1 Sets and Mappings

1.1 Sets

We assume that we know what sets are, and we assume some familiarity with standard operations. For a candidate x and a set X, we say $x \in X$ if and only if x is an element of X. Otherwise, we say $x \notin X$. For two sets Y, Z, we say that $Y \subseteq Z$, if every element x such that $x \in Y$ implies that $x \in Z$. For sets X, Y, $X \cup Y$ and $X \cap Y$ will denote, respectively, the **union** and the **intersection**. We assume the familiar identity that $X \subseteq Y$ and $Y \subseteq X$ implies that $X = Y$[1] The symbol ϕ will usually denote the empty set. We assume we know when a set X has finite cardinality, and we denote this by $|X|$.

There are some standard constructions which help in creating new sets from old. For example, if X and Y are sets, then we define

$$X \times Y = \{(x, y) | x \in X, y \in Y\}$$

This is called the **product** of the sets X and Y. Another construction is the **power-set** 2^X which is the collection of all subsets of X:

$$2^X = \{Y | Y \subseteq X\}$$

When k is a positive integer, we may construct X-**choose**-k:

$$\left(\begin{array}{c} X \\ k \end{array} \right) = \{Z \subseteq X \; s.t. \; |Z| = k\}$$

When X and Y have finite cardinality, we see that $|X \times Y| = |X||Y|$, $|2^X| = 2^{|X|}$, and $\left| \left(\begin{array}{c} X \\ k \end{array} \right) \right| = \left(\begin{array}{c} |X| \\ k \end{array} \right)$.

A **partition** $\pi = \{X_\alpha\}_{\alpha \in I}$ is a collection I of subsets X_α of X such that (i) $X_\alpha \cap X_\beta = \phi$, for distinct elements X_α, X_β of I, and (ii) $\cup_{\alpha \in I} X_\alpha = X$. Thus a partition of X is a decomposition of the elements of X into disjoint subsets.

1.2 Relations

A relation R is a subset of $X \times X$. When $(x, y) \in R$, we also alternately say that x *is related to* y or that xRy. A relation R is called:

- **reflexive** if xRx for all $x \in X$. In other words, $(x, x) \in R$ for all $x \in X$.
- **transitive** if xRy and yRz always imply xRz.
- **symmetric** if xRy always implies yRx.
- **anti-symmetric** if xRy and yRx always imply $x = y$.

[1] This is rather delicate. We assume that elements x, x' can be compared, and that we can ask whether $x = x'$?

Definition 1.1 *A relation R is called an* **equivalence** *if R is reflexive, transitive, and symmetric.*

Let us fix an equivalence R on a set X. For an element $x \in X$, we have the **equivalence class** $[x]_R$ (or simply $[x]$) as:

$$[x]_R = \{y | y \in X, \; and \, xRy\}$$

Note that $[x]$ is a subset of X. Here are the first few observations on equivalences:

Lemma 1.2 *For an equivalence R on X, if $x, y \in X$, then either (i) $[x] = [y]$, or (ii) $[x] \cap [y] = \phi$.*

Proof: Suppose that we have $z \in [x] \cap [y]$. Thus yRz and xRz. By symmetry, and then by transitivity, we have xRy and yRx. Thus if $w \in [y]$, whence yRw, then xRy implies that xRw, and that $w \in [x]$. Thus $[x] \supseteq [y]$, and the converse is also easily shown. $\square$

Proposition 1.3 *Let R be an equivalence relation on X, then there is an index set I and elements $\{x_\alpha\}_{\alpha \in I}$ such that the collection $\{[x_\alpha]\}_{\alpha \in I}$ defines a partition on X. This partition is denoted by π_R.*

Proof: Let S be an index set, and let $\{x_s\}_{s \in S}$ be a family of subsets such that for any distinct $s, s' \in S$, we have $[x_s] \cap [x_{s'}] = \phi$. Let $X_S = \cup_{s \in S}[x_s]$. Clearly, one such index set is the set $\{1\}$ and x_1 is any element of X.

If $X_S \neq X$, then there must be an element $y \in X$ such that $y \notin X_S$. We create a new symbol s^* and let $S^* = S \cup s^*$, and let $x_{s^*} = y$. By the lemma above, $[y]$ does not intersect X_S, and thus S^* is an index set with the above properties. Now X_{S^*} is strictly bigger than X_S. This process can be continued to obtain an index set I so that $X_I = X$. $\square$

1.3 Mappings

Mappings or functions are a special family of subsets of $X \times Y$.

Definition 1.4 *For sets X, Y and $f \subseteq X \times Y$, we say that f is a* **function** *if (i) $(x, y) \in f$ and $(x, y') \in f$ always imply that $y = y'$, and (ii) for all $x \in X$, there is always a y such that $(x, y) \in f$. We say that f is a* **partial function** *if $f \subseteq Z \times Y$, is a function for a suitable subset $Z \subseteq X$.*

Generally, we denote a function f on $X \times Y$ as $f : X \to Y$ and we say that "f is a function from X to Y". When f is a function, we denote $(x)f$ or [2] $f(x)$ to be that y such that $(x, y) \in f$. For partial functions f, the set $Z \subseteq X$ above is called the **domain** of f and is easily shown to be well-defined.

The basic observation about functions is **composition** and its **associativity**. If $f : X \to Y$, and $g : Y \to Z$, then we can construct $f \circ g : X \to Z$, which is defined as $(x)f \circ g = ((x)f)g$. If $h : Z \to W$ was yet another function, then

[2] The "postfix" notation can rather useful later.

we have potentially two functions $(f \circ g) \circ h : X \to W$ and $f \circ (g \circ h) : X \to W$. However it turns out that:

$$(f \circ g) \circ h = f \circ (g \circ h)$$

A function $f : X \to Y$ is called

- **injective** if $(x)f = (x')f$ always implies $x = x'$.
- **surjective** if $y \in Y$ implies the existence of an $x \in X$ such that $(x)f = y$.
- **bijective** if f is both injective and surjective.

The function f is called an **injection**, **surjection** or **bijection** if it is, respectively, injective, surjective, or bijective.

For sets X, Y, the set (collection) of all functions from X to Y is denoted by $Hom(X,Y)$. Important subsets of $Hom(X,Y)$ are (i) $Inj(X,Y)$, the collection of all injections (ii) $Sur(X,Y)$, the collection of all surjections, and (iii) $Bij(X,Y)$, the collection of all bijections from X to Y. Of special significance is $Bij(X,X)$, which is simply denoted as $Bij(X)$. When X, Y are finite sets $|Hom(X,Y)| = |Y|^{|X|}$, and $|Bij(X)| = |X|!$.

When $f, g \in Hom(X,X)$, we see that $f \circ g \in Hom(X,X)$ as well. In particular, $f \circ f$ and $f \circ f \circ f$ are both in $Hom(X,X)$. We abbreviate $f \circ f$ as f^2, and $f \circ f \circ f$ as f^3, and so on. f^0 will stand for the identity function $1_X : X \to X$, where $(x)1_X = x$, for all x.

2 Analysis of a Single Injection

2.1 The Relation $\sim$

Let $f : X \to X$ be an injection, which we fix for the moment. We quickly check that if f is an injection, then so are f^k, for every k. We define the relation $\sim_f$, or simply $\sim$, on X as follows: $x \sim y$ iff there is a $k \geq 0$ such that $(x)f^k = y$ or $(y)f^k = x$. We then have the following lemma:

Lemma 2.1 *The relation $\sim$ is an equivalence relation.*

Proof: It is clear that $\sim$ is a symmetric and reflexive relation. The only non-trivial part is to show that $\sim$ is transitive. So let $x \sim y$ and $y \sim z$. In the case that $(x)f^m = y$ and $(y)f^n = z$, we have that $(x)f^m \circ f^n = (x)f^{m+n} = z$, and thus $x \sim z$. This is the easy case. The harder case is when, say, $(x)f^m = y$ and $(z)f^n = y$, with $m \leq n$. We claim that $(z)f^{n-m} = x$. Suppose not; then $(z)f^{n-m} = w$ is an element such that $(w)f^m = (z)f^{n-m} \circ f^m = (z)f^m = y$. Thus, both w and x are such that $y = (x)f^m = (w)f^m$. Now, f is an injection and therefore, so is f^m, whence $x = w$, which is a contradiction. $\Box$

We next analyse the nature of equivalence classes for $\sim$. We define the 'successor' function `succ`: $X \to X$, and the 'predecessor' partial function `pred`: $X \to X$ as follows: (x)`succ`$= (x)f$, while `pred`$= \{(x,y) | (y)f = x\}$. Thus

(x)pred is defined if and only if there is a pre-image y to x under f, and then it is defined to be this pre-image.

For an element $x \in X$, we carry out the following two procedures: define $x_0 = x$, and (1) for $i > 0$, define $x_i = (x_{i-1})\mathtt{succ}$, (2) for $i \leq 0$, if $(x_i)\mathtt{pred}$ exists, then define $x_{i-1} = (x_i)\mathtt{pred}$. Clearly, the distinct elements in the list of elements (x_i) above is exactly the equivalence class $[x]$. We see now that the distinctness of the elements in the list (x_i) is completely determined by the list $(x_i)_{i\leq 0}$. Clearly, for this "left-half", we have the following three mutually exclusive, and exhaustive possibilities:

1. **x_i exist for all $i \leq 0$ and are all distinct**: If that is so, then, in fact, the larger list $(x_i)_{-\infty<i<\infty}$ is composed of distinct elements. For is $x_N = x_{N+m}$, for some $N \geq 0, m > 0$, then we will have $x_N = (x_{-m})f^{N+m} = (x_0)f^{N+m} = x_{N+m}$. Whence, by the injectivity of f^{N+m}, we have $x_{-m} = x_0$, contradicting the hypothesis we have made in this case.

2. **x_i exist for all $i \leq 0$, and $x_{-(N+m)} = x_{-N}$, for some $N \geq 0$ and $m > 0$.** We claim, in this case, that $x_{i+m} = x_i$ for all i, and the sequence (x_i) is cyclic with period m, where m is the smallest integer satisfying the hypothesis. To see this, if $i < -(N+m)$, then apply f^{-i-N-m} to x_{i+m} and x_i. In the other case, apply f^{i+N+m} to $x_{-(N+m)}$ and x_{-N}.

3. **There is an $N \geq 0$ such that (x_{-N})pred does not exist**. In which case, we claim that $(x_i)_{i\geq -N}$ are all distinct. This is similar to either of the cases above.

We thus arrive at the classification of the equivalence classes:

Proposition 2.2 *Let $f : X \to X$ be an injection, and let $\sim_f$ be as defined above. Then, for any x, exactly one of the three cases hold:*
(i) $[x] = \{x_0, \ldots, x_{m-1}\}$ is finite, and $(x_i)f = x_{i+1}$, for $0 \leq i \leq m-2$, and $(x_{m-1})f = x_0$.
(ii) $[x] = \{\ldots, x_{-2}, x_{-1}, x_0, x_1, \ldots\}$, such that $x_0 = x$, and $(x_{i-1})f = x_i$, for all i.
*(iii) There is an $x_0 \in [x]$ such that $[x] = \{x_0, x_1, \ldots, \}$, where (x_0)*pred *does not exist, and $(x_{i-1})f = x_i$, for all $i \geq 1$.*

2.2 The (Finite) Cycle Representation

We next obtain a simple representation of f, when the domain X is a finite set. Clearly, in such a case, f is a bijection, every $[x]$ is finite, and therefore must be **cyclic** as in case (i) above. We may thus partition X by equivalence classes: $\pi_\sim$ is $X = [x^1] \cup \ldots \cup [x^k]$, for special elements $x^1, \ldots, x^k \in X$. Each x^i above is an element of the equivalence class $[x^i] = \{x_0^i, x_1^i, \ldots, x_{m_i-1}^i\}$, where $m_i = |[x^i]|$, and the numbering of the elements are in in Proposition 2.2.

The function f is then represented as a list of cyclic sequences:

$$f \equiv (x_0^1, \ldots, x_{m_1-1}^1), \ldots, (x_0^k, \ldots, x_{m_k-1}^k)$$

For any $x \in X$, to evaluate $(x)f$, we locate x in (exactly) one of the lists, say as x^i_j. The element $(x)f$ is then the next element in the i-th cycle. In other words, if $j < m_i - 1$, then $(x)f = x^i_{j+1}$, and equals x^i_0 in the case when $j = m_i - 1$.

This is best demonstrated by an example: if $X = \{1, 2, \ldots, 10\}$, and let f be represented as follows:

$$f \equiv (1, 3, 5, 6)(4, 10)(9)(2, 7, 8)$$

We conclude, for example, that $(1)f = 3$, $(6)f = 1$, $(9)f = 9$ and $(7)f = 8$.

Definition 2.3 *Let $f : X \to X$, and $Y \subseteq X$. We say that Y is an* **invariant subset** *for f, if for all $y \in Y$, $(y)f \in Y$.*

We abbreviate the above condition by saying $(Y)f \subseteq Y$. The following observation is then immediate:

Lemma 2.4 *If $f : X \to X$ is an injection on a finite set X, and $Y \subseteq X$ is an invariant subset, then Y there are elements $\{y_i | i = 1, \ldots, r\}$ such that $Y = \cup_{i=1}^r [y_i]$.*

Proof: If that were not so, then in the cycle representation of f, there would be an $y = x^i_j \in Y$ such that $x^i_{j+1} \notin Y$. However, $(x^i_j)f = x^i_{j+1}$, and thus $(y)f \notin Y$, and Y is not invariant! $\Box$

3 Cardinality of Infinite Sets

In this section we will associate an entity $|X|$ with every set X and arrive at some useful relations between $|X|$ and $|Y|$. For any set X, we say that the symbol $|X|$ is a cardinality.

The first relation on cardinalities is $\simeq$: if there is a bijection $f : X \to Y$, then we say that $|X| \simeq |Y|$. It is clear that $\simeq$ is an equivalence on cardinalities. The next relation is $\preceq$: if there is an injection $f : X \to Y$, then we say that $|X| \preceq |Y|$. Note that $\simeq$ and $\preceq$ simulate and extend the familiar relations $=$ and $\leq$, on cardinalities of finite sets.

Lemma 3.1 *If there is a surjection $f : X \to Y$, then $|Y| \preceq |X|$.*

Proof: We construct an injection $g : Y \to X$. For any $y \in Y$, since f is surjective, there is an x such that $(x)f = y$. We assign $(y)g = x$. Thus by making a choice[3] of an element in the set $(y)f^{-1}$, we may construct the required injection. $\Box$

Definition 3.2 *Let $\mathbb{N}$ be the set of natural numbers. We say that X is countable if either (i) X is a finite set, or (ii) $|X| = |\mathbb{N}|$.*

[3]This step follows from the so-called Axiom of Choice, which we cant get into, here.

3.1 The Schroeder-Bernstein Theorem

We now establish an important relationship between $\simeq$ and $\preceq$:

Theorem 3.3 (**Schroeder-Bernstein**) *If* $|X| \preceq |Y|$ *and* $|Y| \preceq |X|$*, then* $|X| \simeq |Y|$.

Proof: By translating the definitions of $\preceq$ and $\simeq$, we see that we need to prove the following: If there are injections $f : X \to Y$ and $g : Y \to X$, then there is a bijection $h : X \to Y$. So let us assume the above injections f and g. We also assume that $X \cap Y = \phi$. Let $Z = X \cup Y$, and define $\mu : Z \to Z$ as:

$$(z)\mu = \begin{cases} (z)f & \text{if } z \in X \subseteq Z \\ (z)g & \text{if } z \in Y \subseteq Z \end{cases}$$

We easily see that μ is an injection and that $(X)\mu \subseteq Y$, and $(Y)\mu \subseteq X$. Thus, for any $z = z_0$, if we form the sequence $z_i = (z)\mu^i$, then we see that the sequence (z_i) alternates between elements of X and elements of Y.

Thus, by Proposition 2.2, every equivalence class of $\sim_\mu$ is one of three types, *viz.*,
(i) $(z_i)_{-\infty < i < \infty}$ with $(z_i)\mu = z_{i+1}$.
(ii) $(z_i)_{i \geq 0}$, with $(z_i)\mu = z_{i+1}$, for all $i \geq 0$, and
(iii) $(z_i)_{0 \leq i \leq m-1}$ with $(z_i)\mu = z_{i+1}$, for $i < m-1$, and $(z_{m-1})\mu = z_0$.

In all cases, we see that in the listing of any equivalence class, the elements of X and Y alternate. Since $Z = X \cup Y$ and $X \cap Y = \phi$, every element of $X \cup Y$ appears exactly once, and is followed by an element from the 'opposite camp'. Thus the equivalence relation $\sim_\mu$ 'weaves' the elements of X and Y, which we will use to formally define the bijection $h : X \to Y$. For $x \in X$, if $[x]$ is of type (i) or (iii) above, we define $(x)h = (x)\mu \in Y$. When $[x] = (z_i)_{i \geq 0}$, we have two cases: (a) if $z_0 \in X$, then we define $(x)h = (x)\mu$, and (b) if $z_0 \in Y$, then we define $(x)h = (x)\texttt{pred}$, the predecessor of x. It is clear that $h : X \to Y$ is a bijection. $\Box$

The theorem is extremely useful in proving the existence of a bijection between sets. For example, let $\mathbb{Z}$ denote the set of integers. We show that $|\mathbb{Z}| \simeq |\mathbb{N}|$. The natural injection $i : \mathbb{N} \to \mathbb{Z}$ shows that $|\mathbb{N}| \preceq |\mathbb{Z}|$. Next, we construct $f : \mathbb{Z} \to \mathbb{N}$ as $(i)f = 2^i$ if $i \geq 0$, and $(i)f = 3^i$ if $i < 0$. Clearly, f is an injection, and thus by the Schroeder-Bernstein Theorem 3.3, $|\mathbb{Z}| \simeq |\mathbb{N}|$.

Similarly, we show that $|\mathbb{N} \times \mathbb{N}| \simeq |\mathbb{N}|$. The natural injection $(i)f = (i, 1)$ shows that $|\mathbb{N}| \preceq |\mathbb{N} \times \mathbb{N}|$. In the other direction, define $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ as $(i, j)g = 2^i 3^j$, which is an obvious injection. These two injection tell us that $|\mathbb{N} \times \mathbb{N}| \simeq |\mathbb{N}|$.

3.2 The Diagonalization Argument

We know construct two sets such that $|X| \preceq |Y|$, but $|Y| \not\preceq |X|$, provably!

Consider the set $\mathbb{N}$ and $Y = 2^{\mathbb{N}}$, the power-set of $\mathbb{N}$. Clearly, there is the natural injection $\alpha : \mathbb{N} \to Y$, defined as $(n)\alpha = \{n\}$. Thus, the integer maps to the corresponding singleton set. We claim that there is no bijection between $\mathbb{N}$ and Y.

Suppose there were such a bijection $\beta : \mathbb{N} \rightarrow Y$. We will arrive at a contradiction as follows. Note that every element of Y may be regarded as a boolean sequence: for a subset $S \subseteq \mathbb{N}$, we form the infinite sequence $v_S = (v[1], \ldots, v[i], \ldots)$, where $v[i] = 1$ iff $i \in S$, and $v[i] = 0$ otherwise. Thus v_S is 'indicator' for the set S. Conversely, any 0-1 vector $(v[1], \ldots)$ corresponds to a subset of $\mathbb{N}$. Thus the bijection β sets up a bijection between $\mathbb{N}$ and infinite 0-1 vectors. Thus for each i, there is the sequence [4] $\beta(i) = (\beta(i)[1], \beta(i)[2], \ldots)$, and since β is a bijection, for any 0-1 sequence v, there must be an i such that $\beta(i) = v$. Based on this bijection, we construct the special sequence $y = (y[1], y[2], \ldots)$ defined as:

$$y[i] = \begin{cases} 0 & \text{if } \beta(i)[i] = 1 \\ 1 & \text{if } \beta(i)[i] = 0 \end{cases}$$

Since y is an infinite 0-1 sequence, there must be an n such that $\beta(n) = y$. However, that cannot be because y disagrees with the n-th sequence in the n-th place! In other words, $y[n] = 1$ iff $\beta(n)[n] = 0 = y[n]$!. This is is nonsensical, and thus β cannot exist.

To understand the sequence y better, imagine the matrix M such that $M[i, j] = \beta(i)[j]$, i.e., the $[i, j]$-th entry of M is the j-th entry of the i-th sequence. The sequence y is the *complement of the diagonal* of the matrix M, and hence the so called **diagonalization argument**.

We generalize this result for arbitrary X:

Proposition 3.4 *For any set X, there cannot be a bijection between X and 2^X.*

Proof: Suppose there were such a $\beta : X \rightarrow 2^X$. Form the set $Y \subseteq X$ defined as:

$$x \in Y \text{ iff } x \notin \beta(x)$$

We claim that there is no $x' \in X$ such that $Y = \beta(x')$. If indeed there were such an x', then let us investigate if $x' \in Y$. To check this, we see that $x' \in Y$ iff $x' \notin \beta(x') = Y$. Thus $x' \in Y$ iff $x' \notin Y$, which is clearly untenable! $\Box$

4 Groups

In this section, we generalize the notion of $\sim_f$, that we defined for a single bijection, and then arrive at the notion of a **concrete group**. We then give an alternate formulation of this notion, which is the **abstract group**.

[4] We use the prefix notation for functions in this subsection.

4.1 Concrete Groups

So let $F = \{f_1, \dots, f_r\}$ be a collection of bijections on the set X. We define a relation $\sim_F$, for this family:

Definition 4.1 *For elements $x, y \in X$, we say $x \sim_F y$ iff there is an $f \in F$ such that $(x)f = y$.*

We next examine if $\sim_F$ is an equivalence relation:

- **reflexivity** requires $x \sim_F x$ for all $x \in X$. This is certainly not guaranteed. However, if the identity function $1_X : X \to X$ is in the family F, i.e., $1_X(x) = x$, then $\sim_F$ is reflexive.
- **symmetry** requires $x \sim_F y$ to imply $y \sim_F x$. This is easily ensured if $f \in F$ should imply $f^{-1} \in F$. Whence, $(x)f = y$ will imply $(y)f^{-1} = x$, and thus symmetry would follow.
- **transitivity**: supposing that $x \sim_F y$ and $y \sim_F z$, and say further that $(x)f = y$ and $(y)g = z$, where $f, g \in F$, the if $f \circ g$ were also to be in F, then $(x)f \circ g = z$, and thus $x \sim_F z$ would follow.

Motivated by this, we make the following definition:

Definition 4.2 *An* **concrete group** *F, X is a collection of bijections $F \subseteq Bij(X)$, on the set X, such that:*
*(i) $1_X \in F$. (***presence of identity***)*
*(ii) $f \in F \Rightarrow f^{-1} \in F$. (***presence of inverses***)*
*(iii) $f, g \in F \Rightarrow f \circ g \in F$. (***closure under composition***)*

This makes $\sim_F$ an equivalence relation on X. The equivalence class $[x]$ is called the **orbit** of x, and denoted by $O(x)$.

We begin with an important example:

Example 4.3 *Let S be a square cardboard piece with vertices $1, 2, 3, 4$, in that order, going clockwise. So let $X = \{1, 2, 3, 4\}$, and let D_4 be the collection of* symmetries *of the square. We have identified* 8 *such symmetries: $\sigma_0, \dots, \sigma_3, \mu_0, \dots, \mu_3$. While σ_i is a rotation, μ_j is a reflection, and exposes the back face of the cardboard piece. Each symmetry operation produces a bijection on the vertices of the square, e.g., the symmetry σ_1 takes the vertex 1 to the place of vertex 2, and 2 to the place of 3, and so on. These 8 symmetries and the induced bijections (in cycle notation) on the vertices are shown in the figure 4.3 below. For example, μ_2 corresponds to the reflection along the* 2-4 *diagonal, and thus fixes those vertices, but interchanges 1 and 3.*

One may check that D_4 enjoys all the requirements of a concrete group: for example, (i) σ_0 is the identity, (ii) (iii) the inverse of σ_1 is σ_3 and that of μ_0 is μ_0 its elf, and (iii) $\sigma_1 \circ \sigma_1 = \sigma_2$, and $\sigma_1 \circ \mu_0 = \mu_3$, and so on.

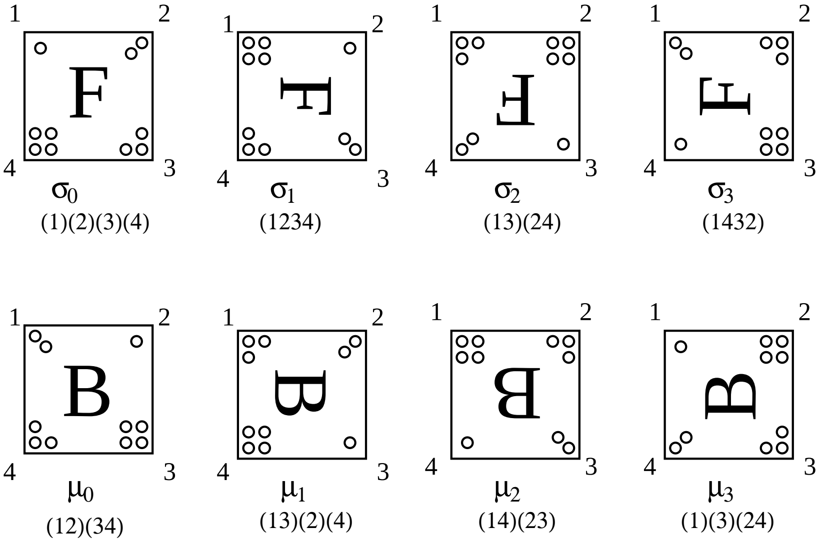


Figure 1: The Group D_4

In fact, the elements $\sigma_1 = \sigma$ and $\mu_0 = \mu$ 'generate' the group D_4 under succesive operations of composition, for example, $\sigma^3 = \sigma_3$. The 'defining relations' are the identities which are easily verified: (i) $\sigma^4 = 1_X$, (ii) $\mu^2 = 1_X$, and (iii) $\mu\sigma\mu = \sigma^3$.

There is only one equivalence class, viz., the whole of X. In other words, a vertex may be taken to any other vertex by some symmetry.

4.2 Abstract Groups

Definition 4.4 *The* **abstract group** *is a set G with an operation $\cdot : G \times G \to G$ called* **multiplication**. *Thus $g, g' \in G$, then $g \cdot g' = g''$ is another element of G. This multiplication has the following properties:*
*(i) There is an $e \in G$ such that $e \cdot g = g \cdot e = g$ for all $g \in G$ (***existence of identity***).*
*(ii) For every $g \in G$, there is a g' such that $g \cdot g' = g' \cdot g = e$ (***existence of inverse***).*
*(iii) Given any three elements g, g' and g'', we have $(g \cdot g') \cdot g'' = g \cdot (g' \cdot g'')$ (***associativity***).*

We begin with some examples:

Example 4.5 *1. The set of integers $((Z), +)$ under addition. The identity is 0, and the inverse of a is $-a$.*

2. The set of reals $(\mathbb{R}, +)$ under addition.

3. *Let n be a fixed positive integer. The set of integers modulo n, i.e., $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ under addition also form a group. Recall that $a+b$ in $\mathbb{Z}_n$ is obtained by treating the numbers a and b as integers, performing the addition as integers, and then taking the remainder after dividing by n. Note that associativity of the addition in $\mathbb{Z}_n$ requires proof.*

Example 4.6 1. *The set of non-zero reals $\mathbb{R}^*$ under multiplication is a group. The identity is 1.*

2. *Let $GL_n(\mathbb{R})$ denote all real valued, invertible $n \times n$ matrices. These form a group under matrix multiplication with the identity matrix I_n as the identity.*

3. *Let $SL_n(\mathbb{R})$ denote that subset of $GL_n(\mathbb{R})$ with determinant 1. Since $det(AB) = det(A)det(B)$, we see that $SL_n(\mathbb{R})$ is a group.*

4. *Let X be a set, and $Bij(X)$, the collection of all bijections on X. Then $Bij(X)$ is a group under composition. If $X = \{1, 2, \ldots, n\}$, then $|Bij(X)| = n!$ and it is called the* **symmetric group** *S_n.*

Our next suites of example come from concrete groups, and because of its importance, we state it as a proposition.

Proposition 4.7 *Let (F, X) be a concrete group of bijections on a set X. Then F is an abstract group under composition, with 1_X as the identity.*

Proof: We first note that by the definition of a concrete group, F is closed under composition. Thus composition does indeed define a multiplication on F. Next, by its vary nature, this multiplication is associative. The existence of the identity and inverses are implied by the other requirements of a concrete group. □

Thus all concrete groups, and specifically D_4, are abstract groups. It is also true that abstract groups may be realized as concrete groups, but we will not need that here.

5 Subgroups and Cosets

5.1 Subgroups

Definition 5.1 *Let G be a group. A subset $H \subseteq G$ is a* **subgroup** *if H is closed under multiplication (that from the overlying set G) and is an abstract group under this multiplication.*

Examples of subgroups abound:

Example 5.2 1. *For a fixed integer n, let $n\mathbb{Z} = \{na | a \in \mathbb{Z}\}$. We see that $0 \in n\mathbb{Z}$, and that it is indeed closed under addition and taking inverses.*

2. *Let m, n be integers such that m divides n and let*[5] $m\mathbb{Z}_n = \{ma | a \in \mathbb{Z}_n\}.i$ *This is a subgroup.*

3. $SL_N(\mathbb{R})$ *is a subgroup of* $GL_n(\mathbb{R})$.

4. *Non-zero rational* $\mathbb{Q}^*$ *is a subgroup of* $\mathbb{R}^*$.

5. *Every concrete group* (F, X) *is a subgroup of* $Bij(X)$.

6. *Let* $S_{n-1} = \{\sigma \in S_n | (n)\sigma = n\}$ *be all bijection on* $\{1, \ldots, n\}$, *which fix* n. *Then* S_{n-1} *is a subgroup of* S_n.

7. $\{\sigma^i | i = 0, 1, 2, 3\}$ *is a subgroup of* D_4.

An important class of subgroups arise from concrete groups:

Lemma 5.3 *Let* (F, X) *be a concrete group and let* $x \in X$ *be a fixed element of* X. *Let* $F_x = \{f \in F | (x)f = x\}$ *be the collection of all bijections in* x *which* **fix** x. *Then* F_x *is a subgroup of* F.

We leave the proof of this easy lemma to the reader. The subgroup F_x is called the **stabilizer** of $x \in X$. In our example of D_4, we see that the stabilizer of vertex 1 is $\{\sigma_0, \mu_3\}$.

Any subgroup $H \subseteq G$ defines two equivalences L_H and R_H (or simply L and R) on the elements of G.

Definition 5.4 *Let* $H \subseteq G$ *be a subgroup. We say:*
(i) gLg' *iff there is an* $h \in H$ *such that* $hg = g'$.
(ii) gRg' *iff there is an* $h \in H$ *such that* $gh = g'$.

Proposition 5.5

- *Both* L *and* R *are equivalences.*
- *For either of the relations, say* L, *the equivalence class* $[g]_L$ *of the element* $g \in G$ *equals* $Hg = \{hg | h \in H\}$. *In particular,*$[e]_L = H$.
- *Furthermore, for any element* $g \in G$, *the map* $\phi : H \to Hg$, *given by* $\phi(g) = hg$ *is a bijection.*

Proof: We prove the assertion for the relation L. Clearly, since $e \in H$, hLh and L is reflexive. Furthermore, $hg = g' \Rightarrow h^{-1}g' = g$, and since $h^{-1} \in H$ as well, L is symmetric. Finally, $hg = g'$ and $h'g' = g''$ implies $h'hg = g''$, and since $h'h \in H$, transitivity of L follows.

Clearly, every element of the form $g' = hg$ certainly belongs to $[g]_L$. On the other hand, if $g' = hg$ then $g' \in Hg$, and thus $[g]_L = Hg$. Next we consider the map $\phi : H \to Hg$. The surjectivity of ϕ is obvious. If $h'g = hg$, then $h'gg^{-1} = hgg^{-1}$ and thus $h = h'$ and ϕ is injective. □

The set Hg (respectively gH) is called the **right coset** (respectively **left coset**) of g with respect to H.

[5] Here, and in the previous example, ma will mean the addition of the element a succesively, m times.

5.2 Coset Representatives

Let us fix a subgroup $H \subseteq G$, and the relation L_H. We see that since L is an equivalence class, G may be expresses as the disjoint union of equivalence classes, or cosets. Thus there is an index set I and elements $\{g_\alpha | \alpha \in I\}$ such that

$$G = \cup_{\alpha \in I} H g_\alpha$$

This simple observation, and the 5.5(3) has the following simple consequence:

Theorem 5.6 *(Lagrange) If G is a finite group and $H \subseteq G$ is a subgroup, then $|H|$ divides $|G|$ and $|G|/|H|$ equals the number of distinct cosets of H in G.*

Proof: We see that $|G| = \sum_{\alpha \in I} |Hg_\alpha|$, and since there is a bijection between H and Hg_α, we see that $|Hg_\alpha| = |H|$. The result follows. □

These special elements $\{g_\alpha | \alpha \in I\}$ are called **coset representatives**. They are certainly not unique in having the above property. We must also warn that if (g_α) serve for the relation L, it **may not** be a family of coset representatives for R. In other words, for some $g_1, g_2 \in (g_\alpha)$, there may be no element of H such that $g_1 = hg_2$, while it may be that $g_1 = g_2 h$ for some $h \in H$.

As examples of coset representatives, we have $H = 5\mathbb{Z} \subseteq \mathbb{Z}$. The cosets of H in $\mathbb{Z}$ are the 5 subsets $H_0, \ldots, H_4$, where

$$H_i = \{5n + i | n \in \mathbb{Z}\}$$

Typical coset representatives are $\{0, 1, 2, 3, 4\}$, where, e.g.,

$$H_3 = H + 3 = \{5n + 3 | n \in \mathbb{Z}\}$$

Another possibility for the coset representaives is $\{5, 11, 13, -2, 104\}$. Note that $H + 3 = H + 13$.

A nice set of coset representatives for the subgroup $\{\sigma^0, \mu_3\}$ are $\{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$.

5.3 Stabilizers and Orbits

Recall, that for a concrete group (F, X), the orbit $O(x) = \{y \in X | \exists f \in F s.t. (x)f = y\}$ is the equivalence class $[x]$ under $\sim_F$. There is a direct relationship between cosets and orbits which exhibits the difference between the relations R and L.:

Theorem 5.7 *Let (F, X) be a concrete group. Let $x \in X$ be a fixed element, and let $O(x)$ be its orbit. Consider the maps $\psi_L, \psi_R : F \to O(x)$ defined as $\psi_L(f) = (x)f \in O(x)$, and $\psi_R(f) = (x)f^{-1} \in O(x)$. We have:*
(i) The inverse image $H = (x)\psi_L^{-1}$ is the stabilizer of x. The inverse image $H_y = (y)\psi_L^{-1}$ is the coset Hf, where f is any element of F such that $(x)f = y$.
(ii) The inverse image $H = K = (x)\psi_R^{-1}$ is the stabilizer of x. The inverse image $K_y = (y)\psi_R^{-1}$ is the coset fK, where f is any element of F such that $(y)f = x$.
(iii) If F is finite, then $|F| = |H||O(x)|$.

Proof: We shall prove (i). Part (ii) is identically proved, while (iii) follows from Lagrange's theorem 5.6. Firstly, it is clear that $H = F_x$, the stabilizer of x. Next, if $f \in F$ is any element such that $(x)f = y$, then $\psi_L(f) = y$. Further, if $h \in F_x$ then $(x)h \circ f = y$ as well, and thus $Hf \subseteq H_y$. Conversely, if $g \in H_y$, then $(x)g \circ f^{-1} = (y)f^{-1} = x$, and thus $g \circ f^{-1} = h \in H$, and thus $g \in Hf$. $\Box$

Thus, for concrete groups, coset representatives for stabilizers may be constructed from the orbit elements by using either relation L or R. For example, with R, one may choose coset representatives f for each element $y \in O(x)$ such that $(y)f = x$.

For the example D_4, we have $O(1) = \{1, 2, 3, 4\}$, and $F_1 = \{\sigma_0, \mu_3\}$. Thus $|O(1)||F_1| = 4 \cdot 2 = 8 = |D_4|$. The listing $1, 2, 3, 4$ of the orbit leads us to elements $\sigma_0, \sigma_3, \mu_1, \sigma_1$ for R, and $\mu_3, \sigma_1, \mu_1, \sigma_3$ for L, as possible coset representatives.

In gneral, it is clear that, there may exist $f, g \in F$ such that $(x)f \neq (x)g$ while $(y)f = (y)g = x$ for some $x, y \in X$. In which case, f, g may be chosen as elements of a system of coset representatives for one relation (here L) but not for the other.

6 Symmetries

In this section, we discus groups which arise naturally as symmetries of rigid bodies. Let S be a polyhedral (i.e., its faces are all parts of planes) rigid body. An example of a a non-polyhedral rigid body is the cylinder, or say, the sphere. In general, however, any rigid body may be 'approximated' by a polyhedral rigid body. Clearly, polyhedrality also implies that its edges are straight lines.

We consider the ambient space to be $\mathbb{R}^3$, the real euclidean space, familiar to all of us. An affine transformation on $\mathbb{R}^3$ is a re-coordinatization of the space by substituting in place of x, y and z, linear forms of the type $ax + by + cz + d$ such that the transformation should be a bijection on $\mathbb{R}^3$. It is easy to show that affine transformations compose and lead to affine transformations, and that their inverses are also affine. Thus they form an important subgroup of all bijections on $\mathbb{R}^3$.

A symmetry of $S \subseteq \mathbb{R}^3$ is an affine linear tranformation $\phi : \mathbb{R}^3 \to \mathbb{R}^3$, such that $\phi(S) = S$. It is clear that, planes go to planes, and thus faces of S go to faces of S, and edges to edges, vertices to vertices. Thus each symmetry of S induces a separate permutation on the collection of vertices, and then on the edges, and similarly on the faces. Furthermore, usually the affine transformation is completely determined by the permutation it induces on the finite sets above. It is clear that $Symm(S) = \{\phi \text{ affine } | \phi(S) = S\}$ is actually a subgroup.

We have already seen an exmaple of a group of symmetry, viz., D_4, the symmetries of a flat square. We shall next compute symmetries of a few more rigid bodies:

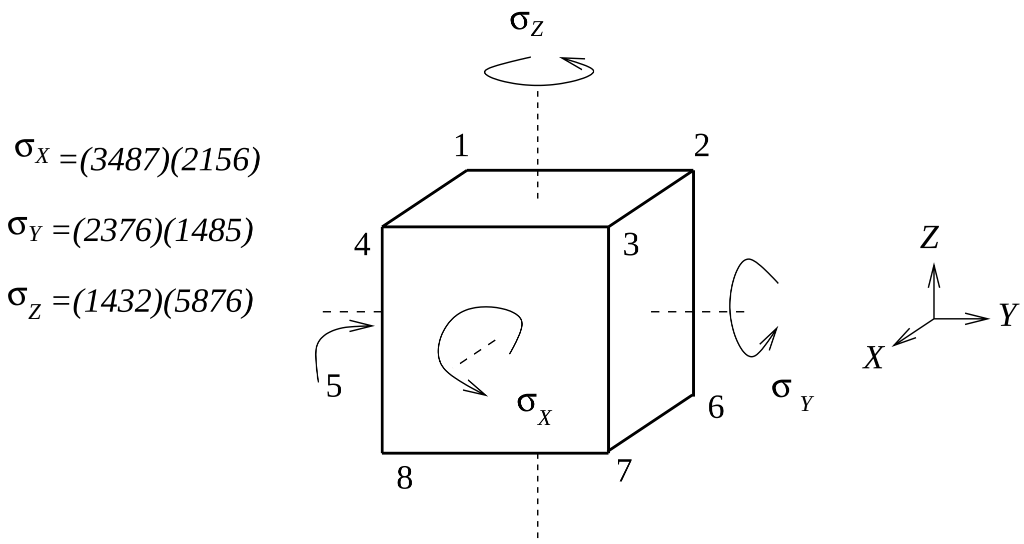


Figure 2: The Cube

6.1 The Cube

We consider first the unit cube C, which is shown in the figure below. The coordinate axes are as marked, and the basic symmetries are σ_X, σ_Y and $\sigma_Z \in Sym(C)$ as shown in the figure, which correspond to rotations of the cube along the appropriate axis.

Note that these basic symmetries induce a permutation on the vertices $V = \{1, 2, \ldots, 8\}$. These permuations are also reported in the figure, in their cycle notation. In general, too, every symmetry will induce an action on the set V, and thus we may say that $Sym(C)$ is a concrete group acting on V. The converse is also true: any symmetry is completely determined by its action on the vertices V.

The first objective is to work out $|Sym(C)|$, the number of possible symmetries of C. This is easily calculated by applying Theorem 5.7 suitably. Since $Sym(C)$ is a concrete group acting on V, lets fix a vertex, say 1, and compute the stabilizer $Stab(1) \subseteq Sym(C)$. This is easily seen to be obtained by rotations of the cube around the body-diagonal 1-7. Thus, if μ is a single rotation with its action on V as $\mu = (1)(7)(245)(386)$, then we see that

$$Stab(1) = \{\mu^0, \mu^1, \mu^2\}$$

Thus μ^3 is the identity, and $|Stab(1)| = 3$. Now, it is clear that there are symmetries which will take the vertex 1 to any of the eight vertices, and thus the orbit $O(1)$ equals V. Thus, by Theorem 5.7, $|Sym(C)| = |Stab(1)||O(1)| = 8{\cdot}3 = 24$. Indeed, one may check that the permutations σ_X, σ_Y and σ_Z generate, under compositions, a subgroup of size 24, of the ambient group $Bij(V)$, of all

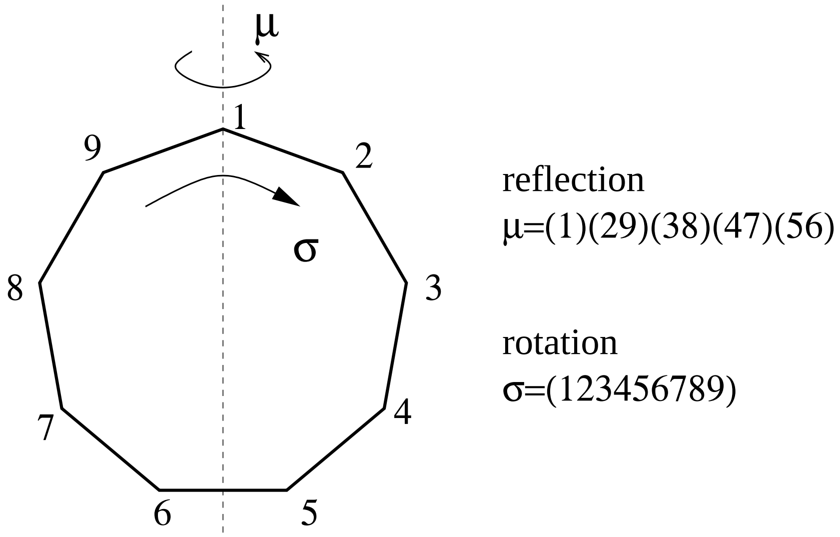


Figure 3: The regular nonagon

bijections on V. In effect, we thus 'know' the group $Sym(C)$ concretely, in terms of its action on V.

The action of $Sym(C)$ on V induces an action on $X = \binom{V}{2}$ as well: given a $\phi \in Sym(C)$, and a $\{i,j\}$, we say that $\{i,j\}\phi = \{i\phi, j\phi\}$. Thus $Sym(C)$ will also act on all 'edges' which connect two vertices. Under this action, we see that X splits into 3 orbits: $O(\{1,4\})$ the collection of 12 'true' edges, $O(\{1,3\})$ the collection of 12 face diagonals, and $O(\{1,7\})$, the collection of 4 body diagonals, adding up to the total $28 = |X|$. One may apply Theorem 5.7 backwards and conclude that there are 2 symmetries which will stabilize a 'true' edge, 2 again which will stabilize a face diagonal, and 6 for a body diagonal.

6.2 The Dihedral Groups D_n

Our next rigid body is the regular n-sided polygon P_n in the plane $\mathbb{R}^2$. The regular 9-gon is shown in the figure below. Note that the vertices are labelled as $V = \{1, 2, \ldots, 9\}$, and along with that are shown two obvious symmetries: (i) σ, the rotation, by $\frac{2\pi}{n}$, and in this case $\frac{2\pi}{9}$. and (ii) μ, the reflection about the axis defined by the vertex and the centre. The cycle notation for these symmetries as acting upon the vertices, is also shown below.

The group $Sym(P_n)$ is tarditionally denoted as D_n, and is called the **dihedral group**. As before, if we fix the vertex 1, we see that σ^0 and μ are the only permutations which will fix the vertex 1, and preserve adjacencies. Since the orbit must be the whole of V, we see that $|D_n| = 2 \cdot |V| = 2n$.

It will turn out that σ and μ 'generate' the group D_n. A couple of simple observations about these special elements:

(i) $\sigma^n = 1 = \mu^2$. In other words, n consecutive rotations or 2 reflections result in the identity map on P_n. Thus $\mu^{-1} = \mu$ and $\sigma^{-1} = \sigma^{n-1}$.
(ii) $\mu\sigma\mu = \sigma^{n-1} = \sigma^{-1}$. This is also expressible as $\mu sigma = \sigma^{n-1}\mu$. This is an important commutation property, as we shall see below.

Next, note that if we have two symmetries, then their composition is also a symmetry. Thus interpreting σ and μ to be elements of the group $Bij(V)$, of bijections on V, and doing succesive compositions on σ and μ, we see that the smallest subgroup of $Bij(V)$ containing σ and μ must contain all elements of the form $\sigma^i\mu^j\sigma^k \ldots \mu^r\sigma^s$. Now the commutation rule comes in handy: we illustrate this by an example: say $n = 9$, as in our case, and we wish to 'simplify' the element $\sigma^3\mu^3\sigma^2\mu^2$. Rule (i) above tells us that $\mu^3 = \mu$ and $\mu^2 = 1$, and thus $\sigma^3\mu^3\sigma^2\mu^2 = \sigma^3\mu\sigma^2$. Tne next rule tells us that $\mu\sigma = \sigma^8\mu$ and thus: $sigma^3\mu^3\sigma^2\mu^2 = \sigma^3\mu\sigma^2 = \sigma^3\sigma^8\sigma^8\mu = \sigma^{19}\mu = \sigma\mu$ (since $\sigma^8 = 1$). Thus, in general, every element in the group which contains σ and μ may be written as $\mu^i\sigma^j$ with $0 \leq i \leq 1$ and $0 \leq j \leq n-1$. We leave it to the reader to check that each of these $2n$ elements are actually distinct, and that they result in different actions on the set V.

Thus, we have identified $2n$ symmetries which arise just from composing σ and μ. Since $2n$ is precisely the cardinality of D_n, these elements must constitute the whole of D_n. Thus

$$D_n = \{\mu^i\sigma^j | 0 \leq i \leq 1, 0 \leq j \leq n-1\}$$

7 Polya Theory

In this section, we will investigate a problem, which is now traditionally known as the Polya's Counting Problem.

7.1 The Necklace Problem

A simple example is that of counting coloured necklaces. Consider, for example, the three necklaces in Figure 7.1 below. Each necklace has 9 beads, with 5 coloured white, 2 each, grey and black. In some sense, these pictures may well be pictures of the same necklace, albeit in different positions. For example, the necklace (a) and (c) may well be pictures taken from the front and back of the same necklace, while those in (a) and (b) differ by a 'rotation'.

Thus, to explain the equivalence of the three necklaces, we may model this necklace as a regular nonagon with coloured vertices corresponding to the colorings of the bead. Thus, for example, the necklace in Figure 7.1(a) corresponds to the colouring function $f : V \to \{Black, Grey, White\}$ as shown in Figure 7.1. Let us fix $\mathcal{C}$ as the set of colours. Let $f, g : V \to \mathcal{C}$ denote the functions for necklaces (b) and (c) respectively. The assertion that the necklaces (a) and (b) are equivalent is the same as saying that (i) there is a ϕ which is a symmetry of the regular nonagon, and thus acts as a bijection (also) $\phi : V \to V$, and (ii) the function g is obtained by composing ϕ with f. Thus $g = \phi \circ f$. In this case, ϕ is actually given by the reflection μ, see Figure 6.2.

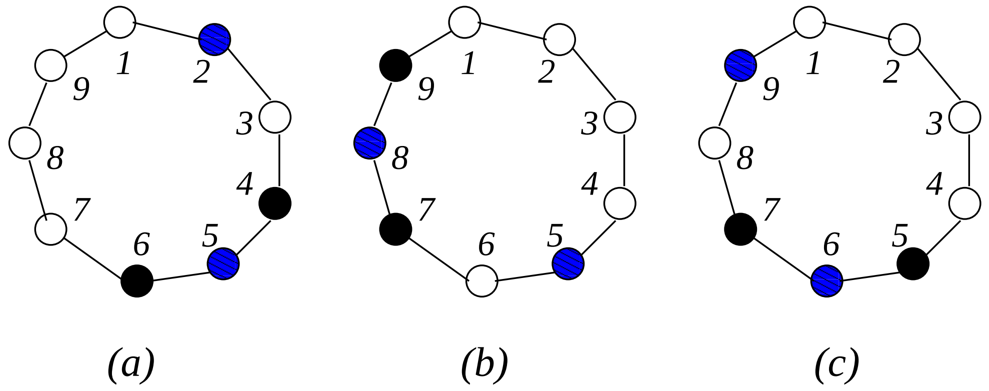


Figure 4: Equivalent Necklaces

We may thus say that colourings correspond to functions $h, h' : V \to \mathcal{C}$. Given such functions h, h', we say that h is 'equivalent' to h' if there is a symmetry $\phi : V \to V$ such that $h = \phi \circ h'$. The Necklace Counting question is:

Question: What is the number of distinct un-equivalent necklaces?

7.2 The Question and Orbit-Counting

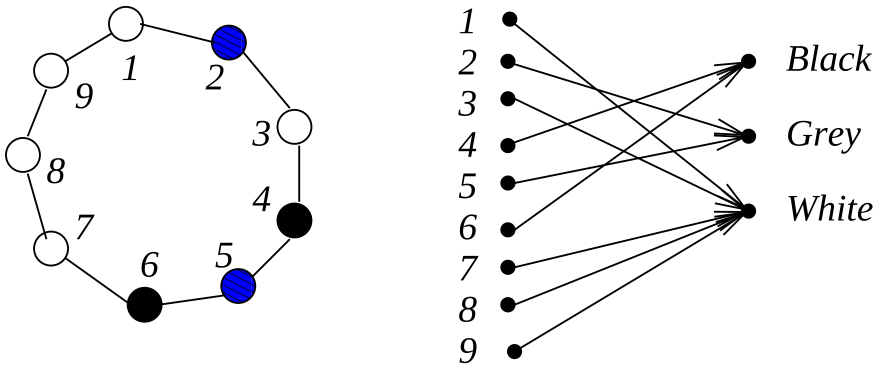
Thus, let G be a concrete group acting on a set X. Let $\mathcal{C}$ be a set of colours and let $\mathcal{F}$ be the collection of all functions $f : X \to \mathcal{C}$. Thus, when $X = V$, the set of vertices of the nonagon, or alternately the beads of our necklace, and $\mathcal{C} = \{Black, Grey, White\}$, the set $\mathcal{F}$ is the collection of all coloured necklaces.

We put a relation $\sim$ on $\mathcal{F}$ thus: $h, h' \in \mathcal{F}$, then we say $h \sim h'$ if there is an element $\phi \in G$, the group, such that $h = \phi \circ h'$. We check easily. using the group axioms on G, that $\sim$ is an equivalence relation. Let $[h]$ denote the equivalence class of h under $\sim$. Our question is then just counting the number of equivalence classes into which $\sim$ divides $\mathcal{F}$. Thus, there must be $\mathcal{H} = \{h_1, \ldots, h_k\} \subseteq \mathcal{F}$ such that $\mathcal{F} = \uplus_{i=1}^{k} [h_i]$ is a disjoint union. This sub-collection $\mathcal{H}$ is a maximal collection of inequivalent 'necklaces'.

In fact, we can easily show that the set $\mathcal{F}$ is acted upon by the group G 'from the left'. Given any $\phi \in G$, we define the map: $\phi_{\mathcal{F}} : \mathcal{F} \to \mathcal{F}$, as $\phi(h) = \phi \circ h$. Thus, the action of G is by 'left composition'. One can easily see that if $1_X \in G$, is the identity element, then $1_X(h) = 1_X \circ h = h$ for all $h \in \mathcal{F}$. Furthermore, if $\phi, \phi' \in G$, then $\phi(\phi'(h)) = \phi \circ \phi' \circ h = (\phi' \circ \phi) \circ h$, and thus $(\phi\phi')_{\mathcal{F}} = \phi_{\mathcal{F}}\phi'_{\mathcal{F}}$.

Thus, we have a concrete group G acting on a set $\mathcal{F}$. We see that $h \sim h'$ iff h is in the orbit $O(h')$ of h', for the above action. In other words, the determination of the number of inequivalent necklaces, is identical to computing the number of orbits for the action of G on $\mathcal{F}$.

We now have a proposition for arbitrary group actions:



(a) A Colouring (b) Its function.

Figure 5: Colourings and Functions

Proposition 7.1 *Let G be a concrete group acting on a set $\mathcal{F}$. Let $\mathcal{F} = O_1 \cup \ldots \cup O_k$ be the expression of $\mathcal{F}$ as a disjoint union of k orbits. For any element $\phi \in G$, let $Fixed(\phi, \mathcal{F}) = \{h \in \mathcal{F} | \phi \circ h = h\}$, be the elements in $\mathcal{F}$ fixed by $\phi \in G$. Then*

$$k = \frac{1}{|G|} \sum_{\phi \in G} |Fixed(\phi, \mathcal{F})|$$

Proof: Let h be a typical element of $\mathcal{F}$ and let $O(h)$ be the orbit of h under the action of G. It is easy to see that

$$k = \sum_{h \in \mathcal{F}} \frac{1}{|O(h)|}$$

In other words, every element of an orbit O contributes exactly $\frac{1}{|O|}$ to the sum.

We now simplify the right hand side. Since $|G| = |O(h)||Stab(h)|$, we have:

$$
\begin{aligned}
k &= \sum_{h \in \mathcal{F}} \frac{1}{|O(h)|} \\
&= \sum_{h \in \mathcal{F}} \frac{|Stab(h)|}{|G|} \\
&= \frac{1}{|G|} \sum_{h \in \mathcal{F}} \sum_{\phi \in G \ s.t.\ \phi \circ h = h} 1 \\
&= \frac{1}{|G|} \sum_{\phi \in G} \sum_{h \in \mathcal{F} \ s.t.\ \phi \circ h = h} 1 \\
&= \frac{1}{|G|} \sum_{\phi \in G} |Fixed(\phi, \mathcal{F})|
\end{aligned}
$$

This proves the proposition. □

We will now specialize to the case when $\mathcal{F}$ is the collection of all functions $h : X \to \mathcal{C}$, and G acts on X.

Thus let G act on X, and let ϕ be a typical element of G. We will now compute $Fixed(\phi, \mathcal{F})$. In order for $\phi \circ h = h$, we see that if $(x)h = blue$, and $(x)\phi = y$, then $\phi \circ h = h$ implies that $(y)h = (x)\phi \circ h = (x)h = blue$, as well. Recall the equivalence relation $\sim_\phi$ on X (see Section 2.1), and the definition of a ϕ-invariant subset (see Definition 2.3). In this notation, we see that for every colour $c \in \mathcal{C}$, $h^{-1}(c)$ must be a ϕ-invariant subset of X. Now, lemma 2.4 tells us that $h^{-1}(c)$ must be a union of the cycles of ϕ. Thus, functions h such that $\phi \circ h = h$, must colour each cycle of X under ϕ identically. If X splits into k cycles, and $|\mathcal{C}| = r$, then $|Fixed(\phi, \mathcal{F})| = r^k$.

7.3 The 9-necklace.

We will use this fact to compute the number of non-equivalent 2-coloured necklaces with 9-beads. As we know, D_9 has 18 elements. There are 9 'reflections' and 9 rotations. Each reflection is similar to μ, in that, it reflects the necklace about an axis passing through a vertex and the centre. Thus, since $\mu = (1)(29)(38)(47)(56)$, which has 5 cycles, we have $|Fixed(\mu, \mathcal{F})| = 2^5$. On the other hand $\sigma^0 = 1_X$ has 9 cycles. $\sigma^1 = (123456789)$ has 1 cycle. So do $\sigma^2, \sigma^4, \sigma^5, \sigma^7, \sigma^8$. The element $\sigma^3 = (147)(258)(369)$ has 3 cycles, and so does σ^6. We may thus evaluate the sum: $\frac{1}{|G|} \sum_{\phi \in G} |Fixed(\phi, \mathcal{F})|$ as :

$$
\begin{aligned}
k &= \frac{1}{18}(9 \times 2^5 + 1 \times 2^9 + 6 \times 2^1 + 2 \times 2^3) \\
&= \frac{288 + 512 + 12 + 16}{18} = \frac{828}{18} \\
&= \mathbf{46}
\end{aligned}
$$

One may actually check this answer by a routine but tedious enumeration.

7.4 A Refined Inventory

Our next objective is to have a more refined inventory of the in-equivalent necklaces. Towards that, let say $\mathcal{C} = \{black, white, grey\}$, which we shorten to the symbols $\{b, w, g\}$. For a function $h : X \to \mathcal{C}$, we define the monomial $m(h)$ to be $\prod_{x \in X}(x)h$. For example, the monomial of the colouring in Figure 7.1 is $b^2g^2w^5$ indicating that the necklace has 2 black, 2 grey and 5 white beads. Next, for an element $\phi \in G$, we define $m(Fixed(\phi, \mathcal{F}))$ to be $\sum_{h \in Fixed(\phi,\mathcal{F}} m(h)$, i.e., the sum of the monomials of all functions h fixed by ϕ. Note that if $h' = \phi \circ h$, then $m(h) = m(h')$, since the number of beads of a particular colour cant change after a bijection on the beads. Thus, if $\{h_1, \ldots, h_k\}$ is a maximal collection of inequivalent functions, we may define $\mathcal{I}(G, \mathcal{F}))$ as

$$\mathcal{I}(G, \mathcal{F}) = m(h_1) + \ldots + m(h_k)$$

Thus $\mathcal{I}(G, \mathcal{F})$ lists the inequivalent necklaces by their monomials, and thus refines the count.

The next bit of notation: let $\{c_1, c_2, \ldots, c_k, \ldots\}$ be a sequence of variable symbols. For a $\phi \in G$, we now define the symbol $c(\phi, X)$. Recall that, since ϕ is a bijection on X, it splits X into a bunch of cycles, say, n_1 cycles of length 1, n_2 cycles of length 2, and so on. We define $c(\phi, X)$ as $\prod_k c_k^{n_k}$. The **cycle polynomial** $Z(G, X)(c_1, c_2, \ldots)$ of the action of G on X is:

$$\frac{1}{|G|} \sum_{\phi \in G} c(\phi, X)$$

As an example, $c(\sigma, X) = c_9$, while $c(\mu, X) = c_1c_2^4$. Further:

$$Z(D_9, X) = \frac{9c_1c_4 + c_1^9 + 2c_3^3 + 6c_9}{18}$$

Finally, let $s_1 = b + g + w$, and $s_2 = b^2 + g^2 + w^2$, and so on with $s_i = b^i + g^i + w^i$. For an element $\phi in G$, we denote by $s(\phi)$ as the polynomial in the variables $\{b, g, w\}$ obtained by substituting s_i in place of c_i for every i, in the polynomial $c(\phi)$. Thus $s(\sigma) = (b^9+g^9+w^9)$ and $s(\mu) = (b+g+w)(b^2+g^2+w^2)^4$.

The first lemma:

Lemma 7.2 *The polynomial $m(Fixed(\phi, \mathcal{F}))$ equals $s(\phi)$.*

Proof: Let $Y_1Y_2 \subseteq X$ be ϕ-invariant subsets such that $X = Y_1 \cup Y_2$, while $Y_1 \cap Y_2$ is empty. Let $\mathcal{F}_i$ be the collection of all functions $h_i : Y_i \to \mathcal{C}$. Since each Y_i is an invariant subset, we easily see that ϕ restricted to Y_i yields us a bijection ϕ_i. It is then easily seen that $s(\phi) = s(\phi_1)s(\phi_2)$. We now claim that

$$m(Fixed(\phi, \mathcal{F})) \quad = \quad m(Fixed(\phi_1, \mathcal{F}_1))m(Fixed(\phi_2, \mathcal{F}_2)) \qquad (1)$$

To see this, note that if $h \in Fixed(\phi, \mathcal{F})$, then the restriction of h to Y_i gives us functions h_i which are in $Fixed(\phi_i, \mathcal{F}_i)$. Conversely, given a pair of functions h_1, h_2 with $h_i \in Fixed(\phi_i, \mathcal{F}_i)$, we get the function $h : X \to \mathcal{C}$ by 'merging' the domains of h_1, h_2. This function h is fixed by ϕ. Thus there is a bijection:

$$\eta : Fixed(\phi, \mathcal{F}) \to Fixed(\phi_1, \mathcal{F}_1) \times Fixed(\phi_2, \mathcal{F}_2)$$

This implies the earlier result (1) above.

Thus, since both sides of the main assertion are multiplicative, it suffices to prove the lemma when X cannot be decomposed into two invariant subsets. This is only possible when ϕ acts on X cyclically. Thus if $|X| = r$, then $s(\phi) = b^r + g^r + w^r$. On the other hand, the only invariant functions on X are the constant functions h_b, h_g and h_w, where, for example, $h_b(x) = b$ for all $x \in X$. Thus $m(Fixed(\phi, \mathcal{F})) = b^r + g^r + w^r$. This proves the lemma. □

Our final result is what is tradionally called the **Polya Theorem**.

Theorem 7.3 *The inventory polynomial $\mathcal{I}(G, \mathcal{F})$ equals the substitution of $c_i = s_i$ in the cycle polynomial $Z(G, X)$. In other words:*

$$\mathcal{I}(G, \mathcal{F}) = Z(G, X)(s_1, s_2, \dots)$$

Proof: The proof of this theorem follows easily from that of Proposition 7.1, and the above lemma. To be precise, we see that:

$$\begin{aligned}
\mathcal{I}(G, \mathcal{F}) &= \sum_{h \in \mathcal{F}} \frac{1}{|O(h)|} m(h) \\
&= \sum_{h \in \mathcal{F}} \frac{|Stab(h)|}{|G|} m(h) \\
&= \frac{1}{|G|} \sum_{h \in \mathcal{F}} \sum_{\phi \in G\ s.t.\ \phi \circ h = h} m(h) \\
&= \frac{1}{|G|} \sum_{\phi \in G} \sum_{h \in \mathcal{F}\ s.t.\ \phi \circ h = h} m(h) \\
&= \frac{1}{|G|} \sum_{\phi \in G} m(Fixed(\phi, \mathcal{F})) \\
&= \frac{1}{|G|} \sum_{\phi \in G} s(\phi) \qquad \text{(By lemma 7.2)} \\
&= Z(G, X)(s_1, s_2, \dots)
\end{aligned}$$

This proves the theorem. □

8 Homomorphisms

In this section, we develop the notion of homomorphisms, which are maps which 'preserve' the group structure. After a few basic results, we see two important example homomorphisms, viz., the *sign* and the *det*.

8.1 Kernels and Images

Let G and H be groups. A function $f : G \to H$ is called a homomorphism if for every $g, g' \in G$, we have (i) $f(gg') = f(g)f(g')$, and (ii) $f(e_G) = e_H$, i.e., the identity element e_G is mapped to the identity element e_H of H. Note that, in (i) above, on the left, the multiplication gg' happens in the group G, while on the right, the multiplication $f(g)f(g')$ happens in H. Thus, f must be concommitant with the multiplications of both the groups.

Example 8.1 *1. Let $(\mathbb{Z}, +)$ and $(\mathbb{R}, +)$ be the additive groups of integers and reals, respectively. Let $\phi_1 : \mathbb{Z} \to \mathbb{R}$ be the natural inclusion. Then ϕ_1 is a homomorphism. Clearly $0_{\mathbb{Z}} = 0_{\mathbb{R}}$ and thus the identity elements match. Also, for integers m, n, whether the addition happens in $\mathbb{Z}$ or in $\mathbb{R}$ is immaterial to the result.*

2. *Let $G = (\mathbb{Z}, +)$ be the group of integers, and $H = (\mathbb{Z}_n, +)$ be the group of integers modulo n. The map $\phi_2 : \mathbb{Z} \to \mathbb{Z}_n$ is defined as $\phi_2(m) = m \, modulo \, n$. It is easily verified that this is a group homomorphism.*

3. *Let $G = D_4 = \{\mu^i \sigma^j | 0 \le i \le 1, 0 \le j \le 3\}$, and $H = \{+1, -1\}$ under multiplication. Let $\phi_3 : D_4 \to H$ be given by $\phi_3(\mu^i \sigma^j) = (-1)^i$. Clearly, the identity element of D_4 is $\mu^0 \sigma^0$, and thus $\phi_3(1_{D_4}) = 1$. For the other condition, note that $\mu^{i_1}\sigma^{j_1} \cdot \mu^{i_2}\sigma^{j_2} = \mu^{i_1+i_2}\sigma^j$ for some j.*

4. *Let $G = GL_n(\mathbb{R})$ be the group of invertible $n \times n$ real matrices under matrix multiplication. Let $H = (\mathbb{R}^*, \cdot)$ be the group of non-zero reals under multiplication. Let $det : GL_n(\mathbb{R}) \to \mathbb{R}^*$ be defined as $A \to det(A)$, the determinant of A. Note that the identity matrix has determinant 1, and that (which we will prove later) $det(AB) = det(A)det(B)$.*

Definition 8.2 *For a homomorphism $\phi : G \to H$, the* **kernel** *of ϕ is the set $ker(\phi) = \{g \in G | \phi(g) = e_H\}$, and the* **image** *of ϕ is $Im(\phi) = \{h \in H | \exists g \in G \; s.t. \; \phi(g) = h\}$.*

Thus the kernel of ϕ are those elements of G which go to the identity element of H, and the image of ϕ is the usual image of ϕ as a function.

Lemma 8.3 *The image of ϕ is a subgroup of H. The kernel $K = ker(\phi)$ is a subgroup of G.*

Proof: Clearly $e_H \in Im(\phi)$. Next, if $h, h' \in Im(\phi)$, then there are $g, g' \in G$ such that $\phi(g) = h$ and $\phi(g') = h'$. Whence $hh' = \phi(g)\phi(g') = \phi(gg')$ lies in the image of ϕ. Finally, if $\phi(g) = h \in Im(\phi)$ then

$$e_H = \phi(e_G) = \phi(gg^{-1}) = \phi(g^{-1})\phi(g) = \phi(g^{-1})h$$

Thus the inverse of h is precisely $\phi(g^{-1})$ and thus lies in $Im(\phi)$.

For the second part, note that if $g, g' \in K$, then $\phi(gg') = \phi(g)\phi(g') = e_H \cdot e_H = e_H$, and thus $gg' \in K$. The existence of inverses within K is starightforward. □

The kernels of homomorphisms are rather special subgroups of a group. We recall Example 8.1 above, and note that in (1) above, the kernel $ker(\phi_1)$ was trivial (i.e., just the identity element), while $ker(\phi_2) = n\mathbb{Z} = \{ni | i \in \mathbb{Z}\}$. The kernel of ϕ_3 were all rotations, which we easily see, is a subgroup. The kernel of the determinant are all matrices of determinant 1.

Recall that with every subgroup $K \subseteq G$, we have two equivalence relations L_K and R_K on G. The relation L_K is defined as gL_Kg' iff there is a $k \in K$ such that $g = kg'$. The relation is R_K is similarly defined: gR_Kg' iff there is a $k \in K$ such that $g = g'k$.

Definition 8.4 *A subgroup $K \subseteq G$ is called a* **normal subgroup** *if $gkg^{-1} \in K$ for all $k \in K$ and $g \in G$.*

Proposition 8.5 *(i) If K is a normal subgroup of G, then R_K and L_K coincide.*
(ii) If $\phi : G \to H$ is a homomorphism, and $K = ker(\phi)$, then K is normal.

Proof: Let gR_Kg', or in other words, let $g = g'k$. Post-multiplying both sides by $(g')^{-1}$, we see that $g(g')^{-1} = g'k(g')^{-1}$. By the normality of K, we see that $g(g')^{-1} = k'$ for some $k' \in K$, whence $g = k'g'$. Thus gL_Kg'. The other direction is similarly proved.

For the second part, note that if $g \in G$ and $k \in ker(\phi)$, then $\phi(gkg^{-1} = \phi(g)e_H\phi(g^{-1}) = \phi(gg^{-1}) = e_H$. Thus $gkg^{-1} \in ker(\phi)$ for all $g \in G$ and $k \in ker(\phi)$. □

The following two propositions explain the centrality of normal subgroups and homomorphisms.

Proposition 8.6 *(i) Let $\phi : G \to H$ be a homomorphism, and K be the kernel. Then, if $\phi(g) = h$, then $\phi^{-1}(h) = Kg = gK$.*
(ii) If G is finite and ϕ is surjective, then $|G| = |K||H|$.

Proof: First note that since K is normal, left cosets equal right cosets, i.e., $gK = Kg$. Next, examine the element gk, with $k \in K$. We see that $\phi(gk) = \phi(g)\phi(k) = \phi(g)e_H = \phi(g)$, and thus $gK \subseteq \phi^{-1}(h)$. Next, if $\phi(g') = \phi(g) = h$, then $\phi(g'g^{-1}) = \phi(g')\phi(g^{-1}) = hh^{-1} = e_H$, and thus $g'g^{-1} = k$ for some k in the kernel. Thus $g' \in Kg$. This proves that $Kg \subseteq \phi^{-1}(h)$.

For the second part, note that for every $h \in H$, there is a g such that $\phi(g) = h$. Thus, every inverse image exist for every $h \in H$, and by part (i), $\phi^{-1}(h)$ is a coset of K. Since for every coset gK, we have $|gK| = |K|$, we see that every inverse image has the same cardinality, viz., $|K|$. The result follows. □

Let $K \subseteq G$ be a normal subgroup, and denote by $G/K = \{g_\alpha K\}_{\alpha \in I}$ to be the collection of cosets of K in G. We define a 'multiplication' structure on G/L. Given two cosets $g_\alpha K$ and $g_\beta K$, we define $g_\alpha K \circ g_\beta K$ to be $g_\alpha g_\beta K$. Thus, the multiplication is defined by taking two coset representatives g_α and

g_β, multiplying them in G to get $g_\alpha g_\beta$, and then taking the coset of this element. Next, we define the 'identity' in G/K to be the coset $e_G K = K$.

Proposition 8.7 *If K is a normal subgroup of G, then $\circ$ is well-defined and the structure $(G/L.\circ)$ is a group.*

Proof: Proving the well-defined-ness of $\circ$ is equivalent to showing that the multiplication defined on the cosets does not depend on the choice of the coset representatives. In other words, if $g_1 R_K g_1'$ and $g_2 R_K g_2'$, then we have $g_1 g_2 R_K g_1' g_2'$. To see this, let $g_1 = g_1' k_1$ and $g_2 = g_2' k_2$. Then $g_1 g_2 = g_1' k_1 g_2' k_2$. But by the normality of K, we have $k_1 g_2' = g_2' k'$ for some $k' \in K$. Thus $g_1 g_2 = g_1' g_2' k' k_2$, and thus $g_1 g_2 R_K g_1' g_2'$.

It is now easy to show that $\circ$ is associative which directly follows from the associativity of the multiplication in G. The identity coset K has e_G as a representative. Thus $e_G \circ KgK = e_G gK = gK$ and thus K is indeed the identity for $\circ$. The inverse of gK is clearly $g^{-1}K$, the coset containg the inverse of any coset representative of gK. This proves the second part. □

Finally, we have the so-called **first isomorphism theorem**:

Theorem 8.8 *Let $\phi : G \to H$ be a surjective homomorphism with kernel K. Then, as groups, $(G/K, circ)$ and H are isomorphic.*

Proof: We construct the isomorphism $\overline{\phi} : G/K \to H$ as $\overline{\phi}(gK) = \phi(g)$. It is easy to verify that this is indeed a group isomorphism. □

9 The Sign and the Determinant

In this section, we construct two important homomorphisms $sign : Bij(X) \to \{+1, -1\}$ and the determinant $det : GL_n(\mathbb{R}) \to \mathbb{R}^*$. Both these are fundamental in the theory of groups.

9.1 The Sign

Let X be a set of cardinality n, for simplicity, let $X = \{1, 2, \ldots, n\}$. Let $S_n = Bij(X)$ be the group of all bijections on X, under compositions. Let $H = \{+1, -1\}$ be the multiplicative group with two elements. We will devise a homomorphism $sign : S_n \to H$.

We first observe a simple lemma: for any non-zero real number r, let $sign(r)$ be -1 if the number is negative, and $+1$ otherwise. We see easily that $sign : \mathbb{R}^* \to H$ is actually a homomorphism. Thus, for non-zero reals $r_1 r_2$, we have $sign(r_1 r_2) = sign(r_1) sign(r_2)$.

A central concept in the definition of the homomorphism is that of **inversion**. For a permutation $\mu : X \to X$, we say that $\{i, j\}$ is an **inversion** if $((i)\mu - (j)\mu)(i - j)$ is negative. In other words $\{i, j\}$ is an inversion, when $i < j$ but $(i)\mu > (j)\mu$, or vice-versa. Thus μ inverts the order of i and j. A pictorial

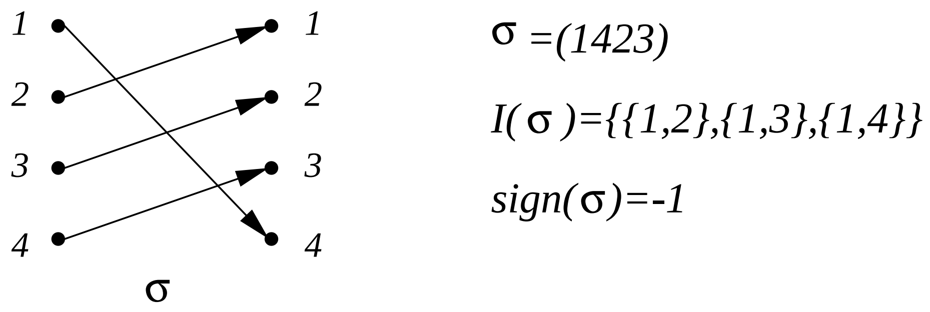


Figure 6: Inversions

way of observing an inversion is to 'draw' the diagram of μ, and see that the arrows coming out of i and j cross each other. See figure 9.1 below.

Let $\binom{X}{2}$ stand for all 2-subsets of X, and thus a ground set for possible inversions. For a permutation μ, we define:

$$I(\mu) = \{\{i,j\} \in \binom{X}{2} | \{i,j\} \text{ is an inversion for } \mu\}$$

Thus $I(\mu) \subseteq \binom{X}{2}$ is the collection of all inversions for the permutation μ. Clearly, the identity permutation 1_X has no inversions, while the 'opposite' permutation η defined as $(i)\eta = n - i$ has $I(\eta) = \binom{X}{2}$. Let $i(\mu)$ denote the number $|I(\mu)|$. We are now ready to define the sign:

$$sign(\mu) = (-1)^{i(\mu)}$$

The the sign of a permutation is -1 if it has odd number of inversions, and is $+1$ otherwise. The sign of 1_X is $(-1)^0 = +1$, while the sign of σ of figure 9.1 is -1.

Note that, when μ is a permutation, $((i)\mu - (j)\mu)(i-j)$ is a non-zero number. The sign of a permutation may then be also defined as follows:

Lemma 9.1 *For a permutation μ, we have:*

$$sign(\mu) = \prod_{\{i,j\} \in \binom{X}{2}} sign(((i)\mu - (j)\mu)(i-j))$$

The proof is straight-forward. The main theorem of this section is:

Theorem 9.2 *If α and β are two permutations, then $sign(\alpha \circ \beta) = sign(\alpha) sign(\beta)$. Thus $sign : S_n \to H$ is a group homomorphism.*

Proof: Let us construct two row vectors (of length $N = \binom{n}{2}$) R_1 and R_2 wherein we list all the elements of $\binom{X}{2}$ in a particular order. The row R_1 lists the elements of $\binom{X}{2}$ in an arbitrary order, for convenience, say in the 'natural order', i.e., $\{1,2\},\{1,3\},\ldots,\{1,n\},\{2,3\},\{2,4\},\ldots,\{n-1,n\}$. In the row R_2, the k-th element of R_2 follows from the k-th element of R_1 as follows: if $R_1[k]=\{i,j\}$, then $R_2[k]=\{(i)\alpha,(j)\alpha\}$. Thus the k-th entry of R_2 is obtained by applying α to the k-th entry of R_1. Note that since α is a permutation, R_2 has no duplications, and each 2-subset appears somewhere in R_2.

Next, we say that $sign(R_1[k])$ is -1 if $R_1[k]$ is a inversion for α. Otherwise, we say that $sign(R_1[k])$ is $+1$. Similarly, $sign(R_2[k])$ depends on whether $R_2[k]$ is an inversion for β. Note that

$$sign(\alpha)=\prod_{k=1}^{N} sign(R_1[k]) \quad sign(\beta)=\prod_{k=1}^{N} sign(R_2[k])$$

Now, let us examine when $\{i,j\}$ is an inversion for $\alpha\circ\beta$. In other words, we analyse the sign of $((i)\alpha\circ\beta-(j)\alpha\circ\beta)(i-j)$. Multiplying this by $((i)\alpha-(j)\alpha)^2$, which is a positive number, we see that:

$$\begin{array}{l} sign((i)\alpha\circ\beta-(j)\alpha\circ\beta)(i-j)= \\ sign((i)\alpha-(j)\alpha)(i-j)sign((i)\alpha\circ\beta-(j)\alpha\circ\beta)((i)\alpha-(j)\alpha) \end{array}$$

In other words, if $R_1[k]=\{i,j\}$, then

$$sign((i)\alpha\circ\beta-(j)\alpha\circ\beta)(i-j)=sign(R_1[k])sign(R_2[k])$$

Now applying lemma 9.1, we see that:

$$\begin{array}{rcl} sign(\alpha\circ\beta) & = & \prod_{\{i,j\}} sign((i)\alpha\circ\beta-(j)\alpha\circ\beta)(i-j) \\ & = & \prod_{k=1}^{N} sign(R_1[k])sign(R_2[k]) \\ & = & \prod_{k=1}^{N} sign(R_1[k])\prod_{k=1}^{N} sign(R_2[k]) \\ & = & sign(\alpha)sign(\beta) \end{array}$$

This proves the theorem. □

There is yet another way of defining the sign of a permutation, which is based on the number of 'flips' needed to 'sort' the permutation. We say that a permutation is a **transposition** if in cycle notation, it is of the form (r,s). In other words, a transposition τ fixes all elements except two elements r,s, which it flips. We have a small lemma which essentially says that an array can be sorted.

Lemma 9.3 *Every permutation μ may be expressed as a composition $\tau_1\circ\tau_2\circ\ldots\circ\tau_k$.*

Proof: We prove this by induction on $|X|$. Given a permutation μ, let $(n)\mu=k$. If $k=n$, then μ is effectively a bijection on $\{1,2,\ldots,n-1\}$ and thus is expressible as a product of transpositions. If $n\neq k$, then let $\tau=(n.k)$, and examine $\sigma=\mu\circ\tau$. We see that $(n)\sigma=(n)\mu\circ\tau=(k)\tau=n$, and thus σ fixes n. Thus σ is effectively a bijection on $\{1,2,\ldots,n-1\}$ and therefore a product a transpositions, say:

$$\mu\circ\tau=\sigma=\tau_1\ldots\tau_{k-1}$$

Observing that $\tau^{-1}=\tau$, we see that $\mu=\tau_1\ldots\tau_{k-1}\tau$. □

Lemma 9.4 *If the permutation $\mu = \prod_{i=1}^{k} \tau_i$ be expressible as a product of k transpositions, then $sign(\mu) = (-1)^k$.*

The proof just follows from the observation that $sign(\tau) = -1$ for every transposition.

9.2 The Determinant

In this section, we will develop the determinant as first, a multi-linear map, and then as a group homomorphism.

Let us first begin with matrices. For a fixed n, let $M_n(\mathbb{R})$ refer to $n \times n$-matrices with real entries. For a matrix $X = (x_{ij}) \in M_n(\mathbb{R})$, we define:

$$det(X) = \sum_{\sigma \in S_n} sign(\sigma) \prod_{i=1}^{n} x_{i,(i)\sigma}$$

Thus $det(X)$ is a signed sum of $n!$ monomials, each of degree n, such that each monomial contains exactly one entry from each row and column. For $n = 3$, this expression equals:

$$det(X) =$$
$$x_{11}x_{22}x_{33} - x_{11}x_{23}x_{32} + x_{12}x_{23}x_{31} - x_{12}x_{21}x_{33} + x_{13}x_{21}x_{32} - x_{13}x_{22}x_{31}$$

Noting that $sign(\sigma) = sign(\sigma^{-1})$, and that $(i)\sigma = j$ is the same as saying $(j)\sigma^{-1} = i$, we have:

$$\begin{aligned} det(X) &= \textstyle\sum_{\sigma \in S_n} sign(\sigma^{-1}) \prod_{j=1}^{n} x_{(j)\sigma^{-1},j} \\ &= \textstyle\sum_{\mu \in S_n} sign(\mu) \prod_{j=1}^{n} x_{(j)\mu,j} \end{aligned}$$

Thus, the expression of the determinant by 'rows' equals that by 'columns', and we have $det(X) = det(X^T)$, i.e., the determinant of the transpose of a matrix equals that of the original.

From the definition of the determinant, we easily see that $det(I) = 1$, where I is the identity matrix. Also, for any permutation $\sigma \in S_n$, we may define a matrix P_σ, where $P_\sigma(i,j) = 1$ iff $(i)\sigma = j$, and is zero otherwise. Again, the definition of the determinant tells us that $det(P_\sigma) = sign(\sigma)$. Further note that $P_\sigma P_\mu = P_{\sigma\mu}$, whence we have:

$$det(P_\sigma P_\mu) = det(P_{\sigma\mu}) = sign(\sigma\mu) = sign(\sigma)sign(\mu) = det(P_\sigma)det(P_\mu)$$

One simple observation is that the determinant may be 'expanded' by the first row, or for that matter, any row or column. Thus for example, we have:

$$det(X) = \sum_{i=1}^{n} x_{1,i} \left(\sum_{\sigma \in S_N \ s.t. \ (1)\sigma = i} sign(\sigma) \prod_{k=2}^{n} x_{k,(k)\sigma} \right)$$

Thus, in effect, we have $det(X) = x_{11}M_{11} + x_{12}M_{12} + \ldots + x_{1n}M_{1n}$, where each M_{1i} does not involve any variable from the first row.

Here is another useful lemma, which we will need later. Let τ be a transposition, say (r, s), and let us examine the matrix product $Y = P_\tau X$. Note that Y is obtained from X by intercahnging the rows r and s of X. The lemma:

Lemma 9.5 *For τ as above, we have:*

$$det(P_\tau X) = det(P_\tau) det(X) = -det(X)$$

Proof: Let $Y = P_\tau X$ as before. Note that $(i)\tau = i$ unless $i = r$ or $i = s$, in which case, τ transposes them. Thus $Y_{i,(i)\sigma} = X_{(i)\tau,(i)\sigma}$. Thus

$$\prod_{i=1}^{n} Y_{i,(i)\sigma} = \prod_{i=1}^{n} X_{(i)\tau,(i)\sigma} = \prod_{k=1}^{n} X_{k,(k)\tau^{-1}\sigma} = \prod_{k=1}^{n} X_{k,(k)\tau\sigma}$$

The last equality followed from the fact that $\tau^{-1} = \tau$. Further, note that as σ ranges over S_n, so will $\tau\sigma$. Thus, we have:

$$\begin{array}{ll} det(Y) & = \sum_{\sigma \in S_n} sign(\sigma) \prod_{i=1}^{n} y_{i,(i)\sigma} \\ & = \sum_{\sigma \in S_n} sign(\sigma) \prod_{i=1}^{n} x_{i,(i)\tau\sigma} \\ & = sign(\tau) \sum_{\sigma \in S_n} sign(\tau\sigma) \prod_{i=1}^{n} x_{i,(i)\tau\sigma} \\ & = sign(\tau) \sum_{\sigma \in S_n} sign(\tau\sigma) \prod_{i=1}^{n} x_{i,(i)\tau\sigma} \\ & = sign(\tau) \sum_{\tau\sigma \in S_n} sign(\tau\sigma) \prod_{i=1}^{n} x_{i,(i)\tau\sigma} \\ & = -det(X) \end{array}$$

This completes the proof. $\square$

Our next objective will be to show that $det(AB) = det(A)det(B)$ for general matrices. The route to this fact will require us to uncover some more fundamental properties of the determinant. For this, we will consider the determinant as a function of n row vectors, each of size n.

More generally, let $g : \mathbb{R}^n \times \ldots \times \mathbb{R}^n \to \mathbb{R}$, be a function from n copies of $\mathbb{R}^n$ to $\mathbb{R}$.

We say that g is **multi-linear** if

(L1) $g(r_1, \ldots, r_{i-1}, r_i + s_i, r_{i+1}, \ldots, r_n) =$

$g(r_1, \ldots, r_{i-1}, r_i, r_{i+1}, \ldots, r_n) + g(r_1, \ldots, r_{i-1}, s_i, r_{i+1}, \ldots, r_n)$,

where $r_1, \ldots, r_n$ and s_i are any elements of $\mathbb{R}^n$ (i.e., are row vectors of size n).

(L2) $g(r_1, \ldots, r_{i-1}, \alpha r_i, r_{i+1}, \ldots, r_n) = \alpha g(r_1, \ldots, r_{i-1}, r_i, r_{i+1}, \ldots, r_n)$,

again for arbitrary elements of $\mathbb{R}^n$, and for arbitrary $\alpha \in \mathbb{R}$.

Thus, the multi-linearity of g merely asserts that g is linear in each argument.

Next, we say that g is **alternating** if

(A1) $g(r_1, \ldots, r_{i-1}, r_i, r_{i+1}, \ldots, r_{j-1}, r_j, r_{j+1}, \ldots, r_n) =$

$-g(r_1, \ldots, r_{i-1}, r_j, r_{i+1}, \ldots, r_{j-1}, r_i, r_{j+1}, \ldots, r_n)$.

Thus, whenever two arguments of g are interchanged, the function g changes sign.

Some immediate properties of multi-linear and alternating functions:

Proposition 9.6 *Let $g : \mathbb{R}^n \times \ldots \times \mathbb{R}^n \to \mathbb{R}$ be multi-linear and alternating, then:*
(i) $g(r_1, \ldots, r_{i-1}, r_i, r_{i+1}, \ldots, r_{j-1}, r_i, r_{j+1}, \ldots, r_n) = 0$
(ii) $g(r_1, \ldots, r_{i-1}, r_i + \alpha r_j, r_{i+1}, \ldots, r_{j-1}, r_j, r_{j+1}, \ldots, r_n) =$
$g(r_1, \ldots, r_{i-1}, r_i, r_{i+1}, \ldots, r_{j-1}, r_j, r_{j+1}, \ldots, r_n)$.
(iii) Let g_1 and g_2 be multi-linear and alternating. We define $g_1 + g_2$ as

$$(g_1 + g_2)(r_1, \ldots, r_n) = g_1(r_1, \ldots, r_n) + g_2(r_1, \ldots, r_n)$$

Then $g_1 + g_2$ is also multilinear and alternating. In other words, (i) g vanishes if any two arguments of g are equal, (ii) g is invariant under the addition of a multiple of one row to another, and (iii) a linear combination of two multi-linear and alternating forms has the same property.

Proof: By applying (**A1**) to $g(r_1, \ldots, r_{i-1}, r_i, r_{i+1}, \ldots, r_{j-1}, r_i, r_{j+1}, \ldots, r_n)$, we see that
$g(r_1, \ldots, r_{i-1}, r_i, r_{i+1}, \ldots, r_{j-1}, r_i, r_{j+1}, \ldots, r_n) =$
$-g(r_1, \ldots, r_{i-1}, r_i, r_{i+1}, \ldots, r_{j-1}, r_i, r_{j+1}, \ldots, r_n)$.
Thus the number equals its negative, whence it must be zero.

To prove (ii), we use (**L1**) and (**L2**) to get:
$g(r_1, \ldots, r_{i-1}, r_i + \alpha r_j, r_{i+1}, \ldots, r_{j-1}, r_j, r_{j+1}, \ldots, r_n) =$
$g(r_1, \ldots, r_{i-1}, r_i, r_{i+1}, \ldots, r_{j-1}, r_j, r_{j+1}, \ldots, r_n) +$
$\alpha g(r_1, \ldots, r_{i-1}, r_j, r_{i+1}, \ldots, r_{j-1}, r_j, r_{j+1}, \ldots, r_n)$
Since the second term equals zero, we have the required result.

Part (iii) is easy and left to the reader. This proves the proposition. $\Box$

An important corollary:

Corollary 9.7 *If g is multi-linear and alternating such that $g(r_1, \ldots, r_n) \neq 0$, then (i) $r_1, \ldots, r_n$ are linearly independent, (ii) $g(r_{(1)\sigma}, r_{(2)\sigma}, \ldots, r_{(n)\sigma}) \neq 0$ where σ is any permutation on the set $\{1, 2, \ldots, n\}$.*

Proof: Suppose, say $r_1 = \sum_{i=2}^n \alpha_i r_i$, then we have

$$g(r_1, r_2, \ldots, r_n) = \sum_{i=2}^{n} \alpha_i g(r_i, r_2, \ldots, r_n)$$

Since each summand on the right has a repeated argument, we see that the RHS reduces to zero. This contradicts the hypothesis that $g(r_1, r_2, \ldots, r_n) \neq 0$. As regards part (ii), we know that σ may be expressed as the product of transpositions. Applying these transpositions one after another, we see that $g(r_{(1)\sigma}, r_{(2)\sigma}, \ldots, r_{(n)\sigma}) = sign(\sigma) g(r_1, \ldots, r_n) \neq 0$. $\Box$

Our next step is to convert the determinant into a multi-linear form: Firstly, given n row vectors $r_1, \ldots, r_n$, let $matrix(r_1, \ldots, r_n)$ denote the $n \times n$-matrix with rows $r_1, \ldots, r_n$, in that order. Next, we define $mdet : \mathbb{R}^n \times \ldots \times \mathbb{R}^n \to \mathbb{R}$, as $mdet(r_1, \ldots, r_n) = det(matrix(r_1, \ldots, r_n))$. Thus, $mdet$ takes in n rows, forms a matrix and evaluates the determinant.

Lemma 9.8 *The form $mdet : \mathbb{R}^n \times \ldots \times \mathbb{R}^n \to \mathbb{R}$ is multi-linear and alternating. Furthermore, if e_i is the i-th unit row vector (i.e., it is 1 in the i-th place, and zero everywhere else), then $mdet(e_1, e_2, \ldots, e_n) = 1$.*

Proof: We will prove linearity in the first arguments, the others being similar. Recall that $det(X) = \sum_i x_{1i}M_{1i}$, where M_{1i} does not involve anything from the first row. So assuming the other rows as fixed, we see that $mdet$ is a linear form in the entries of the first row. This proves its linearity in the first argument. That $mdet$ is alternating follows easily from lemma 9.5. Next, $det(I) = 1$ proves the remaining assertion. □

We see that Proposition 9.6 already proves some important and well-known properties of the determinant. We now show that, multi-linearity and alternation in fact, **define** the determinant.

Theorem 9.9 *Let f be multi-linear and alternating such that $f(e_1, \ldots, e_n) = \alpha$. Then $f(r_1, \ldots, r_n) = \alpha \cdot mdet(r_1, \ldots, r_n)$ for all $r_1, \ldots, r_n \in \mathbb{R}^n$. In other words, the determinant and its multiples are the unique multi-linear and alternating forms.*

Proof: Consider the form $g = f - \alpha mdet$, which is also multi-linear and alternating (prop. 9.6). Further, it also has the property that $g(e_1, \ldots, e_n) = 0$. We show that, in fact, $g(r_1, \ldots, r_n) = 0$ for any choice of the arguments.

Suppose that were not, then we can choose some rows $s_1, \ldots, s_n$ such that $g(s_1, \ldots, s_n) \neq 0$. We call such an ordered collection $(s_1, \ldots, s_n)$ a **witness** to the fact that g is not identically zero. Clearly then, by the corollary 9.7, we have that $s_1, \ldots, s_n$ are linearly independent. Thus, by re-ordering the arguments, we can construct another witness (again, corollary 9.7) such that the first entry of the first vector, viz., $s_1[1] \neq 0$ (if it were that $s_i[1] = 0$ for all i, then the set would be linearly dependent). Now we use Proposition 9.6 (ii). By choosing, $s_i - \alpha_i s_1$, instead of s_i for $i = 2, \ldots, n$, we may further assume that there is a witness $(s_1, \ldots, s_n)$ such that $s_1[1] \neq 0$, and $s_i[1] = 0$ for all $i > 1$. Going on like this, we may actually assume that $(s_1, \ldots, s_n)$ is a witness such that $s_i[i] \neq 0$, and $s_i[j] = 0$ whenever $j < i$. The reader may notice that is the 'forward' step in the 'Gauss Elimination' on the witnessing rows.

We now do the 'backward' elimination: Starting with s_n, we see that $s_n[n] \neq 0$, and thus, we may eliminate the last entry from $s_1, \ldots, s_{n-1}$. Carrying on thus, we may assume that $(s_1, \ldots, s_n)$ is such that $s_i[i] = \beta_i \neq 0$, and $s_i[j] = 0$ whenever $j \neq i$. Thus we have:

$$g(\beta_1 e_1, \ldots, \beta_n e_n) = (\prod_{i=1}^{n} \beta_i) g(e_1, \ldots, e_n 0) \neq 0$$

This contradicts the construction that $g(e_1, \ldots, e_n) = 0$. □

We now present the final result that the determinant is actually a homomorphism from $GL_n(\mathbb{R})$ to $\mathbb{R}^*$.

Corollary 9.10 *For $n \times n$ matrices A, B we have $det(AB) = det(A)det(B)$.*

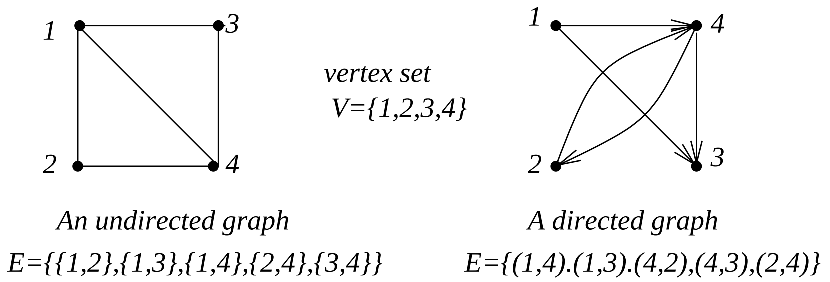


Figure 7: Two Graphs

Proof: Let us fix A and let B have *variable* rows $(r_1, \ldots, r_n)$. Define the form f as

$$f(r_1, \ldots, r_n) = mdet(Ar_1, \ldots, Ar_n)$$

Note that if r_i is a row vector, then so is Ar_i. Since $A(r_i + s_i) = Ar_i + As_i$, and $\alpha(Ar_i) = A(\alpha r_i)$ for any $\alpha \in \mathbb{R}$, we see easily that f is multi-linear. Considering alternation, we see that:

$$\begin{aligned} f(r_2, r_1, r_3, r_4, \ldots, r_n) &= mdet(Ar_2, Ar_1, Ar_3, Ar_4, \ldots, Ar_n) \\ &= -mdet(Ar_1, Ar_2, Ar_3, Ar_4, \ldots, Ar_n) \\ &= -f(r_1, r_2, r_3, r_4, \ldots, r_n) \end{aligned}$$

Thus f is indeed alternating. Thus, by the theorem above, we have

$$det(AB) = f(r_1, \ldots, r_n) = f(e_1, \ldots, e_n) \cdot mdet(r_1, \ldots, r_n) = det(A)det(B)$$

This proves the corollary. $\Box$

10 Graphs

In this section, we begin with a new combinatorial structure, viz., graphs. These structures useful in defining various entities and their dependencies.

Definition 10.1 1. *An* **undirected** *graph $G(V, E)$ is given by the data V, which is a finite set of* **vertices**, *and $E \subset \binom{V}{2}$, a collection of 2-subsets of V, called* **edges**.

2. *A* **directed** *graph $G(V, E)$ is given by the data V, which is a finite set of* **vertices**, *and $E \subset V \times V$, a collection of 2-tuples of V, called* **edges**.

A graph is frequently represented as a picture. See figure 10.

For a large part of our analysis, we shall only be considering undirected graphs. Henceforth, unless specified, we shall look at only undirected graphs. However, for convenience of notation, (i, j) will also refer to $\{i, j\}$. Thus (i, j) is an edge in an undirected graph will mean that in fact $\{i, j\} \in E$.

Definition 10.2 *1. A* **trail** *in a graph $G(V, E)$ is a sequence of vertices $(v_1, \ldots, v_k)$ such that $(v_i, v_{i+1}) \in E$ for $i = 1, \ldots, k-1$. The number $k-1$ is called the* **length** *of the trail.*

2. A **path** *in a graph $G(V, E)$ is a sequence of vertices $(v_1, \ldots, v_k)$ such that it is (i) a trail, and (ii) the vertices $v_1, \ldots, v_k$ are all distinct.*

3. A **loop** *in a graph $G(V, E)$ is a sequence of vertices $(v_1, \ldots, v_k, v_1)$ such that (i) $(v_i, v_{i+1}) \in E$ for $i = 1, \ldots, k-1$, and (ii) $(v_k, v_1) \in E$ as well. The number k is called the* **length** *of the loop.*

4. A **cycle** *in a graph $G(V, E)$ is a sequence of vertices $(v_1, \ldots, v_k, v_1)$ such that (i) it is a loop, and (ii) $v_1, \ldots, v_k$ are all distinct.*

10.1 Connectedness

For two vertices $i, j \in V$, we define the relation $i \sim j$ (and say that i is **connected** to j), if there is a path $\pi = (v_1, \ldots, v_k)$ such that $v_1 = i$ and $v_k = j$. We also say that, there is a path from i to j.

Lemma 10.3 *The relation $\sim$ on the vertices is an equivalence relation.*

Proof: It is clear that $i \sim i$, since (i) is a path. Next, if $i \sim j$, then surely $j \sim i$: for if $\pi = (v_1, \ldots, v_k)$ is a path from i to j, then $\pi^R = (v_k, v_{k-1}, \ldots, v_2, v_1)$ is a path from j to i. Thus the only part which remains is to prove the transitivity of $\sim$. So, let $\pi = (v_1, \ldots, v_k)$ be a path from i to j, and $\mu = (w_1, \ldots, w_r)$ be a path from j to k. Let us concatenate these two paths to get a trail $\beta = (v_1, \ldots, v_k, w_2, \ldots, w_r)$. Note that $v_k = w_1 = j$. If this trail is actually a path, then we are done: $i \sim k$. Whence, if this is not a trail, then there is a $s < k$ and a $t > 1$ such that $v_s = w_t$. Let us look at the smallest such s such that $v_s = w_t$ with $s < k$ and $t > 1$. having located this s, t, we construct $\alpha = (v_1, \ldots, v_s, w_{t+1}, \ldots, w_r)$.

We claim that this α is a path from i to k. It is already clear that α is a trail (since we have just 'shortened' a loop from the trail β). Further $v_1 = i$ and $w_r = k$. Now, if α were not a path then there are two vertices which appear twice on the trail. But these two vertices cannot lie purely in the v-part or the w-part. Whence, there must be a v_m with $m < s$ such that $v_m = w_n$ with $n > t$. This is impossible, by the choice of s. $\Box$

Thus $\sim$ is an equivalence relation on V. Whence, given a graph $G(V, E)$, $\sim$ on V partitions V into disjoint sets $V = \cup_{i=1} V_i$, such that each $V_i = [v_i]_\sim$ is an equivalence class. Each equivalence class is called a **connected component** of the graph. The graph is called **connected** if V is itself an (unique) equivalence class. A lemma that we will need later, and whose proof is easy from the above observation:

Lemma 10.4 *Let $G(V, E)$ be a graph, then V may be expresses as a disjoint union $V = V_1 \cup \ldots \cup V_k$ and E as a disjoint union $E = E_1 \cup \ldots \cup E_k$, where $E_i \subseteq \binom{V_i}{2}$, such that $G(V_i, E_i)$ is connected, for all i. The quantity k is called the number of* **components** *of G.*

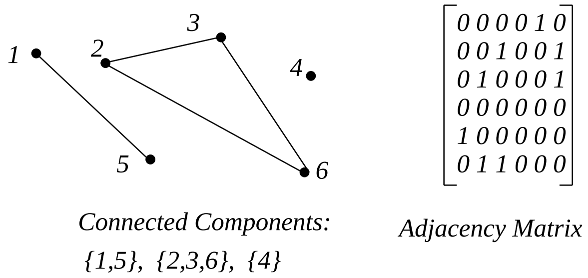


Figure 8: A graph and its adjacency matrix

We shall now outline a representation of graphs on a computer, and see how to compute the relation $\sim$ for this representation. For a graph $G(V, E)$ with vertex set $V = \{1, 2, \ldots, n\}$ we for an $n \times n$-matrix A such that $A[i, j] = 1$ iff (i, j) is an edge, and is zero otherwise. This matrix is called the **adjacency matrix** of the graph G. An example of a graph and its adjacency matrix appears in figure 10.1. Notice that for an undirected graph, its adjacency matrix must be symmetric.

Proposition 10.5 *Let $G(V, E)$ be an undirected graph and A be its adjacency matrix. Let $|V| = n$ and I be the $n \times n$ identity matrix. Let $C = (A + I)^{n-1}$ be the $(n-1)$-th power of the matrix $A + I$. Then $C[i, j] \neq 0$ iff $i \sim j$.*

Proof: Notice that for any matrix $D = (d_{ij})$, we have

$$D^{n-1}[i, j] = \sum_{s_1, \ldots, s_{n-2}} D[i, s_1]D[s_1, s_2] \ldots D[s_{n-3}, s_{n-2}]D[s_{n-2}, j]$$

Applying this to when $D = A + I$, we see that (i) all entries of A and I are non-negative. Thus $C[i, j]$ is non-zero iff there is a sequence $(i, s_1, s_2, \ldots, s_{n-2}, j)$ such that $D[i, s_1], \ldots, D[s_{n-2}, j]$ are all non-zero.

Let us consider such a sequence $\alpha = (i = s_0, s_1, \ldots, s_{n-2}, s_{n-1} = j)$. We see that $D[s_i, s_{i+1}]$ is non-zero iff either $s_i = s_{i+1}$ or $A[s_i, s_{i+1}] \neq 0$, i.e., $(s_i, s_{i+1}) \in E$. Thus we see that $s_0 \sim s_1, \ldots, s_i \sim s_{i+1}, \ldots, s_{n-2} \sim s_{n-1}$. By the transivity of $\sim$, we have $s_0 \sim s_{n-1}$, i.e., $i \sim j$. Thus $C[i, j] \neq 0$ implies that $i \sim j$. On the other hand, if $i \sim j$, then there is a path $(i = s_0, \ldots, s_k = j)$ connecting i to j. Since the length of the path is at most $n - 1$, we may extend this to the sequence $(s_0, \ldots, s_k, s_k, \ldots, s_k)$ of length $n + 1$. This sequence will contribute a non-zero number to $D^{n-1}[i, j]$ and thus $C[i, j] \neq 0$. $\square$

Now we move to another important equivalence relation, but this time, on the edges of a graph.

Definition 10.6 *Given a graph $G(V, E)$ and two edges $e = (i, j)$ and $f = (k, l)$, we say that $e \approx f$ if either $e = f$ or there is a cycle $(v_1, \ldots, v_k, v_{k+1} = v_1)$ such that both edges e and f appear in that cycle. In other words, if there is an r and an s such that $(v_r, v_{r+1}) = e$ and $(v_s, v_{s+1}) = f$.*

Thus two edges are related if they appear in the same cycle.

Proposition 10.7 *For any graph $G(V, E)$, $\approx$ is an equivalence relation on E.*

Proof: It is clear that $\approx$ is reflexive and symmetric. What remains is the transitivity of $\approx$. So let e, f, g be three distinct edges such that $\pi = (v_1, \ldots, v_a, v_{a+1} = v_1)$ is a cycle containing e and f, and $\mu = (w_1, \ldots, w_b, w_{b+1} = w_1)$ is a cycle containing f and g. We may as well assume that $(v_1, v_a) = e$ and $(w_1, w_b) = g$. Let $r \geq 1$ be the smallest r such that v_r appears somewhere on cycle μ, and say $v_r = w_u$. Similarly, let $s \leq a$ be the largest such s such that v_s again appears on μ, and say $v_s = w_v$. Since there is an edge f on π which appears in μ, it must be that $r < s$ and $u \neq v$.

There are now two cases:
(i) **Case** $u < v$: Consider

$$\alpha = (v_r, v_{r-1}, \ldots, v_1, v_a, v_{a-1}, \ldots, v_s, w_{v+1}, w_{v+2}, \ldots, w_b, w_1, w_2, \ldots, w_{u-1}, w_u = v_r)$$

We claim that all the vertices appearing in α are distinct. Clearly those coming from π and and those coming from μ are separately distinct. What remains is the possibility that $v_i = w_j$ when both appear in α. Such an offending i must either be less than r or greater than s, but both possibilities are precluded by the choice of r and s. Thus α is indeed a cycle. It is clear that $e = (v_a, v_1)$ and $g = (w_b, w_1)$ are on this cycle.

(i) **Case** $u > v$: Consider

$$\beta = (v_r, v_{r-1}, \ldots, v_1, v_a, v_{a-1}, \ldots, v_s, w_{v-1}, w_{v-2}, \ldots, w_1, w_b, w_{b-1}, \ldots, w_{u+1}, w_u = v_r)$$

It is similarly shown that β is a cycle containing both e and g. □

11 Trees and Spanning Trees

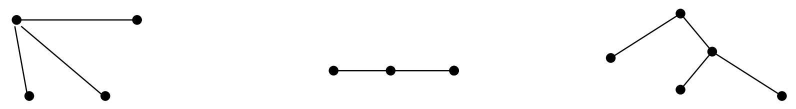
Trees are some of the most simple families of graphs.

Definition 11.1 *A graph $G(V, E)$ is a* **tree** *if it is (i) connected, and (ii) acyclic, i.e., contains no cycles.*

See figure 11 for examples of trees.
We will need an auxiallary definition. Given a graph $G(V, E)$, we define the **degree** $d(v)$ of a vertex $v \in V$ to be the number of edges incident on it. In other words $d(v) = |\{e | e = (v, w) \in E\}|$.

Lemma 11.2 *If $G(V, E)$ is a tree, then it has at least two vertices of degree 1.*

Proof: We choose v_1 as the solitary vertex of degree 1, if there is only one such vertex, or an arbitrary vertex, if there is no vertex of degree 1. Next, we



(a) (b) (c)

Figure 9: Examples of Trees

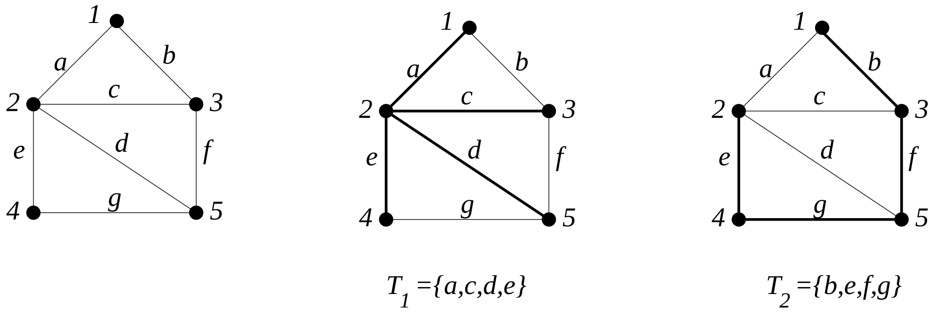
choose v_2 to be adjacent to v_1. We proceed thus, choosing v_{i+1} to be adjacent to v_i but *distinct* from v_{i-1}. This can always be done since every v_i with $i \geq 2$ has degree at least 2. Since this sequence is potentially infinite, there must be a first r such that $v_r = v_s$, with $s < r$. Let us look at the sequence $\mu = (v_s, v_{s+1}, \ldots, v_{r-1}, v_r)$. By the choice of r, there are no duplications in μ. Furthermore, every pair of adjacent vertices in the list actually make an edge. Thus μ is a cycle, which contradicts the hypothesis that G is acyclic. $\Box$

Proposition 11.3 *(i) If $G(V, E)$ is a tree then $|E| = |V| - 1$.*
(ii) If $G(V, E)$ is a connected graph with $|V| - 1$ edges, then it must be acyclic, and hence a tree.
(iii) If $G(V, E)$ is an acyclic graph with $|E| = |V| - 1$ edges, then it must be connected, and hence a tree.

Proof: We prove this by induction on $|V|$. We know, by lemma 11.2, that there is a vertex v with only one edge $e = (v, w)$ incident at v. Consider the graph $G'(V', E')$ with $V' = V - v$, and $E' = E - e$. We claim that G' is a tree. It is clearly acyclic, since $E' \subset E$ and E allowed no cycles. What remains is to show that G' is connected. For that, note that if $x, y \in V'$, then $x, y \in V$ as well. Since, G was connected, there was a path from π from x to y. We next argue that this path does not use the edge e, and thus lies completely in E'. For if it did, then the path would terminate at v, since there is no 'exit' from v. However, $v \notin V'$, and there $v \neq x, y$. Thus π lies completely in E' proving that x is connected to y in G'. Thus G' is a tree, and we have, inductively, $|E'| = |V'| - 1$, which proves the same for G as well.

Now we prove part (ii). First note that if α is a cycle in the graph G, and $e \in \alpha$ is an edge on the cycle, then $G'(V, E')$ with $E' = E - e$ is also connected. This is because any path using the edge e may now use the cycle α and go the 'other way'. Whence, beginning with a connected graph G, we may sequentially delete edges from cycles, thus maintaining connectivity but reducing the number of edges. At some point this must stop and we will have a connected acyclic graph $G''(V, E'')$. Since G'' is then a tree, we have $|E''| = |V| - 1 = |E|$. this means that G was acyclic to begin with.

Finally, we prove (iii). Suppose G is not connected, we have, by lemma 10.4, a decomposition of G into its connected components. Whence, the identity $E| = |V| - 1$, tells us that G has a component $G(V_i, E_i)$ such that $|E_i| \geq |E_i|$. Consequently, it is clear from part (i) that it cannot be a tree, and thus must



(a) The original graph *(b) Two spanning trees*

Figure 10: Spanning Trees

contain a cycle. Thus G itself must contain a cycle, which contradicts the hypothesis. $\square$

Proposition 11.4 *Let $G(V, E)$ be a connected graph with n vertices. If $|E| \geq n$ then G has a cycle. If $|E| = n$ then G has a unique cycle.*

Proof: Proposition 11.3 tells us that G cannot be acyclic, which proves the first assertion. Now, suppose $E| = n$, and there are two cycles α and β. Since these are distinct cycles, the subsets of edges on these cycles must also be distinct (this needs some thought). Thus there must be an edge $e \in \alpha$ but not in β. Upon deleting e from the graph G, we have a connected graph with $n-1$ edges which *also* contains the cycle β. This contradicts proposition 11.3, (ii). $\square$

Now, we come across an important application relating trees and general graphs.

Definition 11.5 *Let $G(V, E)$ be a connected graph. A subset $T \subseteq E$ of the edges is called a* **spanning tree** *if $G(V, T)$ is a tree.*

Thus a spanning tree T is a subset of the edges of the orginal graph so that T is acyclic and connects the vertex set of the original graph. An exmaple of a graph and some spanning trees of the graph, is shown in figure 11.

It is clear that, when $|V| = n$, not every collection T of $n-1$ edges make a spanning tree. It must either be connected or (equivalently) be acyclic. One representation of graphs is particularly revealing in this matter.

Let G be a graph $G(V, E)$ with n vertices $V = \{1, 2, \ldots, n\}$ and m edges $E = \{e_1, \ldots, e_m\}$. We form the **edge-adjacency matrix** $B(V, E) = B$, which is $n \times m$, such that (i) $B[v, j] = 1$ if $e_j = (v, w)$ and $v < w$, (ii) $B[v, j] = -1$ if $e_j = (v, w)$ and $v > w$, and (iii) $B[v, j] = 0$ if e_j is not incident at vertex v. The **reduced edge-adjacency matrix** $B'(V, E)$ is obtained by deleting the last row of B.

The matrices B and B' for the graph of figure 11 (a) is shown below (where $E = \{a, b, c, d, e, f, g\}$ are listed in that order):

$$B = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & -1 & -1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & -1 & 0 & -1 & -1 \end{bmatrix} \quad B' = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & -1 & -1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 1 \end{bmatrix}$$

First note that, though B has n rows, the last row depends on the first $n-1$ rows by the relation :$r_1 + \ldots + r_n = 0$. Thus no information is 'lost' by deleting the last row to get B'. Next, For $E' \subseteq E$, let $B'[][E']$ denote B' restricted to the columns E'.

Lemma 11.6 *Let $T \subseteq E$ be a subset of the edges such that $|T| = n-1$. Let $B'[][T]$ be the $(n-1) \times (n-1)$ sub-matrix corresponding to the edges T. If T contains a cycle then $det(B'[][T]) = 0$.*

Proof: Let $\pi = (v_1, \ldots, v_k, v_{k+1} = v_1)$ be a cycle such that $(v_i, v_{i+1}) \in T$ doe all i. We show that the corresponding columns of $B'[][T]$ are linearly dependent. Let $col(e)$ denote such a column, for $e \in T$. If $e_i = (v_i, v_{i+1})$ and $v_i < v_{i+1}$, then we put $\theta_i = 1$, with $\theta_i = -1$ otherwise.

We show that $\sum_{i=1}^{k} \theta_i col(e_i) = 0$. Looking at the entry for a vertex i, we see that either the cycle misses the vertex v, in which case, every entry $col(e)[i] = 0$, or else it is or appears in two consecutive edges, say e_i and e_{i+1}, where $e_i = (u, v)$ and $e_{i+1} = (v, w)$, where the vertices are listed in the order that they appear in the cycle. Now we consider various cases such as $u < v < w$, in which case (i) $B'[v, e_i] = -1$ and $B'[v, e_{i+1}] = +1$, and (ii) $\theta_i = \theta_{i+1} = 1$. Thus

$$\sum \theta_j col(e_j)[v] = \theta_i col(e_i)[v] + \theta_{i+1} col(e_{i+1})[v] = 0$$

Thus $\sum \theta_j col(e_j)$ is a linear dependence on the columns of $B'[][T]$. This proves the lemma. $\Box$

One may check that for our example, $col(a) + col(c) - col(b) = 0$ corresponds to the cycle $(1, 2, 3, 1)$, and $col(e) + col(g) - col(f) - col(c) = 0$ corresponds to the cycle $(2, 4, 5, 3, 2)$.

An important result is that the converse is also true: every acyclic subset $T \subseteq E$ such that $|T| = n-1$ is 'non-singular'.

Proposition 11.7 *For a subset $T \subseteq E$, with $|T| = n-1$, we have T is a spanning tree if and only if $B'[][T]$ is non-singular.*

Proof: Firstly, if $B'[][T]$ is non-singular then T cannot contain a cycle, by lemma 11.6. Next, by proposition 11.3, every subset T of cardinality $n-1$ must be a spanning tree.

Conversely, Let T be a spanning tree. Note that $B'[][T]$ is also the reduced edge-adjacency matrix $W' = B'(G(V, T))$ for the graph $G(V, T)$. Thus we may as well ignore the larger graph $G(V, E)$ while proving the property at hand.

Further, by lemma 11.2, we know that T has at least two vertices of degree 1 in the graph $G(V,T)$. Thus, there is at least one vertex, say i, in the set $\{1,2,\ldots,n-1\}$ of degree 1. Whence, in row i of matrix W', there is exactly one non-zero entry, ± 1, corresponding to the edge e incident at the vertex i. Thus $det(W') = \pm det(W'')$, where W'' is the matrix W with row i and column $col(e)$ deleted. But W'' is then the reduced edge-adjacency matrix of the graph $G(V'',T'')$, where $V'' = V - i$ and $T'' = T - e$, which is also a tree. Since T'' is smaller than T, we can assume the inductive hypothesis that $det(W'') \neq 0$. Whence $det(B'[][T] = det(W') = \pm det(W'') \neq 0$, and we are done. $\Box$

An important corollary of the proof of the above proposition is that $det(B'[][T]$ is actually ± 1. This results in a surprising formula for the total number of spanning trees in a connected graph, viz., $det(B'(B')^T)$. We leave it to the reader to prove this assertion, while hinting at the classical Laplace expansion of the determinant.

12 Minimum Cost Spanning Trees

In this section, we look at an optimization problem related to spanning trees. Let $G(V,E)$ be a connected graph, and let $c : E \to \mathbb{R}$ be a **cost** function on the edges. For a sub-collection $E' \subseteq E$, we define $c(E')$ as $c(E') = \sum_{e \in E'} c(e)$. thus the cost $c(E')$ of the collection is the sum of the costs of the edges in the collection.

Our objective is to find a spanning tree T in the graph such that $c(T)$ is minimized. This problem occurs in many practical situations, e.g., the cost $c(e)$ may denote the length of the cable between two destinations, and the spanning tree T then computes the cost of a skeletal network connecting all destinations.

We will fix a connected graph $G(V,E)$ with a cost function $c : E \to \mathbb{R}$. Let T be a spanning tree and let $e \notin T$ be a non-tree edge. Let us look at $E' = T + e$, which is a connected graph with $n = |V|$ edges. By proposition 11.4, E' will have a unique cycle, which we will refer to as the **circuit** $Ckt(T,e)$. If f is any edge in $Ckt(T,e)$, then $T' = T + e - f$ is another tree. We say that T' has been obtained by an **exchange** from T.

Since T and T' differ only in two edges, we have $c(T') = c(T) + c(e) - c(f)$. thus if $c(e) < c(f)$, then $c(T') < c(T)$. This motivates the following definition:

Definition 12.1 *We say that a spanning tree T is* **locally optimal** *if for every non-tree edge $e \notin T$, and every $f \in Ckt(T,e)$, we have $c(e) \geq c(f)$.*

Thus, for a locally optimal tree, there is no such convenient exchange which will actually reduce the cost of the spanning tree. We now prove that locally optimal trees are actually globally optimal.

Theorem 12.2 *Let $G(V,E)$ be a connected graph with cost function $c : E \to \mathbb{R}^+$ and let T be a locally optimal spanning tree. if Q is any other spanning tree, then $c(Q) \geq c(T)$. In other words, Q is globally optimal.*

Proof: Suppose there is a Q such that $c(Q) < c(T)$. Out of this collection of cheaper spanning trees, we select P such that $c(P) < c(T)$, and $|P \cap T|$ is the maximum possible, among cheaper trees. Let $\Delta T = T - P$ and $\Delta P = P - T$ be the collection of edges in T but not in P, and respectively, P but not in T. Let $\Delta = \Delta P \cup \Delta T$; we will argue that Δ is in fact, empty.

Suppose then that Δ is non-empty, and $e \in \Delta$ is an edge of minimum cost among all edges in Δ. If $e \in \Delta T$, then e is a non-tree edge for P. Next we look at $Ckt(P, e)$, the cycle formed by introducing e into P. For any edge $f \in Ckt(P, e)$ we must have $c(e) \geq c(f)$, for otherwise $P' = P + e - f$ would be a cheaper tree, contradicting the global optimality of P. Next, examing $Ckt(P, e) \cap \Delta P$, we see that if $f \in Ckt(P, e) \cap \Delta P$, then $c(f) \geq c(e)$, simply because e was chosen as a minimum cost edge in $\Delta \supseteq \Delta P$. This must mean that $c(f) = c(e)$ for all $f \in Ckt(P, e) \cap \Delta P$. Now, if there were such an f, then $P' = P + e - f$ is also a globally optimal tree, but $T \cap P' = T \cap P \cup \{e\}$ and thus $|P' \cap T| > |P \cap T|$ contradicting the choice of P. Thus there are no edges in $Ckt(P, e) \cap \Delta P$. Thus $Ckt(P, e)$ lies completely within $\{e\} \cup (P \cap T)$. But $\{e\} \cup (P \cap T) \subseteq T$, and thus $Ckt(P, e)$ is a cycle contained in a tree T, which is a contradiction. Thus we are forced to conclude that $e \notin \Delta T$. In fact, we are forced the stronger assertion that every minimum cost edge from Δ actually lies in ΔP.

So then, let $e \in \Delta P$ be of minimum cost among all edges in Δ. We know that if $f \in \Delta T$, then $c(f) > c(e)$, for no minimum cost edge can be in ΔT. We now show that T is not locally optimal. Since e is a non-tree edge for T, we consider $Ckt(T, e)$. By a similar argument, it is clear that $Ckt(T, e)$ cannot completely lie in $\{e\} \cup (T \cap P)$. Whence, there is an edge $f \in Ckt(T, e) \cap \Delta T$. Since $c(f) > c(e)$, we see that there is a non-tree edge e, with an $f \in Ckt(T, e)$ such that $c(f) > c(e)$. This contradicts the local optimality of T. $\Box$

next, we consider a 'greedy' approach to building minimum cost spanning trees. We show that such trees are actually locally optimal, and hence globally optimal.

Recall first, that a maximal acyclic subset of edges $T \subset E$ is actually a spanning tree. Let $E = \{e_1, \ldots, e_m\}$ be so ordered such that $c(e_i) \leq c(e_{i+1})$.

We define the sets E_i, $i = 0, 1, \ldots, m$ recursively as follows: $E_0 = \phi$, the empty set.

$$E_i = \begin{cases} E_{i-1} & \text{if } E_{i-1} \cup \{e_i\} \text{ contains a cycle} \\ E_{i-1} \cup \{e_i\} & \text{otherwise} \end{cases}$$

Let $T = E_m$.

Lemma 12.3 *The set T is a maximal acyclic subset of E, and thus is a tree.*

Proof: Since E_i grows only when $E_{i-1} + e_i$ is acyclic, it is clear that the final set $E_m = T$ is also acyclic. Next suppose that E_m is not maximal acyclic, i.e., there is an $e = e_j \notin E_m$ but $E_m + e_j$ is also acyclic. Looking at E_j, we see that since $e_j \notin E_m$, it must be that $e_j \notin E_j$ as well. Whence, it must be that $e_j + E_{j-1}$ contained a cycle. This cycle persists in $E_m + e_j$, a contradiction. Thus such an e_j cannot exixt, and $E_m = T$ must be acyclic. $\Box$

Theorem 12.4 *The set $E_m = T$ is a locally optimal spanning tree (and thus, by Theorem 12.2, globally optimal as well).*

Proof: Suppose that T is not locally optimal. Whence, there is an edge $e \notin T$, and an edge $f \in Ckt(T, e)$ such that $c(e) < c(f)$. Let $e + e_j$ and $f = e_k$, and conclude that, since the edges are ordered by increasing cost, it must be that $j < k$. Looking at $T + e_j$, we know that there is a unique cycle, which is broken by excluding the edge f. Thus $T' = T + e - f$ is also a tree, and hence acyclic. If we now look at E_{j-1} and $E_{j-1} + e_j$, we note that both these sets are subsets of T' and hence acyclic. Thus, it must be that $E_j = E_{j-1} + e_j$, and $e = e_j \in E_m$ as well, a contradiction. $\Box$

A similar construction of minimum cost spanning trees exist by considering spanning trees as minimally connected subsets. We may thus order the edges of $E = \{f_1, \ldots, f_m\}$ by *decreasing* cost. Define $F_0 = E$, and F_i recursively as:

$$F_i = \begin{cases} F_{i-1} & \text{if } F_{i-1} - e_i \text{ is disconnected} \\ F_{i-1} - e_i & \text{otherwise} \end{cases}$$

A similarly proved theorem asserts that F_m is locally and therefore globally optimal.

13 Matchings

Let $G(V, E)$ be an undirected graph. We say that a graph is bipartite, if $V = U \cap W$ is a partition of the vertex set into two parts such that if $e = (i, j) \in E$, then $i \in U$ and $j \in W$, or vice-versa. Thus edges run only across the two components of the partition. We also denote such a bipartite graph as $G(U \cup W, E)$.

A matching $M \subseteq E$ is a collection of edges so that no two edges from the matching are incident at the same vertex. In other words, (i) if $(u, w_1), (u, w_2) \in M$, then $w_1 = w_2$, and (ii) if $(u_1, w), (u_2, w) \in M$, then $u_1 = u_2$. For a matching M, we say that a vertex $x \in V$ is **unmatched** in M if there is no $y \in V$ such that $(x, y) \in M$. Thus an unmatched vertex has no matching edge incident at it.

Definition 13.1 *Let M be a fixed matching.*

- *A path $\pi = (v_1, \ldots, v_k)$ is called an* **alternating path** *if*
  (i) (v_1, v_2),$(v_3, v_4), \ldots, (v_{odd}, v_{odd+1}) \notin M$,
  (ii) (v_2, v_3),$(v_4, v_5), \ldots, (v_{even}, v_{even+1}) \in M$, and (iii) v_1 is unmatched, and if k is even, then so is v_k. The length of the path is $k - 1$.
- *A cycle $\pi = (v_1, \ldots, v_k, v_{k+1} = v_1)$ is called an* **alternating cycle** *if*
  (i) k is even, and (v_1, v_2),$(v_3, v_4), \ldots, (v_{odd}, v_{odd+1}) \notin M$,
  (ii) (v_2, v_3),$(v_4, v_5), \ldots, (v_{even}, v_{even+1}), \ldots, (v_k, v_1) \in M$.

Alternating paths of odd length will be very important, and are also called as **augmenting paths**. Note that for odd-length alternating paths, both its end vertices must be un-matched. Let π be an alternating path/cycle. Let $e(\pi)$ be the edges on the path/cycle, i.e., if $\pi = (v_1, v_2, \ldots, v_k)$, then $e(\pi) = \{(v_i, v_{i+1}) | i = 1, \ldots, k-1\}$. Thus both $e(\pi)$ and M are subsets of E.

For two sets S, T, we define $S \oplus T = S \cup T - (S \cap T)$. Thus $S \oplus T$ consists of those elements which belong to S but not T, or vice-versa.

Proposition 13.2 *Let M be a matching and π be an alternating path or cycle. Let $N = M \oplus e(\pi)$. Then N is a matching. If π is an augmenting path, then $|N| = |M| + 1$.*

Proof: Let $e = (x, y)$ and $f = (x, z)$ be two edges in N which meet at the same vertex x. Since $e, f \in N$, it must be that one of the following must hold: (i) both $e, f \in M$ but not on π, but that is untenable because M is a matching, or (ii) both $e, f \in e(\pi)$ but not in M, but this is too is untenable, since in an alternating path/cycle, if two edges share a vertex then one of them must belong to the matching M. Thus we are left with (iii) $e \in M - e(\pi)$ and $f \in e(\pi) - M$. Looking at the edge $f = (x, z) \in e(\pi)$, we see that x is either a terminal vertex of the path and is unmatched, or there must be a w such that $(w, x) \in M \cap e(\pi)$. The existence of $e = (x, y) \in M - e(\pi)$ precludes both possibilities. Thus there are no two edges $e, f \in N$ meeting at the same vertex.

This proves that N is a matching. Now, if π were an augmenting path, then $|e(\pi) - M| = |e(\pi) \cap M| + 1$, and thus $|N| = |M| + 1$. $\Box$

We will need an auxiallary lemma, which we state without proof:

Lemma 13.3 *Let $G(V, E')$ be a graph such that every vertex has degree atmost 2. Then every connected component of G is either a path or a cycle.*

Theorem 13.4 *Let M be a matching in a bipartite graph. If M is not the maximum cardinality matching in G, then there is an augmenting path π with respect to M.*

Proof: Suppose N is a maximum cardinality matching in G. Consider $P = M \oplus N$. First note that if we consider the graph $G' = G(V, P)$ defined by the edges in P, then every vertex in G' has degree atmost 2. This is beacuse a vertex v can have atmost one edge from the matching M, and atmost one from the matching N. Thus, by the above lemma, each component of G' is either a path or a cycle. Since, every vertex v may contain at most one edge from M, and atmost one from M, we see that each component is either an alternating path or an alternating cycle for the matching M. Since $|M| < |N|$, and every cycle will have equal number of edges from M and N, there must be a path with more from N than from N. Whence, this path is an augmenting path. $\Box$

Theorem 13.5 *Let $G(U \cap W, E)$ be a bipartite graph with $|U| = |W| = n$. If there is no complete matching (i.e., a matching of cardinality n), then there is a set $X \subseteq U$ such that $|\Gamma(X)| < |X|$, where $\Gamma(X) = \{w | \exists u \in U, (u, w) \in E\}$.*

Proof: Let M be a maximum cardinality matching in G. Suppose that $|M| < n$, and $u \in U$ is an unmatched vertex. Let

$$X = \{x \in U | \text{there is an alternating path from } u \text{ to } x\}$$

We claim that $\Gamma(X)$ contains no un-matched vertices, or those matched to some vertex outside X. Suppose for example, that $w \in \Gamma(X)$, were unmatched. Since $w \in \Gamma(X)$, there is an alternating path $\pi = (u = v_1, \ldots, v_k = x)$ and $(x, w) \in E$. However, then we have the path $\mu = (v_1, \ldots, v_k, v_{k+1} = w)$ which is an odd-length alternating path, and therefore an augmenting path. By proposition 13.2, we would have a matching better than M, a contradiction. On the other hand, if w were matched to a vertex outside X, say $(u', w) \in M$ then $\eta = (v_1, \ldots, v_k = x, w, u')$ is an alternating path from u to u', whence u' should have been in X. This shows that all vertices $w \in \Gamma(X)$ must be matched to some vertex in X. Since $u \in X$ is unmatched, we have $|\Gamma(X)| < |X|$. $\square$

14 Network Flows

A **network** $N(V, E)$ is a directed graph, with special vertices $s, t \in V$ called respectively, the **source**, and the **sink**. Furthermore, there is a **capacity** function $c : E \to \mathbb{R}^+$, where for $e = (i, j)$, we denote $c(e)$ by c_{ij}.

A **flow** in a netwrok N is a function $f : E \to \mathbb{R}^+$ such that (i) $0 \leq f_{ij} \leq c_{ij}$ for all $e = (i, j) \in E$, and (ii) $\sum_{j \in V} f_{ij} - \sum_{k \in V} f_{ki} = 0$, for all $i \in V - \{s, t\}$. The first requirement is called **feasibility**, while the second is called **conservation**.

If we denote $\delta_i = \sum_{j \in V} f_{ij} - \sum_{k \in V} f_{ki}$, then the requirement δ_i say that 'the fow coming in equals the flow going out' at i. The **value** of a flow $v(f)$ is the quantity δ_s, i.e., the net flow going out of s.

Lemma 14.1 *Let N be a network and f a flow in the network. Then $\delta_s = -\delta_t$. In other words, the net outflow at s equals the net inflow at t.*

Proof: We investigate the sum $\delta = \sum_{v \in V} \delta_v$. For any quantity f_{ij}, we see that it appears with a positive sign in δ_i and with a negative sign in δ_j. Since this accounts for every term in δ, we have that $\delta = 0$. Since conservation implies that $\delta_v = 0$ for all $v \notin \{s, t\}$, we have $\delta_s + \delta_t = 0$. $\square$

Let $X \subseteq V$ be such that $s \in X$ while $t \notin X$. Such a set is called a **cut**. The set $\Gamma(X)$ is defined as:

$$\Gamma(X) = \{(i, j) \in E | i \in X, j \notin X\}$$

The **capacity** of a cut $c(X)$ is defined as $c(X) = \sum_{e \in \Gamma(X)} c(e)$. Thus the cut-capacity is the sum of the capacities of the edges going from X to outside X.

Lemma 14.2 *Let N be a network and f a flow in the network. If X is any cut, then $v(f) \leq c(X)$.*

Proof: Let us examine $\delta_X = \sum_{v \in X} \delta_v$. This quantity, by conservation, equals the number $\delta_s = (v(f)$. On the other hand, it is easy to see that the only quantities that contribute to δ_X are those flows with one end-point in X and the other outside. Thus:

$$\delta_X = (\sum_{i \in X, j \notin X} f_{ij}) - (\sum_{p \in X, q \notin X} f_{qp})$$

Since the first term is clearly upper-bounded by $C(X)$ and the second term is lower-bounded by 0, we have

$$v(f) = \delta_X \leq c(X)$$

That proves the lemma. □

An important theorem is the **Maxflow-Mincut** theorem, which we state without proof:

Theorem 14.3 *Let N be a network and f a flow in the network. If μ is the minimum among all cut capacities, then there is a flow of value μ.*