all edges in the transitive closure, and
- add self-loops at each vertex.

Let us study more closely which edges survive in the Hasse diagram. Suppose we have $x \preceq y$ with $x \neq y$. When we draw the complete digraph of the relation $\preceq$, we will draw an arrow from x to y. But if there is a z, different from x and y, such that $x \preceq z$ and $z \preceq y$, we will delete the arrow from x to y, because it is implied by the arrows from x to z and z to y. So the only edges that survive in the Hasse diagram correspond to $x \preceq y$ for which there is no z with $x \preceq z \preceq y$ with $x \neq z$ and $y \neq z$. In this case, we say that y *covers* x or y is an *immediate successor* of x. Note that x can have multiple immediate successors.

Upper and lower bounds

Let $(P, \preceq)$ be a partially ordered set. Let $A \subseteq P$ be a subset.

Definition 20. *We say that $u \in P$ is an* upper bound for A *if for every $a \in A$, we have $a \preceq u$. We say that $l \in P$ is a* lower bound for A *if for every $a \in A$, we have $l \preceq a$.*

Note that upper and lower bounds may not be unique, and they may not even lie in the set A, as can be seen from Example 23.

Definition 21. *Let $(P, \preceq)$ be a poset. We say that u is the* least upper bound *or* lub *for a subset $A \subseteq P$ if it is the smallest among all upper bounds of A. That is, if u' is any upper bound for A, then we have $u \preceq u'$. We say that l is the* greatest lower bound *or* glb *for a subset $A \subseteq P$ if it is the greatest among all lower bounds of A. That is, if l' is any lower bound for A, then we have $l' \preceq l$.*

Note that lubs and glbs need not always exist, again as demonstrated in Example 23. However, if they exist, they are unique.

Exercise 22. *Let A be a subset of a poset $(P, \preceq)$ and suppose that A has a least upper bound $u \in P$. Show that it is the unique least upper bound for A in P. Similarly, if A has a greatest lower bound l, then show that it is the unique greatest lower bound for A in P.*

Definition 24. *Let $(P, \preceq)$ be a poset. We have the following definitions.*

1. *An element $x \in P$ is called a* minimum element *of P if $x \preceq y$ for every $y \in P$.*
2. *An element $x \in P$ is called a* minimal element *of P if $y \not\preceq x$ for every $y \in P$.*
3. *An element $x \in P$ is called a* maximum element *of P if $y \preceq x$ for every $y \in P$.*
4. *An element $x \in P$ is called a* maximal element *of P if $x \not\preceq y$ for every $y \in P$.*

These definitions are quite similar in flavour to those of upper and lower bounds: in particular, an element is maximum (resp. minimum) if and only if it is an upper (resp. lower) bound for the entire set P.

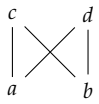


Figure 4: The Hasse diagram of the "bow-tie" poset

Example 23. *Let $(P, \preceq)$ be the* bow-tie poset *shown in Figure 4. We have the following.*

1. *The set $\{a, b\}$ has two upper bounds (c and d), but no lub.*
2. *The set $\{a, b\}$ has no lower bound.*
3. *The set $\{a, b, c, d\}$ has no upper or lower bound.*
4. *The set $\{a, b, c\}$ has c as its unique upper bound (and hence its unique lub), and no lower bounds.*

Do you understand the difference between minimal and minimum (resp. maximal and maximum) elements of a poset? Test your understanding in the bow-tie poset of Figure 4.

Rank functions

Let $(P, \preceq)$ be a poset. We can attempt to campture the partial order by assigning a numerical "rank" to every vertex. Roughly speaking, the rank of a vertex corresponds to its "level" in the Hasse diagram. More precisely, a rank function on P is a function $r \colon P \to \mathbf{Z}_{\geq 0}$ such that

1. if $x \preceq y$, then $r(x) \leq r(y)$,
2. if y covers x, then $r(y) = r(x) + 1$.

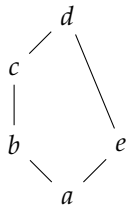
In other words, the second condition says that if y is an immediate successor of x (nothing else between x and y), then the rank of y must be one higher than the rank of x.

There are many examples of posets with a rank function.

Example 25. *Let S be a finite set and let P be the power set of S. We have a partial order on P given by inclusion of sets. Then $r(A) = |A|$ is a rank function on P.*

Example 26. *Consider the poset* **N** *with the relation given by divisibility. For* $n \in \mathbf{N}$*, define* $r(n)$ *as the number of prime factors of* n*, counted with multiplicity. Then* $r(n)$ *is a rank function on* **N***.*

For some posets, there is no possible way to define a rank function! Consider the poset with the following Hasse diagram



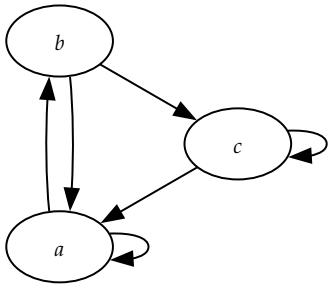
Convince yourself that there is no possible way to define a rank function. (Hint: if the rank of the vertex a is r, then what can be the rank of the vertex e?)

Graphs

Overview

Let us recall the definitions. A (directed) graph consists of a vertex set V and an edge set $E \subset V \times V$. If $(a, b) \in E$, we also write $a \to b$ as a directed edge. Typically we consider finite vertex sets when we work with concrete examples. An *undirected* graph is one in which the edge relation is symmetric: $(a, b) \in E$ if and only if $(b, a) \in E$. In this case, we often group the two flipped ordered pairs $\{(a, b), (b, a)\}$ and think of it as a *single* undirected edge $a - b$. Note that in this case if $a = b$, then the set $\{(a, b), (b, a)\}$ just becomes $\{(a, a)\}$, so we don't get a double loop.

Example 27. *The drawing of a graph where the vertex set is* $V = \{a, b, c\}$ *and the edge relation is* $E = \{(a, a), (a, b), (b, a), (b, c), (c, c), (c, a)\}$.



Why graphs?

Graphs are everywhere! They are a versatile tool to model all kinds of situations. We have already seen how we can use them to model relations on sets. In practice, they arise most naturally when when we model *networks*, for example, the Internet, a series of tubes (i.e. water pipes) connecting various locations, the train or road network in a region, the Twitter/X followers network, the Facebook friends network, the cellphone tower network, the flight network of an airline, and so on.

Graphs also arise when we model *states* and *transitions*, for example, the states of a game and the moves between them, the states of a machine and the transitions between them, flow-charts, and so on.

In many of the applications above, we can enhance the graph by adding more information to the edges. For example, in the graph for the road network between cities, we can add to each edge the length of the road it represents. In a network of tubes, we may want to label an edge by the capacity of the tube it represents. This kind of extra information goes by the name *edge weights*, and the corresponding graph is called an *edge weighted graph*, or simply a *weighted graph*.

Questions about graphs

There are some very natural questions that one can ask about graphs: either practical ones that come up in many of the above contexts, or more theoretical ones.

Here is a sample list, by no means exhaustive.

1. Is there a route from a vertex A to a vertex B?
2. How long is the route, and what is the shortest path?
3. How many routes are there? How long are they?
4. How much water/current/etc can flow through the network when at full capacity?
5. How connected is the graph? If it is connected, how many vertices/edges do we need to remove to make it disconnected? Which vertices/edges are the critical ones?
6. Is there a good way to figure out natural "clusters" in the graph? For example, how does Facebook know whom to suggest to you as a potential friend?
7. Can you find an unbroken path along the edges of the graph that goes through each vertex exactly once? (This is the *Hamiltonian path* problem.)
8. Can you find an unbroken path along the edges of the graph that goes through each edge exactly once? (This is the *Eulerian path* problem.)
9. What is the shortest circuit (path that comes back to the starting point) that visits each vertex exactly once?
10. Is the graph *planar*? That is, can you draw the graph on a plane without crossing any of the edges?
11. Can you colour the vertices of the graph so that no two adjacent vertices have the same colour? How many such colourings are there?

We will study a few such questions to get a taste of the mathematical methods we can employ to study graphs. But there are whole books devoted to graph theory. See, for example, (??, ????).

Adjacency matrix

The *adjacency matrix* gives a convenient numerical way to represent a graph. By performing algebraic operations on the adjacency matrix, we can get important information about the graph.

Let us begin by defining the *adjacency matrix* of a graph. Suppose we are given a graph $G = (V, E)$. We first order the set of vertices V, say $V = \{v_1, \ldots, v_n\}$. The *adjacency matrix* of G is the $n \times n$ matrix A such that

$$A_{ij} = \begin{cases} 1 & \text{if } (i,j) \in E \\ 0 & \text{otherwise.} \end{cases}.$$

In words, the entry in row i and column j of the matrix A is 1 if and only if (i, j) is an edge of A; otherwise, the entry is 0.

Example 28. *Let (V, E) be the directed graph shown in Figure 1, with the ordering on the vertices chosen to be (a, b, c). Then the adjacency matrix is*

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Now if we reorder the vertices as (c, b, a), the adjacency matrix becomes

$$A' = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Matrix products

First we recall matrix products. If A is an $m \times n$ matrix and B is an $n \times p$ matrix, then we can construct a product matrix AB, defined as follows:

$$(AB)_{ij} = A_{i1}B_{1j} + A_{i2}B_{2j} + \cdots + A_{in}B_{nj} = \sum_{k=1}^{n} A_{ik}B_{kj}.$$

Example 29. *Suppose that*

$$A = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 & -2 \\ 2 & 3 & 4 \end{pmatrix}$$

Then

$$AB = \begin{pmatrix} 4 & 7 & 6 \\ -2 & -3 & -4 \end{pmatrix}.$$

Counting paths using the adjacency matrix

Let G be a graph. Take two vertices v_1 and v_2 of the graph. A natural question to ask is whether there is a path from v_1 to v_2. That is, can we go from v_1 to v_2 by following the (directed) edges in G? We may want to count *the number* of paths from v_1 to v_2. Or we may want to find *the shortest* path. All these questions arise in different applications.

BY CLEVERLY USING THE ADJACENCY MATRIX OF THE GRAPH, we can solve many of these questions. Let us take the question of finding the number of paths between two vertices. Let A be the adjacency matrix of G. Recall that

$$A_{i,j} = \begin{cases} 1 & \text{if } v_i \to v_j \text{ is an edge in } G \\ 0 & \text{otherwise.} \end{cases}$$

We can restate this by saying that $A_{i,j}$ is the number of paths of length 1 from v_i to v_j. Indeed, if $A_{i,j} = 1$, then there is exactly one such path, namely the edge $v_i \to v_j$, and if $A_{i,j} = 0$ then there is no such path. Remember that we are only counting paths of length 1 here. Even if $A_{i,j} = 0$, there may be other (longer) paths from v_i to v_j.

Now consider A^2. Look at the example shown in Figure 5. The adjacency matrix A and its square are

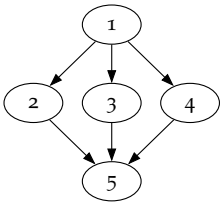


Figure 5: A directed graph

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad A^2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

From the graph and from the matrix, we see that the only nonzero entry in A^2 is the entry at position $(1, 5)$, which equals 3. Also observe that there are exactly 3 paths of length 2 from 1 to 5. Can you also see that between any pair of vertices other than 1 and 5, there are no paths of length 2? So the entries of A^2 match up exactly with the number of paths of length 2.

This is a general phenomenon, and we have the following result.

Theorem 30. *Let A be the adjacency matrix of a simple directed graph (V, E). Suppose that the vertices are ordered as $(v_1, \ldots, v_n)$. Then the*

entry in the (i,j)th position of the kth power A^k of A counts the number of paths of length k from the vertex v_i to the vertex v_j.

The technique of proof of Theorem 30is formally called "the principle of mathematical induction." Suppose we know that a statement is true for $k = 1$. Also suppose that using the statement for k, we can deduce it for $k+1$. Then the statement must be true for all $k = 1, 2, 3, \cdots$.

Proof. We already know that the statement is true for the first power, that is, when $k = 1$.

Let us justify it for the second power, that is, when $k = 1$. By the definition of matrix multiplication, we have

$$A^2_{i,j} = A_{i,1} \cdot A_{1,j} + A_{i,2} \cdot A_{2,j} + \cdots + A_{i,n-1} \cdot A_{n-1,j} + A_{i,n} \cdot A_{n,j}.$$

The product $A_{i,1} \cdot A_{1,j}$ is 0 if either entry is 0 and 1 if both entries are 1. If both entries are 1, we have a length 2 path $v_i \to v_1 \to v_j$. Similarly, $A_{i,2} \cdot A_{2,j} = 1$ if and only if we have a length 2 path $v_i \to v_2 \to v_j$. And so on for the third, fourth, ..., n-th term in the sum above. Conversely, if $v_i \to v_k \to v_j$ is a length 2 path, then it must pass through v_k for some k. Then it is accounted for by the term $A_{i,k} \cdot A_{k,j}$ in the expression for $A^2_{i,j}$. As a result, we see that $A^2_{i,j}$ exactly counts the length 2 paths from v_i to v_j. In other words, the statement is true for $k = 2$.

Now that we know the statement for $k = 2$, let us justify it for $k = 3$. Again, we have

$$A^3_{i,j} = A^2_{i,1} \cdot A_{1,j} + A^2_{i,2} \cdot A_{2,j} + \cdots + A^2_{i,n-1} \cdot A_{n-1,j} + A^2_{i,n} \cdot A_{n,j}.$$

Now, $A^2_{i,1}$ is the number of length 2 paths from v_i to v_1. If $A^2_{1,j} = 1$, then each such path gives a length 3 path from v_i to v_j by concatenating with the edge $v_1 \to v_j$. On the other hand, if $A^2_{1,j} = 0$, then a length 2 path from v_i to v_j does not lead to a length 2 path from v_i to v_j. We repeat the reasoning for all the other terms and see that every length 3 path from v_i to v_j is exactly accounted for by the expression above. Indeed, the length 3 path must split as a length 2 path from v_i to some v_k and an edge from v_k to v_j. Then it is accounted for by the term $A^2_{i,k} \cdot A_{k,j}$. So we deduce that the statement is true for $k = 3$.

Now that we know the statement for $k = 3$, we use the same logic as above to justify it for $k = 4$. And once we know it for $k = 4$, the same logic to justify it for $k = 5$. By continuing in this way, we see that the statement is true for all k. □

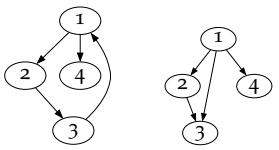


Figure 6: Directed graphs with and without directed cycles

A *directed cycle* in a graph is a path that begins and ends at the same vertex. A loop is the smallest example of a directed cycle. The first graph in Figure 6 has the directed cycle $1 \to 2 \to 3 \to 1$. The second one does not have a directed cycle.

Suppose G is a graph without directed cycles (so, in particular, no loops). Let A be the adjacency matrix of G. From Theorem 30, we can conclude that if k is large enough, then A^k must the zero matrix (all entries are 0). [15] In fact, let n be the number of vertices of G. Then for any $k > n - 1$, we must have $A^k = 0$. Indeed, since G has no cycles, it cannot have a path of length greater than $n - 1$. So, if $k > n - 1$, then all entries of A^k (which count the number of paths of length k) must be zero!

[15] We use $0_{m \times n}$ to denote the zero matrix of size $m \times n$. If m and n are clear from the context, we simply write 0.

Existence of paths using boolean arithmetic

We often want to know whether there *exists* a path from v_i to v_j; we do not care about the number of paths. In that case, we can simplify the calculation. We simply have to keep track of whether the entries in our matrix products are zero or positive.

To do it formally, put an equivalence relation on the set $\mathbf{Z}_{\geq 0} = \{0, 1, 2, \dots, \}$ under which 0 is in its own equivalence class and all positive numbers $1, 2, \dots,$ are equivalent to each other. That is, we set

$$a \sim b \text{ if } a = b = 0 \text{ or both } a, b > 0.$$

We can use the usual $+$ and $\times$ to define $+$ and $\times$ on the equivalence classes, just as we did for modular arithmetic:

$$[a] + [b] = [a + b] \text{ and } [a] \times [b] = [a \times b].$$

People sometimes write 0 and 1 instead of $[0]$ and $[1]$. But then, to distinguish boolean arithmetic from usual arithmetic, it is wise to use different symbols for the two. It is common to use $\vee$ for boolean addition and $\wedge$ for boolean multiplication. So, for example, $1 \vee 0 = 1$ and $1 \wedge 0 = 0$.

Since there are only two equivalence classes $[0]$, namely $\{0\}$, and $[1]$, namely the class of all positive integers, we can explicitly write out the addition and multiplication table:

$$\begin{aligned}
&[0] + [0] = [0],\\
&[0] + [1] = [1] + [0] = [1],\\
&[1] + [1] = [1],\\
&[0] \times [0] = [0] \times [1] = [1] \times [0] = [0],\\
&[1] \times [1] = [1].
\end{aligned}$$

These rules are simply capturing facts like zero plus positive is positive; positive times zero is zero; positive times positive is positive; and so on.

These rule for addition and multiplication are called *boolean rules*.

Let G be a graph and let A be its adjacency matrix. Interpret the entries of A in terms of boolean arithmetic. The entry 0 represents the equivalence class $[0]$ and any non-zero entry (like 1), represents the equivalence class $[1]$. The following theorem follows from Theorem 30.

Boolean arithmetic has an interpretation in terms of boolean logic. If we interpret 0 as `False`, 1 as `True`, boolean $+$ as `OR`, and boolean $\times$ as `AND`, then the boolean rules for addition and multiplication translate into appropriate logical rules.

Theorem 31. *Let A^{*k} be the k-th boolean power of A. Then*

$$A^{*k}_{i,j} = \begin{cases} 0 & \text{if there is no path of length } k \text{ from } v_i \text{ to } v_j, \\ 1 & \text{if there is a path of length } k \text{ from } v_i \text{ to } v_j \end{cases}.$$

Proof. By definition, the entries of A^{*k} are the equivalence classes of the entries of A^k. A non-zero entry in A^k represents the class $[1]$ and a zero entry represents the class $[0]$. On the other hand, a non-zero entry means that there exists a path of length k between the corresponding vertices, and a zero entry means that there does not exist such a path. □

The advantage of Theorem 31 over Theorem 30 is that boolean arithmetic is much easier. For example, since there are only two possibilities $[0]$ and $[1]$, the memory use in a computer will be much smaller in boolean operations (plus, there is no risk of overflow). On the other hand, the entries A^k can grow to be quite big.

The disadvantage is that Theorem 31 only tells whether there is a path or not; it does not give the number of paths.

With boolean operations, finding paths of lengths at most k is also much easier. First, we have the following observation.

Proposition 32. *Let G be a graph that has a loop at every vertex. Then there is a path of length k from v_i to v_j if and only if there is a path of length at most k from v_i to v_j.*

Proof. If there is a path of length ℓ for $\ell \leq k$, simply compose it with $k - \ell$ loops at the end to get a path of length k. □

By combining Theorem 31 and Proposition 32, we get the following.

Proposition 33. *Let G be a graph that has a loop at every vertex. Let A be its adjacency matrix. Then*

$$A^{*k}_{i,j} = \begin{cases} 0 & \text{if there is no path of length at most } k \text{ from } v_i \text{ to } v_j, \\ 1 & \text{if there is a path of length at most } k \text{ from } v_i \text{ to } v_j \end{cases}.$$

What if G does not have a loop at every vertex and we want to find whether there exist paths of length at most k? We simply consider the graph G' obtained from G by adding a loop at every vertex, and then apply Proposition 35!

What if we want to know whether there exists a path (of any length) from v_i to v_j? We have the following observation.

Proposition 34. *Let G be a graph with n vertices. If there is a path from v_i to v_j, then there is a path of length at most $n-1$ from v_i to v_j.*

Proof. Take any path from v_i to v_j. Suppose if it has length n or more. That is, it traversese n or more edges. Then it visits $n+1$ or more vertices. Since our graph only has n vertices, this is only possible if the path revisits a vertex. Suppose it revisits the vertex v. So the path is a concatenation of a path from v_i to v, a cycle beginning and ending at v, and a path from v to v_j (see Figure 7). Just eliminate the middle cycle to get a strictly shorter path from v_i to v_j. By doing this repeatedly, if required, we arrive at a path of length at most $n-1$ from v_i to v_j. □

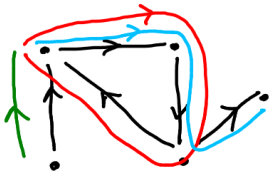


Figure 7: A long path (green followed by red followed by blue) can be shortened by eliminating a cycle (red).

By combining Proposition 32 and Proposition 34, we get the following.

Proposition 35. *Let G be a graph with n vertices that has a loop at every vertex. Let A be its adjacency matrix. Then*

$$A^{*(n-1)}_{i,j} = \begin{cases} 0 & \text{if there is a path from } v_i \text{ to } v_j, \\ 1 & \text{if there is no path from } v_i \text{ to } v_j \end{cases}.$$

Proof. Indeed, by Proposition 34 there is a path from v_i to v_j if and only if there is a path of length at most $n-1$. □

Shortest paths using min-plus arithmetic

In addition to finding the number of paths, or determining the existence of a path, we often want to find the *shortest* path. The adjacency matrix and another clever amendment of our usual arithmetic also solves the problem of finding shortest paths.

It is useful to formulate the problem for *weighted graphs*. Let G be a weighted graph. This means that each edge has an associated *weight*, which is a non-negative real number. It is good to interpret the weight as the length of that edge or the cost of traversing that edge. Given two vertices v_i and v_j, we want to find the path of minimum total weight from v_i to v_j.

We can encode the edges together with their weights in the *weighted adjacency matrix*. It is defined as follows.

Definition 37. *Let G be a weighted graph. Label the vertices as $v_1, \ldots, v_n$. The weighted adjacency matrix of G is an $n \times n$ matrix W, defined as follows:*

$$W_{ij} = \begin{cases} \text{the weight of the edge } v_i \to v_j, & \text{if } v_i \to v_j \text{ is an edge,} \\ \infty, & \text{otherwise.} \end{cases}$$

The ∞ is justified because we want to think of traversing the (non-existant) edge from v_i to v_j as a forbidden operation—it is an operation with infinite cost!

Consider the set $S = \mathbf{R} \cup \{\infty\}$. We are going to define (strange looking) operations of addition and multiplication on S, denoted by $\oplus$ and $\odot$, by declaring

$$a \oplus b = \min(a, b) \text{ and } a \odot b = a + b.$$

We call these rules the *min-plus arithmetic*. If a or b are ∞, we interpret min and $+$ in the obvious way. For example, $\min(1, \infty) = 10$ and $\infty + 1 = \infty$.

We have the following analogue of Theorem 30.

Theorem 38. *Let G be a weighted graph and let W be its weighted adjacency matrix. Let $W^{\odot k}$ be the k-th power of W calculated using min-plus arithmetic. Then $W^{\odot k}_{i,j}$ is the weight of the path from v_i to v_j that has the smallest total weight and has length k.*

Proof. The proof is similar to the proof of Theorem 30.

By the definition of W, the statement is true for $k = 1$. Let us assume that it is true for $W^{\odot k}$ and justify it for $W^{\odot(k+1)}$.

By the definition of matrix multiplication, we have

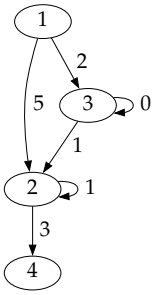
$$W^{\odot(k+1)}_{i,j} = \left(W^{\odot k}_{i,1} \odot W^{\odot k}_{1,j}\right) \oplus \cdots \oplus \left(W^{\odot k}_{i,n} \odot W^{\odot k}_{n,j}\right).$$

Recalling the min-plus rules, the right hand side is

$$\min(W^{\odot k}_{i,1} + W^{\odot k}_{1,j}, \cdots, W^{\odot k}_{i,n} + W^{\odot k}_{n,j}).$$

We can break up a path of length $k+1$ from v_i to v_j as a path of length k from v_i to v_ℓ followed by the edge $v_\ell \to v_j$ for some $\ell \in$

Example 36. *Consider the weighted graph shown below.*



Its weighted adjacency matrix is

$$W = \begin{pmatrix} \infty & 5 & 2 & \infty \\ \infty & 1 & \infty & 3 \\ \infty & 1 & 0 & \infty \\ \infty & \infty & \infty & \infty \end{pmatrix}$$

.

Just as in boolean algebra, it is useful to think of $\oplus$ as `OR` and $\otimes$ as `AND`. Suppose we have an option A that costs a and an option B that costs b. If we have the freedom to choose A `OR` B, the total (optimal) cost is $\min(a, b)$. If we have to choose both A `AND` B, then the total cost is $a + b$.

$\{1, \dots, n\}$. The minimum weight of such a path is the minimum weight of a length k path from v_i to v_ℓ plus the weight of the edge $v_\ell \to v_j$. This is the same as $W^{\odot k}_{i,\ell} + W_{\ell,j}$. If we take the minimum of all these values as ℓ varies in $\{1, \dots, n\}$, we get the weight of a path of minimum weight and of length $k+1$ from v_i to v_j. □

Suppose G is a weighted graph. Assume that

1. all weights are non-negative, and
2. every vertex has a loop and the loop has weight zero.

This is a very common situation. Indeed, the costs are usually non-negative and the cost of going from a place to itself is typically zero.

Proposition 40. *In the setup above, let n be the number of vertices of G, and let W be the weighted adjacency matrix of G. Then $W^{\odot(n-1)}_{i,j}$ is the minimum weight of a path from v_i to v_j.*

Proof. Consider a path of the smallest weight from v_i to v_j. If it has length greater than $n-1$, then we can eliminate a cycle as in the proof of Proposition 34 to create a shorter path. The shorter path has smaller (or the same) weight. So, we do not lose anything by only considering paths of length at most $n-1$.

Now, we can treat a path of length at most $n-1$ as a path of length $n-1$ by simply adding loops at the end as in the proof of Proposition 32. So, the minimum weight of a path from v_i to v_j is the same as the minimum weight of a path of length $n-1$ from v_i to v_j. We conclude using Theorem 38. □

Example 39. *For the graph in Example 36, the second and third min-plus powers of the weighted adjacency matrix are:*

$$W^{\odot 2} = \begin{pmatrix} \infty & 3 & 2 & 8 \\ \infty & 2 & \infty & 4 \\ \infty & 1 & 0 & 4 \\ \infty & \infty & \infty & \infty \end{pmatrix},$$

and

$$W^{\odot 3} = \begin{pmatrix} \infty & 3 & 2 & 6 \\ \infty & 3 & \infty & 5 \\ \infty & 1 & 0 & 4 \\ \infty & \infty & \infty & \infty \end{pmatrix}.$$

Note that they give the total weights of paths of length 2 and 3.

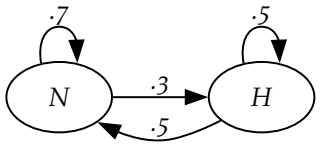
Markov chains

We now consider a special kind of weighted graph, called a *Markov chain*. A *Markov chain* is a weighted graph such that

1. all weights are real numbers in the interval $[0, 1]$
2. for every vertex v, the sum of the weights of all outgoing edges at v is 1.

Markov chains arise when we model random processes. We should think of the vertices in G as "states" of a particular system, which is evolving step by step. Suppose v is a vertex and $e\colon v \to w$ is an outgoing edge from v with weight p. We interpret it as saying that when the system is at state v, it will transition to state w with probability p.

Example 41. *I choose to subscribe to exactly one of Netfilx (N) or HBO (H). Every month, I review my choice, and my choice changes according to the following graph:*

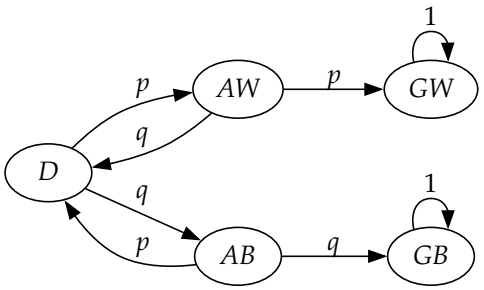


If I am subscribed to Netfilx, then there is a 70% *chance that I will continue to do so next month. But there is* 30% *chance that I will get bored and switch to HBO. Likewise for HBO, but the probabilities are* 50% *and* 50%*.*

We can use Markov chains to describe more than my subscription choices. For example, in Chemistry they are used to describe the kinematics of reactions, in biology, they are used to describe models of DNA evolution, and so on. See the Wikipedia article on "Markov chains" for a staggering array of applications.

Here is another example, thanks to Rachel Fewster (`https://www.stat.auckland.ac.nz/~fewster/325/notes/ch8.pdf`).

Example 42. *In a tennis game of Serena Williams versus Ash Barty, Serena wins a point with probability p and Ash wins a point with probability $q = 1 - p$. The game is at a deuce. The following Markov chain describes the evolution of the game until the game is resolved. The vertices are D (deuce), AW (advantage Williams), AB (advantage Barty), GW (game Williams), and GB (game Barty).*



We add the loops at GW and GB with weight 1 *to indicate that once the process reaches there, it stays there indefinitely (after the game has been won, it remains won indefinitely).*

In the context of a Markov chain, the weighted adjacency matrix is called the *transition matrix*. It is the matrix A defined by

$$A_{i,j} = \begin{cases} \text{the weight of } i \to j & \text{if } i \to j \text{ is an edge} \\ 0 & \text{otherwise.} \end{cases}$$

The 0 indicates that if $i \to j$ is not an edge, then there is 0 chance of the system in the i-th state to transition to the j-th state. In the transition matrix of a Markov chain, all the entries are between 0 and 1 (inclusive), and the entries in each row sum up to 1.

We have the following analogue of Theorem 30. We have the following analogue of Theorem 30.

Theorem 43. *Let G be a Markov chain and let A be its transition matrix. Let A^k be the k-th power of A (with the usual rules of $+$ and $\times$). Then $A^k_{i,j}$ represents the probability of transitioning state v_i to state v_j after exactly k iterations of the random process described by G.*

In the Serana Williams and Ash Barty example, suppose $p = 0.5$. What is the probability that Williams wins the game after 5 points? What about 10 points?

To find the answer, we have to take the 5th (or 10th) power of the weighted adjacency matrix and look at the entry corresponding to row *D* and column *GW*.

Proof. The proof is similar to the proof of Theorem 30.

By the definition of A, the statement is true for $k = 1$. Let us assume that it is true for A^k and justify it for $A^{k+1)}$.

By the definition of matrix multiplication, we have

$$A^{(k+1)}_{i,j} = A^k_{i,1}A_{1,j} + \cdots + A^k_{i,n}A^k_{n,j}.$$

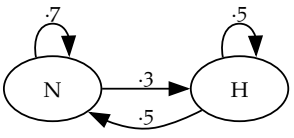
The entry $A^k_{i,1}$ represents the probability of transitioning from v_i to v_1 after k steps. The entry $A_{1,j}$ represents the probability of transitioning from v_1 to v_j in 1 step. So the product $A^k_{i,1} \cdot A_{1,j}$ represents the probability of transitioning from v_i to v_1 in k steps and then transitioning from v_1 to v_j in the next step. Similarly, the product $A^k_{i,2} \cdot A_{2,j}$ represents the probability of transitioning from v_i to v_2 in k steps and then transitioning from v_2 to v_j in the next step, and so on. Taken together, the sum represents the probability of transitioning from v_i to v_j in $(k+1)$ steps. □

Long term behaviour

Consider a Markov chain with transition matrix A. It is particularly meaningful to understand A^k for large values of k, because it lets us analyse the long-term behaviour of the random process represented by the Markov chain.

Recall the Netflix/HBO example, whose transition matrix is

$$A = \begin{pmatrix} 0.7 & 0.3 \\ 0.5 & 0.5 \end{pmatrix}.$$



To find A^k, we first diagonalise A (see the next section). We have

$$\begin{aligned} A &= EDE^{-1} \\ &= \begin{pmatrix} 1 & 1 \\ 1 & -5/3 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1/5 \end{pmatrix} \begin{pmatrix} 5/8 & 3/8 \\ 3/8 & -3/8 \end{pmatrix}. \end{aligned}$$

Therefore, we get

$$A^k = \begin{pmatrix} 1 & 1 \\ 1 & -5/3 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & (1/5)^k \end{pmatrix} \begin{pmatrix} 5/8 & 3/8 \\ 3/8 & -3/8 \end{pmatrix}.$$

As k grows, $(1/5)^k$ approaches 0. So the matrix A^k approaches

$$\begin{pmatrix} 1 & 1 \\ 1 & -5/3 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 5/8 & 3/8 \\ 3/8 & -3/8 \end{pmatrix},$$

which is

$$B = \begin{pmatrix} 5/8 & 3/8 \\ 5/8 & 3/8 \end{pmatrix}.$$

Observe that all rows of B are equal. This is significant! This means that eventually (after a large number of iterations), the probability of being in the N state is $5/8$ *irrespective of the starting state*. Likewise, eventually the probability of being in the H state is $3/8$ *irrespective of the starting state*.

The limiting matrix also allows us to predict what would happen in the long term in a large population. Imagine many people with exactly the same preferences for Netflix/HBO. Then, over a long time period, we should expect $5/8$ of them subscribed to Netflix and $3/8$ of them subscribed to HBO.

In the Serena-Ash example, we see different behaviour. Let us take the the probability p of Williams winning a point to be $p = 0.6$ and the probability q of Barty winning a point to be $q = 0.4$. Then the transition matrix is

$$A = \begin{pmatrix} 0 & 0.6 & 0.4 & 0 & 0 \\ 0.4 & 0 & 0 & 0.6 & 0 \\ 0.6 & 0 & 0 & 0 & 0.4 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Let us compute the powers numerically instead of algebraically. We observe that for large k, we have

$$A^k \approx \begin{pmatrix} 0 & 0 & 0 & 0.69 & 0.31 \\ 0 & 0 & 0 & 0.88 & 0.12 \\ 0 & 0 & 0 & 0.42 & 0.58 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Note that, unlike in the last example, the rows of the limiting matrix are not identical. However, the limiting matrix still gives interesting information. It says that after a long enough play starting at deuce, Williams has a 69% probability of winning the game whereas Barty has 31% probability. If we start with Advantage Williams, her chance goes up to 88%. If we start with Advantage Barty, her chance goes up to 58%.

Random processes whose eventual behaviour is independent of the initial state abound. They are sometimes called *ergodic* or *regular* (the terminology in the literature is inconsistent). The following theorem gives sufficient conditions for this behaviour.

Theorem 44. *Let A be the transition matrix of a Markov chain. Suppose there exists an n such that for every i and j, there is a path of length n from state i to state j. Then*

1. $\lim_{k\to\infty} A^k$ *exists.*
2. *The limiting matrix has identical rows, with non-negative entries summing to* 1.
3. *The limiting row vector v is the unique vector whose entries sum to* 1 *and which satisfies the equation*

$$vA = v.$$

The theorem is called the *Perron-Frobenius theorem.*

The proof of the theorem uses serious linear algebra. You can take this as an invitation to learn some serious linear algebra. But this course is not the place for it. So we will skip the proof.

The theorem applies to the Netflix/HBO example, but not to the Williams/Barty example. Let A be the transition matrix of the Netflix/HBO example. By the Perron-Frobenius theorem, $\lim_{k\to\infty} A^k$ exists and has identical rows. The last assertion in the theorem allows us to calculate the row. Suppose the row is (x, y). Then we have the equations

$$x + y = 1$$

and

$$(x, y)\begin{pmatrix} 0.7 & 0.3 \\ 0.5 & 0.5 \end{pmatrix} = (x, y),$$

that is

$$0.7x + 0.5y = x \text{ and } 0.3x + 0.5y = y.$$

The unique solution of this system is

$$x = 5/8 \text{ and } y = 3/8.$$

This is exactly what we had before!

Computing large powers

Given a matrix A, we often need to compute A^k for large values of k. How do we do it efficiently? Let us discuss two techniques to address this problem.

Diagonalisation

The easiest case is when A is a diagonal matrix—the only non-zero entries of A are on the diagonal. That is, $A_{i,j} = 0$ if $i \neq j$. In this case, A^k is also diagonal and its diagonal entries are the kth powers of the corresponding diagonal entries of A. For example, if $A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$, then $A^k = \begin{pmatrix} 2^k & 0 \\ 0 & 3^k \end{pmatrix}$.

What if A is not diagonal? In many cases, we can *diagonalise* it. That is, we write $A = E \cdot D \cdot E^{-1}$ for a matrix E and a diagonal matrix D. (The negative power E^{-1} denotes the inverse of E. This is the matrix that multiplies with E on either sied to give the identity matrix. That is, $E^{-1}E = EE^{-1} = I$.)

For example, let us take $A = \begin{pmatrix} 0.9 & 0.1 \\ 0.5 & 0.5 \end{pmatrix}$. Then it turns out that $A = EDE^{-1}$ where $D = \begin{pmatrix} 1 & 0 \\ 0 & \frac{2}{5} \end{pmatrix}$ and $E = \begin{pmatrix} 1 & 1 \\ 1 & -5 \end{pmatrix}$, and $E^{-1} = \begin{pmatrix} 5/6 & 1/6 \\ 1/6 & -1/6 \end{pmatrix}$.

Having written $A = EDE^{-1}$, we have

$$\begin{aligned} A^2 &= (EDE^{-1})(EDE^{-1}) \\ &= ED(E^{-1}E)DE^{-1} \\ &= EDDE^{-1} \\ &= ED^2E^{-1}. \end{aligned}$$

Similarly, we have $A^3 = ED^3E^{-1}$, and so on. That is, for all k, we have $A^k = ED^kE^{-1}$. Remember that D^k is easy to compute. So, for any k, we can compute A^k essentially by doing only 3 matrix multiplications.

If we apply this to $A = \begin{pmatrix} 0.9 & 0.1 \\ 0.5 & 0.5 \end{pmatrix}$, we get

$$\begin{aligned} A^k &= \begin{pmatrix} 1 & 1 \\ 1 & -5 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & (\frac{2}{5})^k \end{pmatrix} \begin{pmatrix} 5/6 & 1/6 \\ 1/6 & -1/6 \end{pmatrix} \\ &= \begin{pmatrix} 1 & (\frac{2}{5})^k \\ 1 & -5 \cdot (\frac{2}{5})^k \end{pmatrix} \begin{pmatrix} 5/6 & 1/6 \\ 1/6 & -1/6 \end{pmatrix} \\ &= \begin{pmatrix} 5/6 + 1/6 \cdot (\frac{2}{5})^k & 1/6 - 1/5 \cdot (\frac{2}{5})^k \\ 5/6 - 5/6 \cdot (\frac{2}{5})^k & 1/6 + 5/6 \cdot (\frac{2}{5})^k \end{pmatrix}. \end{aligned}$$

Now, imagine k to be a large number. Then $(2/5)^k = (0.4)^k$ is very close to zero[16]. So, if we ignore this quantity, we see that

$$A^k \approx \begin{pmatrix} 5/6 & 1/6 \\ 5/6 & 1/6 \end{pmatrix}.$$

[16] Any number of absolute value less than 1 raised to a large power is close to zero.

The technique of repeated squaring

THIS SECTION IS AN ASIDE. We discuss the method of *repeated squaring* to quickly find powers of a matrix (or indeed, to quickly find powers in general). This method works for any associative product operation, including the standard matrix product, the Boolean matrix product, and the min-plus matrix product. For concreteness, we discuss it for the standard matrix product.

Let A be a square matrix. The naive method to compute a power of A, for example A^8, would be to multiply A serially with itself 8 times. This consist of 7 matrix product operations. However, there is a quicker method: if we first find and save A^2, then we can multiply that with itself to obtain and save A^4, and finally multiply that with itself to get A^8. In total, that corresponds to only 3 matrix product operations! This is considerably faster than serial multiplication.

But what if we don't have an even number, or a power of two as the power we need to compute? Suppose we are trying to compute A^n where n is not necessarily a power of two. In this case, we simply square the matrix repeatedly, saving the results, until we reach a power less than or equal to n. Then we write n as a sum

of distinct powers of two[17], and then multiply together the corresponding powers of A to get the final result. Here is an example.

Example 45. *Suppose that $n = 19$. In this case, we remember $M_0 = A$, $M_1 = A^2$, $M_2 = M_1^2 = A^4$, $M_3 = A^8$, and $M_4 = A^{16}$. Finally, note that $19 = 16 + 2 + 1 = 2^4 + 2^1 + 2^0$, and so*

$$A^{19} = M_4 \cdot M_1 \cdot M_0.$$

This process corresponds to a total of 6 matrix product operations (four squarings and two multiplications), as opposed to the 18 product operations required for serial multiplication.

[17] Writing a positive integer n as the sum of distinct powers of two is also called *binary writing*. There are several ways to obtain it. For example, we can follow the following recursive algorithm: if n is even, we write it as $2m$, and if n is odd, we write it as $2m + 1$. Repeating the process on the m obtained until we reach 1, we obtain an expression which expands to a sum of distinct powers of two. For example,

$$\begin{aligned} 7 &= 2(3) + 1 = 2(2(1) + 1) + 1 \\ &= 4 + 2 + 1. \end{aligned}$$

Regular expressions and finite automata

In this chapter, we will study regular expressions, regular languages, and finite automata. The aim of the chapter is to build up tools for "pattern-matching" strings over a fixed alphabet, and to isolate subsets of strings that match certain patterns.

Regular expressions

A regular expression is a systematic formula that specifies certain strings of a given alphabet. We first need to define what we mean by alphabet and string, and some basic constructions.

Definition 46. *An alphabet Σ is a finite set of symbols, called the* letters *of Σ. A* string *or a* word *is a finite ordered list of elements of Σ, written without spaces or punctuation. The* length *of a word is the number of letters in the word.*[18]

[18] The unique empty word is also allowed, and is denoted ε. For this reason we usually assume that ε is not a symbol in Σ.

A commonly used alphabet is $\Sigma = \{0, 1\}$. In that case, examples of strings or words in this alphabet are 10, 00, 1110, 0, 1, and ε.

If Σ is a fixed alphabet, then we denote by Σ^* the set of all strings, including ε.

Definition 48. *Fix an alphabet Σ. A* language *L on Σ is any subset of Σ^*.*

Exercise 47. *Check that if $\Sigma = \emptyset$ then $\Sigma^* = \{\varepsilon\}$, but otherwise Σ^* is infinite.*

Unless otherwise specified, we will use the alphabet $\Sigma = \{0, 1\}$ as our default alphabet.

Basic constructions with strings

Fix an alphabet Σ. We begin by listing some basic constructions on languages on Σ and strings in Σ.

Concatenation (on strings) Let $v = a_1 \dots a_k$ and $w = b_1 \dots b_l$ be strings, with $a_i, b_j \in \Sigma$ for every i and j. The *concatenation* of v and w is the string

$$vw = a_1 \dots a_k b_1 \dots b_l.$$

Concatenation (on languages) Let $L_1, L_2 \subseteq \Sigma^*$ be languages. The *concatenation of L_1 and L_2* is a new language on Σ, denoted by $L_1 \circ L_2$ and defined as follows.

$$L_1 \circ L_2 = \{vw \mid v \in L_1, w \in L_2\}.$$

Union (of languages) If $L_1, L_2 \subseteq \Sigma^*$ are languages, then their *union* $L_1 \cup L_2$ is just the set union. So

$$L_1 \cup L_2 = \{w \in \Sigma^* \mid w \in L_1 \text{ or } w \in L_2\}.$$

Star (of a language) Let $L \subseteq \Sigma^*$ be a language. Then the *star of* L, denoted L^*, consists of any number of concatenations of words in L. That is,

$$L^* = \{w_1 w_2 \dots w_k \mid k \geq 0 \text{ and } w_i \in L \text{ for each } i\}.$$

Example 49. *1. If $L = \emptyset$ then $L^* = \{\epsilon\}$.*

Lexicographic order (dictionary order)

Suppose that we have ordered the elements of Σ. Then Σ^* (and any other language on Σ) inherits a total order, known as the lexicographic order. In this order, we can compare two words v and w using the following steps.

1. If v and w have unequal lengths, then the shorter word is said to be less than or equal to the longer word.
2. If v and w have the same length n, then we can write them as

$$v = a_1 \cdots a_n \text{ and } w = b_1 \cdots b_n,$$

where a_i, b_j are letters. Then we compare letter by letter starting from 1 to n. If $v \neq w$ then at least one position i must have $a_i \neq b_i$. Let i be the smallest number for which the letters a_i and b_i differ. If $a_i < b_i$ in the order on Σ, we say $v < w$. Otherwise if $b_i < a_i$, we say $w < v$.

Example 50. *Assume we use the order $(0, 1)$ on $\Sigma = \{0, 1\}$.*

1. *The word ϵ is shorter than every other word, so appears first in the lexicographic order on Σ^*.*
2. *The word 11 appears before 011 (or any other word of three or more letters).*
3. *The word 01 appears before 11 but after 00.*

Regular expression syntax and matching

We are now ready to define regular expressions. A regular expression should be thought of as a particular way to specify a pattern, that can "match" zero or more strings in a given language. Regular expressions are built out of three basic patterns and three "operators" that make bigger patterns using smaller ones.

Definition 51. *Fix an alphabet Σ. A word r written using the letters of Σ, together with the symbols $*$ and $|$, is a valid regular expression if it satisfies one of the following.*[19]

1. $r = \emptyset$
2. $r = \varepsilon$
3. $r = a$ *for some* $a \in \Sigma$
4. $r = r_1 r_2$ *for two valid regular expressions* r_1 *and* r_2
5. $r = r_1 | r_2$ *for two valid regular expressions* r_1 *and* r_2
6. $r = s^*$ *for a valid regular expression* s.

[19] Additionally, we are also allowed to parenthesise subexpressions to avoid ambiguity. We assume that Σ does not contain any of the symbols "(", ")", "|", "$*$", or "$\emptyset$".

We now discuss what it means for a string to "match" a regular expression.

Definition 52. *Let Σ be an alphabet and let r be a regular expression on Σ. Let $w \in \Sigma^*$ be any word. We say that w* matches *r if the following hold.*

1. *$r \neq \emptyset$, because no word matches the regular expression $\emptyset$.*
2. *If $r = \epsilon$ or $r = a$ for some $a \in \Sigma$, then $w = r$.*
3. *If $r = r_1 r_2$ then there is at least one way to break up w into $w = v_1 v_2$, such that v_1 matches r_1 and v_2 matches r_2.*
4. *If $r = r_1 | r_2$ then either w matches r_1 or w matches r_2 (or it matches both).*
5. *If $r = s^*$, then w can be broken up as a concatenation of zero or more subwords, $w = v_1 \dots v_k$, such that each v_i matches s.*

Deterministic finite automata

A *finite automaton* is an abstract machine that performs calculations according to certain rules. We will begin by discussing deterministic finite automata, and discuss their relationship to regular expressions.

Definition 53. *Fix an alphabet Σ. A deterministic finite automaton for Σ is described by the following pieces of data.*

1. *A (usually finite) set of* states*, usually denoted Q.*
2. *A* start state[20]*, usually denoted $q_0 \in Q$.*
3. *A set of* accept states *$A \subseteq Q$.*[21]
4. *A transition function*

$$\delta \colon Q \times \Sigma \to Q.$$

The definition is not very illuminating. It is often much clearer to draw the *state diagram* of a finite automaton, as shown in Example 54. In this example, we can decode the formal data of the DFA as follows.

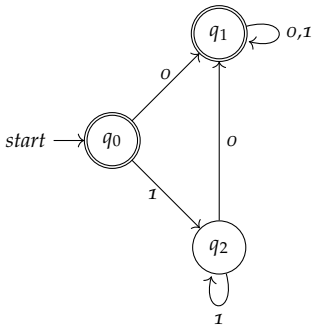
1. The set of states is $Q = \{q_0, q_1, q_2\}$.
2. The start state is q_0.
3. The set of accept states is $A = \{q_0, q_1\}$.
4. The transition function can be represented as a table as follows.

Input state	Letter	Output state
q_0	0	q_1
q_0	1	q_2
q_1	0	q_1
q_1	1	q_1
q_2	0	q_1
q_2	1	q_2

[20] The start state is always unique.

[21] The set of accept states can be *any* subset of Q, including the empty set. Changing the set of accept states while keeping everything else the same typically changes the results of the calculation drastically.

Example 54. *Here is an example of a finite automaton.*



Given a DFA M and a word $w \in \Sigma^*$, we can *run* the machine M on the word w, as follows. Suppose that $w = a_1 a_2 \dots a_k$, where each a_i is a letter of Σ. We then have the following steps.

1. We begin at the start state $p_0 = q_0$ and "read" the letter a_1.
2. We move to the state $p_1 = \delta(p_0, a_1)$. From here, we read the letter a_2.
3. Next, we move to the state $p_2 = \delta(p_1, a_2)$. From here, we read the letetr a_3.
4. Continue in this manner, moving to the state $p_n = \delta(p_{n-1}, a_n)$ by reading the letter a_n.
5. Stop at the state p_k, which is reached after reading the last letter a_k.
6. If p_k is an accepting state of M, we say that M *accepts* w. If p_k is not an accepting state of M, we say that M *rejects* w.

Example 55. *Consider the string $w =$ 1101, running on the machine M from the previous example. It goes through the following steps on M.*

1. *Start at q_0, read 1, move to q_2.*
2. *From q_2 read 1, move to q_2.*
3. *From q_2 read 0, move to q_1.*
4. *From q_1 read 1, move to q_1.*

At the end of this process, we are at q_1, which is an accepting state. Therefore M accepts w.

Definition 56. *Let M be a DFA. The set of all strings accepted by M is called the* language of M, *denoted $L(M)$.*

Nondeterministic finite automata

A *nondeterministic finite automaton* or NFA is a generalisation of a DFA. It is a machine in which, informally, we may have some choices when we try to read letters. In an NFA we relax the restriction that there is *exactly* one outgoing arrow from each state labelled by each letter of Σ. If there are multiple arrows from a state a labelled by a symbol s, then informally it means that if we are at the state a and are reading s, then we may go to any of the target states of these arrows. If there is no arrow from a state a labelled by a symbol s, then we reject the input. We also give ourselves the luxury of allowing arrows labelled by the empty string ε. If there is an arrow labelled ε from a state a to a state b, then informally it means that we have a choice, when we are at a, to teleport to the state b without reading any letter.

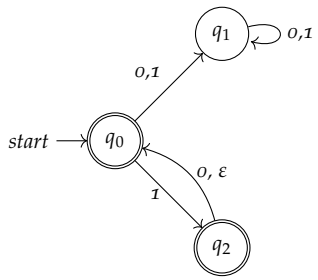
Let us give a formal definition.

Definition 58. *Fix an alphabet Σ. A nondeterministic finite automaton for Σ is described by the following pieces of data.*

1. *A finite set of states, usually denoted Q.*
2. *A start state, usually denoted $q_0 \in Q$.*
3. *A set of accept states, usually denoted $A \subseteq Q$.*
4. *A transition function*[22]

$$\Delta \colon Q \times (\Sigma \cup \{\varepsilon\}) \to \mathcal{P}(Q).$$

Example 57. *Here is an example of a nondeterministic finite automaton.*



[22] This transition function also takes in a pair (q, a) as input, where $q \in Q$ and a is either a letter of Σ or the empty string ε. The output is a (possibly empty) set of states of Q. Visually, we should think of having outgoing arrows from q to each element of $\Delta(q, a)$, each of them labelled by a.

Once again, let us describe the parts of the definition for the example in Example 57. The set of states, the start state, and the set of accept states are exactly as in the previous example (Example 54). The transition function is as follows.

Input state	Letter or ε	Set of output states
q_0	0	$\{q_1\}$
q_0	1	$\{q_1, q_2\}$
q_0	ε	$\emptyset$
q_1	0	$\{q_1\}$
q_1	1	$\{q_1\}$
q_1	ε	$\emptyset$
q_2	0	$\{q_1\}$
q_2	1	$\emptyset$
q_2	ε	$\{q_0\}$

As before, we can *run* strings on NFAs. However, the process of calculation may now involve several choices, depending on how many possible output states there are for each input state and letter (or empty string). We say that an input string is *accepted* by the autamaton, if *some choice* of arrows while reading the string takes us from the start state to an accept state. We represent the calculation as a *calculation tree*, as shown by the following example.

Example 59. *Consider the NFA described by Example 57. We run it on the input string* 110*. Encountered with a choice, we make all possible choices, and record them. We also write states that we encounter after following all possible ϵ arrows*

$$
\begin{array}{c}
q_0 \\
\downarrow 1, \text{ optionally followed by } \varepsilon\text{s} \\
\{q_0, q_1, q_2\} \\
\downarrow 1, \text{ optionally followed by } \varepsilon\text{s} \\
\{q_0, q_1, q_2\} \\
\downarrow 0, \text{ optionally followed by } \varepsilon\text{s} \\
\{q_0, q_1\}
\end{array}
$$

It is possible to reach an accepting state (q_0), so the string 110 *is accepted.*

NFA to DFA

Although NFAs allow much more flexibility than DFAs, they are fundamentally no more expressive. That is, any language that can be described by an NFA can also be described by a DFA. The DFA is typically bigger and clunkier, and the NFA is sleeker and more convenient. But in terms of ability, NFAs are no more than DFAs.

The aim of this section is to convert an NFA to an equivalent DFA. "Equivalent" means that the DFA will accept precisely the same strings as the NFA does. In other words, the two automata describe the same language.

First case: no ε arrows.

We first do a simpler case. Let N be an NFA with states Q and assume that there are no arrows in N labelled by ε. We build the DFA D as follows:

- its states are $\mathcal{P}(Q)$,
- its start state is $\{q_0\}$, where $q_0 \in Q$ is the start state of N,
- its accept states consist of all $S \subset Q$ such that S contains an accept state of N.

Finally, we have to describe the transition function. Let $S \subset Q$ denote a state of D and let $a \in \Sigma$ be a letter. Let δ be the transition function of N. Let T be the union of all $\delta(s)$ as s varies in S. In other words, let T be the set of all states of Q that are reachable from some state in S by following an arrow labelled a. We put the arrow $S \xrightarrow{a} T$ in D.

Convince yourself that D and N accept precisely the same strings.

General case: ε arrows

We need to modify the previous construction a little bit to accommodate ε arrows. Let $S \subset Q$. We say that S is *ε-closed* if any state in Q that is reachable from a state in S by following a ε arrow is already in S. That is, for all $t \in Q$ and $s \in S$ such that $s \xrightarrow{\varepsilon} t$, we have $t \in S$. The *ε-closure* of S is the set obtained by adding to S all possible states that can be reached by starting at a state in S and following zero or more ε arrows. We denote the ε-closure of S by $S^{+\epsilon}$. Observe that $S^{+\epsilon}$ is ε-closed.

In Example 57, what is the ε-closure of $\{q_2\}$?

We are now ready to do the conversion from any NFA to DFA. Let N be an NFA with states Q. We build the DFA D as follows:

- its states are $\{S \in \mathcal{P}(Q) \mid S \text{ is } \varepsilon - \text{closed}\}$,
- its start state is $\{q_0\}^{+\epsilon}$, where $q_0 \in Q$ is the start state of N,
- its accept states consist of all $S \subset Q$ such that S contains an accept state of N.

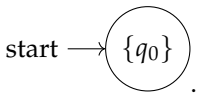
Finally, we have to describe the transition function. Let $S \subset Q$ denote a state of D and let $a \in \Sigma$ be a letter. Let δ be the transition function of N. Let T be the ε-closure of the union of all $\delta(s)$ as s varies in S. In other words, let T be the set of all states of Q that are reachable from some state in S by following an arrow labelled a, optionally followed by a sequence of arrows labelled ε. We put the arrow $S \xrightarrow{a} T$ in D.

Convince yourself that D and N accept precisely the same strings.

Example

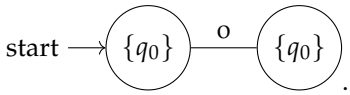
Let us convert the NFA in Example 57 to a DFA. Instead of drawing all possible states, it is more practical to begin with the start state and only draw the states that we need. (States that are not reachable from the start state are irrelevant anyway).

Our start state is the ε-closure of $\{q_0\}$, which is $\{q_0\}$ itself. So far we have the following partial DFA:



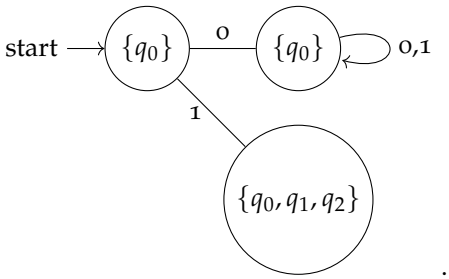
.

We now take a letter 0, apply it to $\{q_0\}$, and find the target state. By definition, the target state is the ε-closure of $\{q_1\}$, which is $\{q_1\}$ itself. We add it to our DFA:



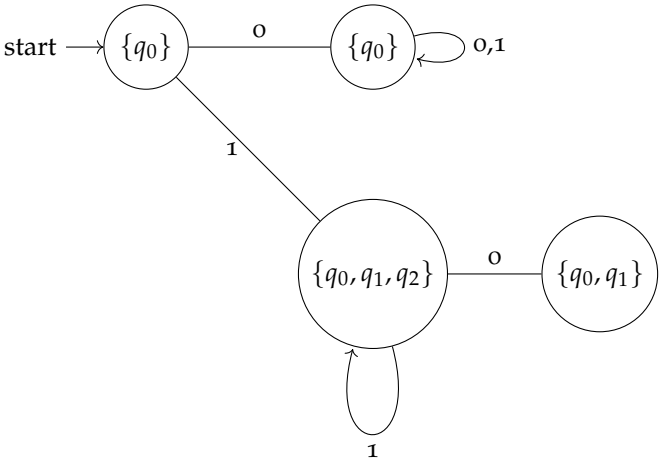
.

We now have multiple options: we can apply 1 to $\{q_0\}$or 0 to $\{q_1\}$ or 1 to $\{q_1\}$. We have to do all of them eventually, and we can do them in any order. Applying 1 to $\{q_0\}$ takes us to $\{q_1, q_2\}$; its ε-closure is $\{q_0, q_1, q_2\}$. So we add $\{q_0\} \xrightarrow{1} \{q_0, q_1, q_2\}$ to our DFA. Applying 1 to $\{q_1\}$ takes us to $\{q_1\}$. Applying 0 to $\{q_1\}$ takes us to $\{q_1\}$. Adding these to the DFA, we have:



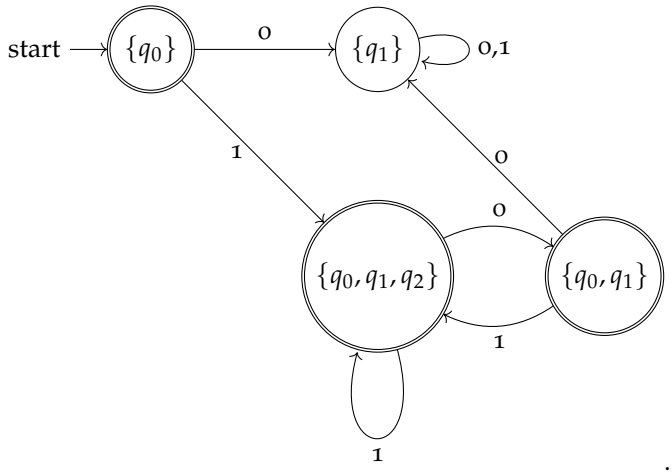
.

Applying 0 to $\{q_0, q_1, q_2\}$ takes us to $\{q_0, q_1\}$, which is already ε-closed. Applying 1 to $\{q_0, q_1, q_2\}$ takes us to $\{q_0, q_1, q_2\}$. After adding these edges, we get



.

Applying 0 to $\{q_0, q_1\}$ takes us to $\{q_1\}$. Applying 1 to $\{q_0, q_1\}$ takes us to $\{q_1, q_2\}$, whose ε-closure is $\{q_0, q_1, q_2$. After adding these two edges, our DFA is complete. We let the accepting states be those that contain an original accepting state.



.

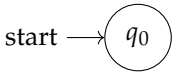
Regular expressions to finite automata

The aim of this section is to try and convert any given regex to an *equivalent*[23] finite automaton (either a DFA or an NFA). We have already seen that given any NFA, one can construct an equivalent (probably much larger) DFA. So to make things simpler for us, we will convert regexes to NFAs.

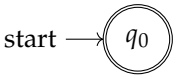
We do this inductively, constructor-by-constructor.

[23] We say that a regex r is equivalent to a finite automaton M if $L(r) = L(M)$.

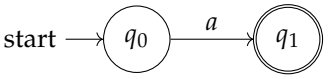
1. If $r = \emptyset$, we simply have to find an NFA that rejects every string. The easiest option is as follows.



2. If $r = \epsilon$, we construct an NFA that only accepts the empty string. A possible option is as follows.

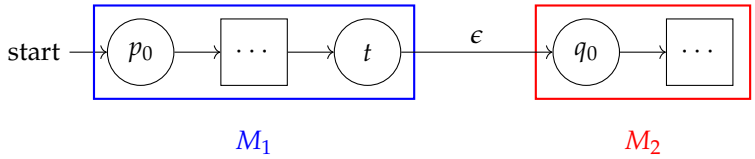


3. If $r = a$ for some $a \in \Sigma$, we construct an NFA that only accepts the string a. A possible option is as follows.

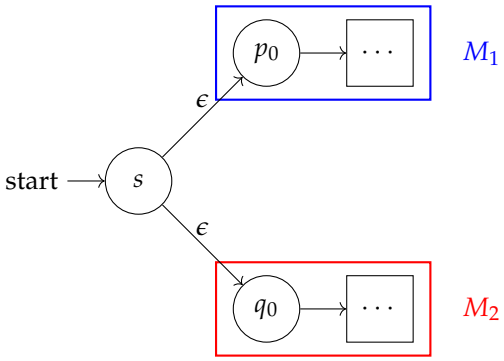


4. If $r = r_1 r_2$ for two regexes r_1 and r_2, we construct an equivalent NFA inductively. Assume that M_1 and M_2 are NFAs equivalent to r_1 and r_2 respectively. Assume furthermore for simplicity that M_1 has exactly one accept state t (if not, we can add a new accepting state, and redirect all previously accepting states to it

by ϵ-transition arrows). Let p_0 and q_0 be the start states of M_1 and M_2 respectively. We can then construct a new automaton that connects M_1 and M_2 by joining t to q_0 by an ϵ transition, whose accepting states are simply the accepting states of M_2. This construction is illustrated below.

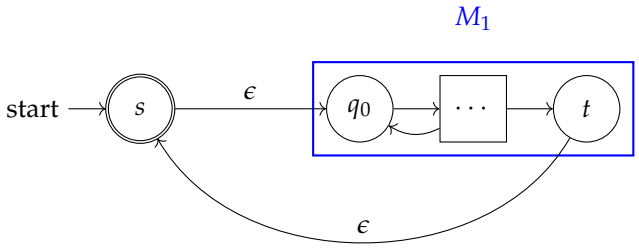


5. If $r = r_1 \mid r_2$ for two regexes r_1 and r_2, we construct an equivalent NFA inductively. Assume that M_1 and M_2 are NFAs equivalent to r_1 and r_2 respectively. Let p_0 and q_0 be the start states of M_1 and M_2 respectively. We construct a new automaton with start state s, which connects to both p_0 and q_0 by ϵ-arrows. The set of accepting states of the new automaton is a union of the sets of accepting states of M_1 and M_2. This construction is illustrated below.



6. If $r = (r_1)^*$ for a regex r_1, we construct an equivalent NFA inductively. Assume that M_1 is an NFA equivalent to r_1. Assume again for simplicity that t is the only accepting state of M_1, and that q_0 is its start state. To construct our new NFA, we add a dummy start state s, make it accepting, and connect t to s via an ϵ arrow. This construction ensures that we accept the empty string, as well as any string that successfully passes through M_1 several times. The construction is illustrated below.

What would happen if we didn't add s, and instead made q_0 accepting, connecting t to q_0?



We see at the end of this process that every regex constructor can be "converted" to an equivalent NFA. By chaining together

these basic constructions, we can therefore convert every regex to an equivalent automaton!

Converting finite automata to regular expressions

Recall that we say that two automata M_1 and M_2 are *equivalent* if $L(M_1) = L(M_2)$. We have already seen that DFAs and NFAs are equivalent in power. That is, for any DFA M there is an equivalent NFA N, and for any NFA N there is an equivalent DFA M.

In this section we focus on converting a given DFA or NFA to an equivalent regular expression r. We will start with an arbitrary machine M, and perform a series of reductions to delete states, successively overloading the arrow labels, until we hit a machine with only two states and a single label, which will be the required regex.

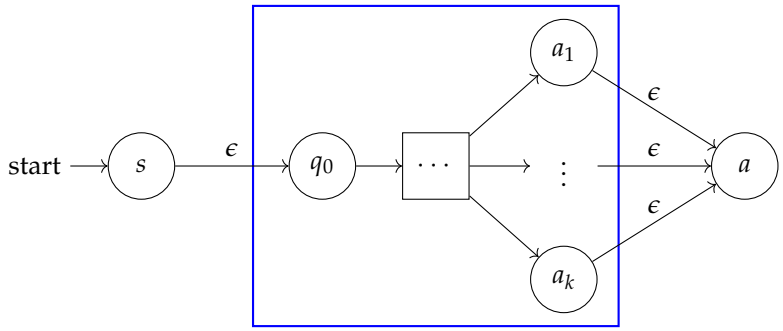
Consider a machine M. First, we *sanitise* or *quarantine* the machine as follows[24].

[24] I use this terminology because you should imagine that you are performing a surgery on your machine, so you want to put it inside a nice sanitised operating box. We then put on our gloves and perform our surgery inside the box, not letting anything in the box interact with anything outside the box, unless strictly necessary.

1. If q_0 was the original start state of M, add a new state s before q_0, connecting it to q_0 by an ϵ arrow. The state s is now our new start state.

2. If $a_1, \ldots, a_k$ were previously the accepting states of M, we add a new accepting state a after $a_1, \ldots, a_k$, with an ϵ-arrow $a_i \xrightarrow{\epsilon} a$ for each $i \in \{1, \ldots, k\}$. We then make $a_1, \ldots, a_k$ non-accepting. Consequently, the new machine has only one accepting state.

   Here is a visual representation.



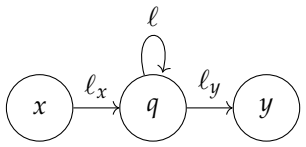
The "operating box".

Once we have done this procedure, we get to work deleting each state of the machine inside the "operating box" one by one. We can't however simply delete a state! We have to compensate for deleting a state by adding extra arrows or labels, so that anything that would have previously gone through that state has an alternate route. The deletion algorithm goes as follows.

1. Choose a state q inside the operating box to delete. If there are no more states left, we are done.

2. Let ℓ be the label on any loop from q to itself. If there is no loop, then we take ℓ to be the empty word ϵ.

3. Consider every possible configuration as follows.



   Here, x and y are states such that $x \neq q$ and $y \neq q$ (but x and y may be equal), and ℓ_x and ℓ_y are the labels on the arrows shown respectively.

4. Each such configuration is a portion that accepts substrings that match the regex $\ell_x \ell^* \ell_y$. In other words, a substring goes through successfully along the portion $x \to q \to y$ if and only if it matches $\ell_x \ell^* \ell_y$. By simply removing q, those substrings would no longer have access to this path. So instead, we add on $\ell_x \ell^* \ell_y$ as a direct label from x to y. Formally, consider any existing arrow $x \to y$ with label r. If there is such an arrow, then change the label on that arrow to $r \mid \ell_x \ell^* \ell_y$. Otherwise, create an arrow $x \to y$ with label $\ell_x \ell^* \ell_y$.

5. Once this has been done for every configuration $x \to q \to y$ for all possible values of x and y, delete q.

6. Note that a string is accepted by the new machine (noting that now an arrow with a label e accepts any substring that matches e) if and only if it is accepted by the old machine.

7. The machine now has one fewer state in the operating box, so go back to step 1.

It is clear that this algorithm terminates with no states left inside the operating box. When there are no more states left, there will be exactly one arrow from s to a, and it will have a regular expression as a label on it. By construction, this regex accepts exactly the strings accepted by the machine we started with, and so it is equivalent to the original machine!

Non-regular languages

Recall that a *regular* language is one that is accepted by a deterministic or non-deterministic finite automaton, or equivalently, one that is the language of some regular expression. It turns out that not all languages are regular.[25]

How do we know whether a given language is regular or not? If we can find a machine or regex that recognises precisely that language, then the language is regular. However, if we cannot come up with a regex or machine that recognises that language, how can we *provably* say that the language is not regular? In this section, we discuss two criteria that allows us to show that a language is regular.

[25] A detailed proof of this is outside the scope of these notes, but here is a proof sketch. If you fix an alphabet Σ, then the cardinality of the set of all languages on Σ is the cardinality of the power set of Σ^*. The set Σ^* is a countable infinite set, and so its power set is uncountable. On the other hand, the set of regular languages is necessarily countable — it is possible to lexicographically enumerate all possible regular expressions, so the set of languages that is recognised by any one of them must also be countable!

Pumping lemma

The first criterion is called the *pumping lemma*.[26]

[26] Be careful — there are non-regular languages that fool the pumping lemma. That is, it does not pick up all non-regular languages.

The idea behind the pumping lemma is relatively simple. Suppose you have a regular language L. This means that there is some DFA M such that $L = L(M)$. This DFA M has finitely many states, say n states.

Every word that M accepts must start at the start state, and pass through (some of) these n states, before ending up at an accepting state. If the language L is infinite, then it must contain words that are longer than n letters. Therefore, as these words travel through M, they must repeat a state. Suppose w is such a word, and note that we can break up w into three pieces $w = xyz$, such that the portion y is non-empty, and starts and ends at the same state. In this situation, because y ends at the same point that it started, the word $xyyz$ must also necessarily end on the same accet state that w ends on! We can say the same thing about the words xz, $xyyyz$, and more generally, xy^iz for any integer $i \geq 0$.

With this background, here is the idea for the pumping lemma. Suppose that there is a language L such that for arbitrarily long words $w \in L$, there is *no way* to split up w into three sections $w = xyz$ such that $xy^iz \in L$ for every L. Then L cannot be regular.

We state this theorem formally first, and will then give an example to see how it can be used.[27] Understanding this theorem is an exercise in getting your order of quantifiers correct!

[27] Typically we use the *contrapositive* of this theorem. That is, we find a language that does not satisfy the consequence of the theorem, and thereby conclude that it is not regular.

Theorem 60. *Suppose L is a regular language. Then there is some positive integer n, called a* pumping length *for L, with the following property. For any $w \in L$ such that $|w| \geq n$, there exists some way to split w as $w = xyz$, such that:*

1. $|y| \geq 1$;
2. $|xy| \leq n$;
3. *the words xy^iz are in L for every integer $i \geq 0$.*

Proof. The proof goes as explained in the previous discussion. Suppose L is regular, and suppose that M is some DFA that recognises L. Suppose also that M has n states. Then we claim that n is a pumping length for L.

Consider any $w \in L$ such that $|w| \geq n$. Now as w travels through M from the start state to the accept state, it will encounter a repeated state q within the first n of its letters. Take x to be the portion of w up until we reach q for the first time. That is, after reading the last letter of x, we are at the state q for the first time. Let y be the portion after x up until we reach q for the second time.

Since we know that q appears at least twice as we travel through the first n letters, we see immediately that

1. $|xy| \leq n$, and
2. $|y| \geq 1$.

Finally, let z be the remainder of w after xy. Recall that after reading the last letter of z, we are at an accepting state of M. Now consider any string of the form xy^iz for i a non-negative integer. As we run xy^iz through M, we reach q after we finish travelling through x. The portion y starts and ends at q, so any power of it will also start and end at q. Finally, the portion z starts at q and ends at an accepting state of M. Therefore it is evident that M accepts xy^iz for each integer $i \geq 0$, and the proof is complete. □

Let us see a simple example of how to use this theorem. Consider the language $L = \{0^k1^k \mid k \geq 0\}$. The words in this language consist of a string of 0s followed by a string of *the same number of* 1s. We will show that L is not regular.

Suppose for contradiction that L is regular, and let n be its pumping length. Then any word in L of size at least n can be split up as in the pumping lemma. Consider the word $w = 0^n1^n$. We have to be able to split up w as $w = xyz$ such that $|xy| \leq n$, $|y| \geq 1$, and $xy^iz \in L$ for every non-negative integer i.

Note however that the first condition ($|xy| \leq n$) guarantees that both x and y only consist of strings of zeroes. Suppose that $x = 0^a$ and $y = 0^b$ for some a, b such that $b \geq 1$ and $a + b \leq n$. Then z is necessarily equal to $0^{n-a-b}1^n$.

Now consider the string $xyyz = xy^2z$. This can be computed to be $0^a0^b0^b0^{n-a-b}1^n = 0^{n+b}1^n$. Clearly, this string is not in L! We have thus managed to violate the pumping lemma, from which we conclude that L could not have been regular in the first place.

The Myhill-Nerode theorem

The Myhill-Nerode theorem gives a necessary and sufficient condition for a language to be regular. It distills the idea that a finite automaton has "finite amount of memory."

Let L be a language (regular or not). Let x, y be strings. We say that L *distinguishes* x and y if there exists a z such that $xz \in L$ and $yz \notin L$ or vice-versa, that is, $xz \notin L$ and $yz \in L$. For example, the language L described by $10^*1|01^*0$ distingushes 0 and 1 (take $z = 10$). But it does not distinguish 010 and 101 (why?)

We say that $x \sim_L y$ if L does not distinguish x and y.

Proposition 61. *The relation $\sim_L$ is an equivalence relation.*

Proof. Reflexivity and symmetry are clear. Let us check transitivity. Suppose $x \sim_L y$ and $y \sim_L w$. Then for any z, either both xz and yz are in L are not in L. Similarly, either both yz and wz are in L or not in L. We have to show that $x \sim_L w$. That is, for any z, we have to show that both xz and wz are in L or not in L. Suppose $xz \in L$. Then $yz \in L$, because $x \sim_L y$ and hence $wz \in L$, because $y \sim_L w$. Similarly, if $xz \notin L$, then $wz \notin L$. □

To show that $x \not\sim_L y$, we have to exhibit *one* z. To show that $x \sim_L y$, we have to check that *all possible* z. How do we do that? If we have an automaton, we have a way.

Proposition 62. *Suppose M is a DFA whose langauge is L. If x and y end at the same state of M, then $x \sim_L y$.*

Proof. For any z, consider the paths that xz and yz take through the automaton. After x and y, the two paths are at the same state. So, after further reading z, they will end at the same state. It is either an accept state, in which case both xz and yz are in L, or not, in which case both xz and yz are not in L. □

In other words, inequivalent strings must end at differest states of M. So we get the following.

Proposition 63. *The number of equivalence classes of $\sim_L$ is at most the number of states of M. In particular, if $\sim_L$ has infinitely many equivalence classes, then L is not regular.*

The converse of the proposition above is also true. The proposition together with the converse is called the Myhill-Nerode theorem.

Example 64. *Consider $L = \{0^n 1^n \mid n \geq 0\}$. The strings $0, 01, 001, 0001, 00001, \cdots$ are pairwise inequivalent (why?). So each of them represents a distinct equivalence class of $\sim_L$. As a result, $\sim_L$ has infinitely many equivalence classes, so it is not regular.*

Theorem 65. *A language L is regular if and only if $\sim_L$ has finitely many equivalence classes.*

Proof. If $\sim_L$ has infinitely many equivalence classes, we saw that there cannot exist a DFA whose language is L. Conversely, suppose $\sim_L$ has finitely many equivalence classes. We build a DFA whose language is L. The states of the DFA are the equivalence classes of $\sim_L$. The start state is the equivalence class of ϵ. Observe that if $x \sim_L y$ then $xz \sim_L yz$ for any z. Using this, we define the transitions as follows. Let S be an equivalence class, or equivalently, a state of our DFA. Let $a \in \Sigma$ be a letter. Take $x \in S$, and draw an arrow labeled a from S to the equivalence class of xa. Choosing a different $y \in S$ changes xa to ya, but ya is still equivalent to xa. So the arrow is unambiguously defined. Let the accept states be the equivalence classes of strings in L. Check that the resulting DFA has language L. □

Combinatorial games

We begin the course with some games. The theory of games is a rich subject that can be used to model problems in logic, computer science, economics, and social science, depending on the rules you impose on your games. We will focus on *impartial combinatorial games*.

An impartial combinatorial game is usually played with two players and satisfies the following conditions.

1. There is a (usually finite) set of possible *game states*.
2. There are rules that describe the possible moves from a given game state to other game states.
3. The game is *impartial*, which means that the rules to go from one game state to the next do not depend on which player is about to make the move[28].
4. The players alternate making moves to move from one game state to the next.
5. The first player to be unable to make a move loses the game[29].
6. There is complete information (the entire game state is known to both players at all times).
7. There are no chance moves.

[28] Contrast this to a game such as chess, in which one player may only move the white pieces and the other player may only move the black pieces.

[29] This is called *normal play*. In the variant called *misère play*, the first player unable to make a move wins the game.

Here is a basic example of an impartial combinatorial game, namely the *subtraction game*.

Fix a finite set of positive integers, say $S = \{1, 3, 4\}$. In the subtraction game with respect to S, we start with a non-negative integer n. A valid move consists of replacing n by $n - k$ where k is some element of S. In this case, the possible valid moves are $n \mapsto n - 1$, $n \mapsto n - 3$, and $n \mapsto n - 4$. The output must remain a non-negative integer, and the person who cannot make a move loses.

Can the first player win if the starting position is $n = 5$? How about $n = 10$? How can you be sure?

Strategic labelling

A basic tool to study an impartial combinatorial game is the *game graph*. This is a directed graph whose vertices represent possible states of the game (usually all states potentially reachable from the starting state). We draw an edge from state s_1 to state s_2 if there is a single move that takes us from s_1 to s_2.

The finiteness condition on impartial combinatorial games means that there are only finitely many states reachable from any given starting state, so the game graph drawn from any fixed starting position is finite. Moreover, there are no directed cycles in this graph, because each possible sequence of moves terminates at a state from which there are no moves possible.

So if we build the full game graph starting at the starting configuration, we can then analyse whether there is a winning strategy. As an easy example, if there are no possible moves from the starting configuration, then the first player will automatically lose.

Since the possible moves from a given state do not depend on which player is going to play next, we can simply figure out if a given state is a "winning" or a "losing" position. Let s be a game state. We say that s is an N state if the *next* player to play has a winning strategy for the state s. We say that s is a P state if the next player has no winning strategy for the state s; equivalently, if the *previous* player has a winning strategy for the state s no matter what move the next player makes. So N states are next-player wins, and P-states are previous player wins.[30]

[30] Remember that this labelling assumes that everyone plays optimally and makes no mistakes! It is still possible for the next player to lose from an N state if they make the wrong move, but a state gets the label N if it is possible for the next player to win by playing optimally.

We can label states as N and P inductively, building up from the bottommost positions. First, it is clear that if s has no outgoing arrows, then it is a P state — the next player to play automatically loses, and hence the *previous* player has won. We call such states *terminal* states, because the game terminates or ends at these states. So any terminal state is a P state.

Therefore, anything that has at least one arrow to a terminal state is an N state: the next player can simply move to the terminal state, so that the player after the next player (aka the previous player) has no possible moves left. To generalise this, any state that has at least one arrow to a P state is an N state: the next player can simply move to the P state, which is guaranteed to be a losing position for the player after next (aka the previous player). So when is a state a P state? Well, a state is a P state if no matter what the next player does, the previous player has a winning strategy. This means that a state is a P state if and only if all outgoing arrows point to N states.

Definition 66. *The* outcome *of a game G is defined to be P if the game state G is a P-state, and N if G is an N-state.*

TODO *Draw running example*

Nim

Let us discuss *nim*, which is a very important example of an impartial combinatorial game. The game is played as follows. The start state consists of a finite number of piles of stones, each possibly of a different size. For instance, we may have the state $\{2, 3, 5\}$. We will represent states as *multisets*: that is, the order is unimportant, but entries can repeat. The size of each pile must be a non-negative integer. If a pile shrinks to size 0, we optionally omit it from the

representation, so that $\{2,3,5\}$ is the same as $\{0,2,3,5\}$.

A move consists of choosing *one* of the piles, and removing and discarding some of the stones in that pile. At least one stone must be removed, and the player may choose to remove all the stones from the chosen pile. For instance, from the state $\{2,3,5\}$, we can move to the state $\{2,2,5\}$ by removing one stone from the pile that had 3 stones. Or for instance, we could move to the state $\{2,5\}$, by removing all the stones from the pile that had 3 stones. The person who cannot make a move loses; this can only happen if the player is presented with the empty state $\{\}$.

Let us work out some easy examples. First, suppose that the start state consists of a single pile with 0 stones: $\{\}$. This is clearly a P-state. Next, suppose that the start state consists of a single pile with n stones for $n > 0$: $\{n\}$. This is an N-state, because the next player can remove all n stones to reach the terminal state $\{\}$.

Next, suppose that the start state is $\{m,n\}$, with both m and n positive. First suppose that $m = n$. We claim that this state, namely $\{n,n\}$, is a P-position. To see this, proceed by induction: the only possible sequence of moves from $\{1,1\}$ is

$$\{1,1\} \to \{0,1\} \to \{0,0\}.$$

Since $\{0,0\}$ is a P state, we see that $\{0,1\}$ is an N state, and so $\{1,1\}$ is a P state.

Now let $n > 1$, and assume the result for all $1 \leq k < n$. The only possible *type* of move from $\{n,n\}$ is $\{n,n\} \to \{m,n\}$, where $m < n$. This state is an N state, because there is a move $\{m,n\} \to \{m,m\}$, and we know by induction that $\{m,m\}$ is a P state. Therefore, $\{m,n\}$ is an N-state for all m such that $m < n$, and so all arrows out of $\{n,n\}$ point to N-states. Hence $\{n,n\}$ is a P state as well.

This is a more general technique, known as *mirroring*. In some situations, it is possible, by symmetry, to mirror the opponent's move so that the opponent is presented with a smaller version of the same kind of state as before. In this situation, the opponent will always be presented with a P state, by the same sort of inductive argument. Watch out for states in other games that can be deduced to be P states via mirroring!

When there are more than two piles, nim is not as easy to analyse. For example, the state $\{1,2,3\}$ is a P-state, although this is not completely obvious.[31] And therefore, for example, a state of the form $\{1,2,n\}$ for $n > 3$ is always an N-state.

[31] Try to convince yourself by drawing the game graph and using existing knowledge about states with one or two piles.

However, it turns out that any state of nim can be completely analysed, and there is an easy algorithm to figure out if the state is an N state or a P state. The answer, which is beautiful and somewhat mysterious, lies in the binary expansions of the pile sizes.

To get to the answer, we first recall some facts. Recall that the binary expansion of a non-negative integer is obtained by successively subtracting the largest power of 2 from that integer until we reach zero, and recording "1" for each power we subtract, and "0" for each power that we don't. We will usually use a subscript of 2 to indicate a binary representation; for example, $5 = 101_2$.

Moreover, we have the following binary[32] operation on non-negative integers, which we call either the *nim-sum* or XOR.

Definition 68. *The* nim-sum *of two non-negative integers m and n, denoted $m \oplus n$, is the bitwise XOR of their binary representations.*

We explain this definition via an example. Take $m = 5$ and $n = 15$. We have seen that $m = 101_2$, and $n = 1111_2$. To compute

Example 67. *Since* $15 = 1 \cdot 8 + 1 \cdot 4 + 1 \cdot 2 + 1 \cdot 1$, *its binary representation is* 1111_2. *Since* $16 = 1 \cdot 16 + 0 \cdot 8 + 0 \cdot 4 + 0 \cdot 2 + 0 \cdot 1$, *its binary representation is* 10000_2.

[32] *Binary* here refers to the number of inputs to this operation, not the base for the representation!

$m \oplus n$, we line up the binary representations aligned by binary place (that is, right aligned), and in each column, take the XOR of the bits, as follows.[33]

[33] Writing bitwise XOR also as $\oplus$, recall that $1 \oplus 1 = 0 \oplus 0 = 0$, and that $1 \oplus 0 = 0 \oplus 1 = 1$.

$$\begin{array}{r} 1\,0\,1 \\ \oplus\, 1\,1\,1\,1 \\ \hline 1\,0\,1\,0 \end{array}$$

Since $1010_2 = 1 \cdot 8 + 1 \cdot 2 = 10$, we see that $5 \oplus 15 = 10$.

We note some properties of the nim-sum operation.

1. Nim-sum is commutative: $m \oplus n = n \oplus m$. This is clear, because (bitwise) XOR is commutative.
2. Nim-sum is associative: $(m \oplus n) \oplus k = m \oplus (n \oplus k)$. This is clear, because (bitwise) XOR is associative.
3. The number 0 is the identity for nim-sum: $0 \oplus m = m \oplus 0 = m$ for every m.
4. Every number is its own inverse under nim-sum: $m \oplus m = 0$ for every m. This is because bitwise XOR has the same property. As a consequence, if we have $a \oplus b = c$, then by adding b to both sides, we see that $a = b \oplus c$, and similarly, $b = a \oplus c$.
5. Every number has a unique inverse: if $m \oplus n = 0$, then $m = n$. To see this, add m to both sides of the equation above, to get $m \oplus m \oplus n = m$, which means that $n = m$.

It turns out that given a nim state $\{n_1, \ldots, n_k\}$, it is useful and important to keep track of the nim-sum of the elements of the state (for short, the nim-sum of the state), which is $n_1 \oplus \cdots \oplus n_k$. The following lemma makes this precise.

Lemma 69. *Suppose that $\{n_1, \ldots, n_k\}$ is a nim state with each $n_i > 0$ and nim-sum 0. Then every possible move from this state will result in a state with a non-zero nim-sum.*

Proof. Suppose that $n_1 \oplus \cdots \oplus n_k = 0$. Consider any move from this state; without loss of generality, suppose that we change n_1 to n_1' after removing some stones. Let us compute the new nim-sum; it is

$$n_1' \oplus \cdots \oplus n_k = (n_1' \oplus \cdots \oplus n_k) \oplus (n_1 \oplus \cdots \oplus n_k),$$

because we know that $0 = n_1 \oplus \cdots \oplus n_k$. Now we cancel the pairs $n_i \oplus n_i$ for $i \neq 1$, to see that

$$n_1' \oplus \cdots \oplus n_k = n_1' \oplus n_1.$$

We know that $n_1' < n_1$, so these are distinct numbers. Their nim-sum cannot be zero! □

It turns out that the converse direction is true as well.

Lemma 70. *Suppose that $\{n_1, \ldots, n_k\}$ is a nim state with each $n_i > 0$, and nim-sum $s > 0$. Then there is* some *move that results in a state with zero nim-sum.*

Proof. We give the proof with a simultaneous running example. Consider the state $\{3, 6, 7\}$. The binary representations of these numbers are 11_2, 110_2, and 111_2 respectively. In general, consider the binary representations of the numbers n_i.

The nim-sum in the example is $010_2 = 2$, which is non-zero.

$$\begin{array}{r} 011 \\ 110 \\ \oplus\, 111 \\ \hline 010 \end{array}$$

In general, since $s > 0$, we see that s contains at least one "1" in its binary representation. In particular, the left-most 1 in s arises precisely because the column above it has an odd number of "1"s. In the example, the second column from the right has this feature; it contains three "1"s, which XOR to produce the "1" we see in s.

Now choose any of the n_i that contain a "1" in the column corresponding to the leftmost "1" in s. Let us call this column C. For instance, in the example, we could choose n_i to be $n_2 = 6$. Consider $n_i' = n_i \oplus s$. In our example, we get $6 \oplus 2 = 4$. Note that $n_i' \oplus s$ has a 0 in column C, and all columns to the left of column C are unchanged in n_i', because s only has zeroes in any column to the left of C.

This implies that n_i' must be less than n_i. This is because we are flipping a "1" in its binary representation to zero, without changing anything to the left of that "1": regardless of what changes happen to the right of this "1", the resulting value must decrease. So $n_i' < n_i$, and hence it is a valid nim move to change n_i to n_i'.

At the same time, let us compute the new nim-sum. Since $n_i' = n_i \oplus s$, it is

$$n_1 \oplus \cdots \oplus n_i' \oplus \cdots \oplus n_k = n_1 \oplus \cdots \oplus (n_i \oplus s) \oplus \cdots \oplus n_k.$$

Moving s out to the left and recalling that $n_1 \oplus \cdots \oplus n_k = s$, we see that

$$n_1 \oplus \cdots \oplus n_i' \oplus \cdots \oplus n_k = s \oplus s = 0.$$

This completes the proof. □

Note by the previous lemmas that in the game graph,

1. every state with zero nim-sum only points to states with positive nim-sum, and
2. every state with positive nim-sum points to *some* state with zero nim-sum.

Furthermore, the empty state, which is the only terminal position, clearly has zero nim-sum, and is a P-state. By following the algorithm of strategic labelling on game graphs, we have proven the following theorem.[34]

Theorem 71. *A nim state is a P-state if and only if it has zero nim-sum, and an N-state if and only if it has positive nim-sum.*

[34] The technical name for such an argument is *structural induction* on the game graph. Because the game graph is directed acyclic and finite, and because the N/P labelling is defined only in terms of states that come after a given state, we can build up the labelling from the labellings of the terminal states. Then at each step, we compare what we do to give the N/P label with the outputs of the two lemmas.

Game sum

In this section we consider the operation of *game sum*. It is a way to construct a new game from two given games. The definition is as follows.

Definition 72. *Let G and H be combinatorial games. Then $G + H$ is defined to be the game whose game state is a disjoint union of the game states of G and of H. Making a move in the game $G + H$ means that you either make a single move either in G or in H (but not both).*

We will think about the following question: can we deduce the outcome of $G + H$ if we know the outcomes of G and H?

Let us start with some easy cases. Let $\emptyset$ denote the "empty game": this is the game which has only one state and there are no possible moves. It is clear that the outcome of the game $\emptyset$ is P. It is also clear that the outcome of $G + \emptyset$ equals the outcome of G. This is because the game graph of $G + \emptyset$ is the same as the game graph of G, since there are no possible moves in the $\emptyset$ game.

What about if we add a game G to itself?

Proposition 73. *Let G be any impartial combinatorial game. The outcome of $G + G$ is always P.*

Proof. Informally, this is because one can use a mirroring strategy. If player 1 makes a move $G \to H$ in (say) the first copy of G, player 2 can make the same move $G \to H$ in the second copy of G. Continuing in this manner, player 1 will be the first one to run out of moves.

More formally, we can use structural induction on the game graph of G. For the base case, consider any terminal position of G, which is the same game as $\emptyset$. Now we know from the previous observation that the outcome of $\emptyset + \emptyset$ is the same as the outcome of $\emptyset$, which is P.

Suppose we know that for any position H reachable from G such that $G \neq H$, the outcome of $H + H$ is P. Starting at $G + G$, the possible reachable positions are $G + H$ for any move $G \to H$, or $H + G$ for any move $G \to H$. Let us show that the outcome of $G + H$ (and hence $H + G$) is N for any possible move $G \to H$. Recall that the outcome of $H + H$ is P, and there is a move from $G + H$ to $H + H$, namely, by making the move $G \to H$ in the first coordinate, namely in G. Therefore in the game graph of $G + G$, the position $G + H$ (and hence $H + G$) is labelled N, for every possible move $G \to H$. But the only arrows from the position $G + G$ are to positions of the form $G + H$ or $H + G$ as above. Therefore, $G + G$ is a P position as well. □

Now, what happens if we add two possibly different games together? Let us start with some examples. Consider the nim game $G = \{1, 2\}$ and $H = \{3\}$. These are both N positions. When we add two nim games, we simply get another, bigger nim game. So the game $G + H$ is just the nim game with state $\{1, 2, 3\}$. However,

we have seen that $G + H$ is a P position because its nim sum is $1 \oplus 2 \oplus 3 = 0$. So in this example, we added two N games to obtain a P game.

On the other hand, if we now take $G = \{1, 2\}$ and $H = \{4\}$, then $G + H$ has nim-sum $1 \oplus 2 \oplus 4 = 7 \neq 0$. So in this case, $G + H$ is an N game!

We observe that if G and H are two N games, then the outcome of $G + H$ may be either N or P. However, it is a powerful fact that if we take the sum $G + H$ where H is a P game, then the outcome of $G + H$ is determined by the outcome of G.

Theorem 74. *Let H be a P game and G be any game. Then the outcome of $G + H$ is the same as the outcome of G.*

Proof. We can see this informally as follows. Suppose that G is an N game. Then player 1 has a winning strategy in $G + H$, as follows. Player 1 should start by making an optimal move in G, sending $G \to G'$ where G' is a P game. Now if player 2 makes a move in H as $H \to H'$, we know that H' is an N position, so player 1 can counter it with an optimal move in H'. If player 2 makes a move in G' as $G' \to G''$, we know that G'' is an N position, so player 1 can counter it with an optimal move in G''. After each pair of moves, player 2 is presented with a game state of the form $A + B$ where A and B are both P games. No matter which move player 2 makes, player 1 can counter it to once again give player 2 a state of the form (P, P). The game eventually terminates with player 2 running out of moves.

If G is a P game, then $G + H$ is of the form (P, P). By reversing the previous argument, we see that no matter which move player 1 makes, player 2 can always counter it so that player 1 always has a game state of type (P, P). Thus player 2 has a winning strategy.

More formally, we can use induction on the game graphs again. The base case is that one of the games is terminal (or empty), in which case we know the result. By induction, suppose that for every possible move from $G + H$, which goes a state of type either (x, P) or (P, x), we know that the outcome of the resulting state is x.

First suppose that G is an N position. Then there is a move $G \to G'$ such that G' is a P position, so that $G' + H$ has type (P, P). Therefore by the inductive hypothesis, $G' + H$ has outcome P. Due to the existence of the arrow $G + H \to G' + H$, the position $G + H$ is an N position.

Now suppose that G is a P position. Then a move from $G + H$ either goes to $G' + H$, which is of type (N, P), or $G + H'$, which is of type (P, N). In either case, the outcome of the resulting state is N by the inductive hypothesis. We conclude that $G + H$ is a P position as well. □

The upshot of all this is that adding a P game to any game preserves the outcome, while adding an N game may change the outcome. The moral of the story is that all P games behave the same, while there are different kinds of N games. The Grundy labelling is a way to distinguish between these different kinds of N games.

Stable equivalence

The sum operation allows us to define an equivalence relation on games.

Definition 75. *We say that two games G and H are* stably equivalent, *written $G \sim H$, if for any game I, the games $G + I$ and $H + I$ have the same outcome. That is, both are N or both are P.*

Observe that the definition of stable equivalence on games is quite similar to the definition of $\sim_L$ for a language L used in the Myhill-Nerode theorem.

Let G be a P game. Then $G \sim \varnothing$. Indeed, for any game I, we have seen that $G + I$ and $I = I + \varnothing$ have the same outcome. In other words, all P games are equivalent to each other.

It turns out that *not* all N games are equivalent to each other. For example, the nim game $\{3\}$ and the nim game $\{4\}$ are both N. But $\{1,2\} + \{3\}$ is P whereas $\{1,2\} + \{4\}$ is N. That is, adding $I = \{1,2\}$ to $\{3\}$ and $\{4\}$ produces two games with a different outcome. So $\{3\}$ and $\{4\}$ are not equivalent.

Grundy labelling

How to we determine if two games are (stably) equivalent? The process of *Grundy labelling* allows us to better capture the behaviour of games under game addition.

First we define an operation called *mex*.

Definition 76. *Let $S = \{s_1, \ldots, s_k\}$ be a finite set of non-negative integers. The* minimum excluded *or* mex *of S, denoted* $\mathrm{mex}(X)$*, is the minimum non-negative integer that is not in S.*

Example 77. *If $S = \{0,1,2\}$ then $\mathrm{mex}(S) = 3$ If $S = \{0,2,4\}$, then $\mathrm{mex}(S) = 1$. If $S = \{4, 2000, 50\}$, then $\mathrm{mex}(S) = 0$.*

Definition 78. *The Grundy labelling is a labelling of a game graph, which takes values in positive integers. It is defined inductively as follows.*

1. *All terminal states are labelled by* 0*.*
2. *Consider a state G such that all states G' that G points to have been labelled. Let S be the set of labels of all G' such that there is an arrow $G \to G'$. Then label G by* $\mathrm{mex}(S)$*.*

Proposition 79. *The Grundy labelling enhances the N/P labelling. More precisely, a position is a P position if and only if its Grundy label is zero. More precisely, a position is an N position if and only if its Grundy label is positive.*

Proof. Once again, we use structural induction on the game graph, and compare both labelling methods. For terminal positions, the proposition is clear: they are P positions, and their Grundy label is always zero. Suppose we know the result for all positions reachable from a given game state G.

Suppose G is an N state. G will be labelled N if and only if there is an arrow $G \to G'$ where G' is labelled P. Since we know that the Grundy label of G' is zero, we see that the set S of all labels following G contains zero, and hence its mex must be positive. So the Grundy label of G is positive.

Suppose G is a P state. For every arrow $G \to G'$, the outcome of G' is N, and hence its Grundy label is positive. Since 0 does not appear among the Grundy labels of the possible G', we see that the Grundy label of G must be zero. This completes the proof. □

It turns out that Grundy labels are extremely useful in terms of computing outcomes, because they behave well with respect to game addition!

Theorem 80. *Let G and H be games with Grundy labels g and h respectively. Then the Grundy label of $G + H$ is $g \oplus h$.*

Proof. Let $s = g \oplus h$. Let S be the set of Grundy labels of $G' + H$ and $G + H'$, for arrows $G \to G'$ and $H \to H'$. By the inductive hypothensis, we know that these labels are precisely $g' \oplus h$ and $g \oplus h'$, where g' and h' are the Grundy labels of G and H respectively. Moreover, we know that g is the mex of all possible g', and h is the mex of all possible h'. Let us show that $s = g \oplus h$ is the mex of S.

First, let us show that $s \notin S$. If s were in S, then we would either have $s = g' \oplus h$ for some g', or $s = g \oplus h'$ for some h'. The two cases are symmetric, so we only tackle the first one. In that case we have $g \oplus h = g' \oplus h$, which means (by adding h to both sides) that $g = g'$. This is not possible.

Next, let us show that if $s' < s$, then $s' \in S$. If $s = 0$, there is nothing to prove, so suppose that $s > 0$. Consider the triple sum $g \oplus h \oplus s'$, which is non-zero. By our arguments in the nim section, we know that there is a possible move in either g, h, or s', such that the resulting nim-sum is zero. Note that because $s' < s$, any nim move that decreases s' takes it to some s'' such that $s'' < s' < s$, and $s'' \oplus g \oplus h = s'' \oplus s$ cannot be zero. So the optimal nim move *does not* decrease s'; instead it either decreases g or h. WLOG suppose it takes g to g'. Then we know that $g' < g$, and that $g' \oplus h \oplus s' = 0$, that is, $s' = g' \oplus h$. Now g' must be one of the labels of the games G' reachable from G, because $g' < g$ and g was the mex of all possible g'. Hence $g' \oplus h$ is the Grundy label of some game $G' + H$, reachable from $G + H$. Therefore $s' \in S$!

Since $s \notin S$ and for every $s' < s$ we have $s' \in S$, we see that $s = \text{mex}(S)$. □

We now show that Grundy labels contain the exact information to distinguish stable equivalence classes.

Theorem 81. *[Sprague-Grundy theorem] Two games are stably equivalent if and only if they have the same Grundy label.*

Before we explain why this is true, we need an intermediate observation.

Lemma 82. *If $G \sum H$, then $G + I \sim H + I$.*

Proof. To establish that $G + I \sim H + I$, we need to prove that for any game J, the games $G + I + J$ and $H + I + J$ have the same outcome. But since we know that $G \sim H$, the games $G + (I + J)$ and $H + (I + J)$ do have the same outcome. □

We are now ready to prove the Sprague-Grundy theorem.

Proof. [Proof of Sprague-Grundy theorem]

Suppose G and H have the same Grundy label, say a We need to prove that $G \sim H$. That is, for any game I, both $G + I$ and $H + I$ have the same outcome. Let the Grundy label of I be b. Then the Grundy label of $G + I$ is $a \oplus b$, which is the same as the Grundy label of $H + I$. Recall that a game is N if and only if the Grundy label is non-zero and P if and only if the Grundy label is zero. Since $G + I$ and $H + I$ have the same Grundy label, it is either non-zero in both cases or zero in both cases.

Conversely, suppose $G \sim H$. We need to prove that G and H have the same Grundy label. Suppose G has Grundy label a and H has Grundy label b. Since $G \sim H$, we have $G + H \sim H + H$. Since $H + H$ is a P-game, $G + H$ must be a P-game. The Grundy label of $G + H$ is $a \oplus b$. Since $G + H$ is a P-game, its Grundy label is zero, so $a \oplus b = 0$. But $a \oplus b = 0$ holds if and only if $a = b$. □

Theorem 83. *A game G with Grundy label n is stably equivalent to the nim game $\{n\}$.*

Proof. Both games have the same Grundy label, namely n. □