Bottom up Computing and Discrete Mathematics

P P Martin

February 28, 2005

Contents

Chapter 1

Introduction

1.1 Overview

The idea of this course is to touch on as many aspects as possible of the process of using the power of computers, and the theory of discrete mathematics which underlies them.

The aim is to make the student of this course one of the people in their workplace (wherever that might eventually be) who 'knows about computers'.

The 'power of computers' is a very big subject. It includes the things we are aware of computers helping us with, such as

- word processing,
- bookkeeping,
- audio-visual applications and
- design;

as well as more subtle things like

- information gathering
- information organisation,

- information enrichment
- systems simulation,
- optimisation problems,
- robotics

and a million other things.

Discrete Mathematics is the theory underlying all these tools.

Obviously one cannot know everything. Even 'about computers'. The idea here is to deal with the following problem (which is 'universal' in the sense that, if you can solve this one you can work out how to solve all the others!):

Your boss wants a report on XXX[1] by the end of next week. All the necessary information is out there on the web somewhere. But all you have on your desk is a couple of broken computers and some components, and the technicians were laid off in the last round of cutbacks. (And anyway, Google is down for two weeks for legal reasons.) What could you do?

The course contains two overall components, corresponding to the hardware and 'software' aspects of this problem. The connection between them will be obvious, but they are very different, and can be studied in any order.

The theory part of the course is largely covered in these notes. A suitably concrete version of the problem described above is set up in Chapter 2, and we will start there. As we work through this, we encounter various problems. The theory needed to resolve these problems is contained in the core of the notes, for example in Chapter 4. We will jump there as soon as appropriate, jumping back once we have enough theory to progress our problem, and so on.

There is also a section of more basic Mathematics which we can refer to as necessary, but will not, by default, discuss in class.

[1] Perhaps XXX is: the price of pork bellies on the Chicago futures exchange?

The practical part of the course will consist largely of 'lab' sessions which we can insert at any time to break up the 'monotony' of the theory!

Essentially we will be stripping down a computer to the smallest realistic components, identifying them, understanding them (as far as possible) and then reassembling. (This process works as a metaphor for the operating system as well as the real hardware.) There will only be limited notes on the practicals, and they will not be heavily examined (or otherwise assessed). The motivation for this part of the course will be its very obvious usefulness!

1.2 Prerequisites

We assume that the reader has a knowledge of naive set theory, such as discussed in first year undergraduate ALGEBRA. However we include a brief refresher on this subject in Chapter 3.

1.3 Other support material

- Check out the course homepage.
- Check out the vast amount of related material on the web.
- Check out past exam papers and solutions.
- Check out books called 'DISCRETE MATHEMATICS' (or similar), such as Mattson [7].
- Check out Stephenson [11], Spiegel [10], Ayers [1], and other related volumes in the Schaum Outline series.

Chapter 2

Paradigms

We do not propose to deal with every aspect of the use of computing and discrete mathematics. Rather we will look at examples. We will look at examples that are so profound that, once we have understood them, we will see how to *transfer* this knowledge to all other appropriate problems.

2.1 Searching

Each of us has access to an accumulated store of knowledge and information. This store is only useful in so far as information can be retrieved from it. Methods for retrieving information from the store are, in this sense, as useful as the store itself. The study of *searching* is the study of these methods.

2.1.1 The PageRank Algorithm: searching the web

The web is part of our accumulated store of knowledge and information. *This* store is only useful in so far as information can be retrieved from it. Methods for retrieving information from this store are, in this sense, as useful as the store itself. We propose to study these methods.

The web provides a useful paradigm, in that it is part of cyberspace, and hence accessible by computer (so some of the practical/physical challenges

of information retrieval are reduced to a standard form).

Problem: Your boss asks you to prepare a report on XXX. (This is not a school exercise or test of your originality — She doesn't care how you get it, she just needs the answer.) The requirement is to access the knowledge store and mine the relevant information. The simplest way is to see what is on the web.

The difficulty is that there are over 3×10^9 pages on the web. Thus even when you use a search engine to restrict to pages including the phrase XXX (an interesting exercise in its own right, but not one which concerns us for the moment) there will be too many pages — too much information.

What we need is a search engine which will rank all the hits in order, so that the ones most likely to be useful will be ranked at the top. Of course current search engines cannot know what the individual regards as useful! So they have to use a generic algorithm to make this judgement. How could we even begin to formulate such an algorithm?

We need to start with some kind of model or representation of the web. A model which attempted to carry any of the real human meaning of the pages would be (interesting but) extremely complicated. Rather let us begin by thinking of the pages simply as points in cyberspace, and concentrate on the links between them. Thus we have a set of pages, and a set of pairs of pages (i.e. pairs with the property that there is a link between them). Abstractly such a contruct is called a *graph*.

The notion of graph is fundamental in discrete mathematics. If you know all about graphs, continue. If you do not, it is time to jump to the section discussing graphs. Return here when you are done.

Exercise 1 *Go to Chapter 4 and return when you are done.*

We will base our answer on the search engine Google's PageRank algorithm [1].

The idea is to represent the web as a directed graph. The direction of the edges in the graph is from linking page to linked page. For simplicity we

[1] L Page, et al, Stanford University 1998.

will assume that there are no pages without outgoing links.

The PageRank algorithm is not too hard to describe in these terms. It has a single free input parameter p, which should lie in $0 < p < 1$ (we will interpret this later). The other input is the adjacency matrix of the web (!), W say. For simplicity we will consider that $W_{ij} = 1$ if there is a link from page i to page j, and is zero otherwise.

The algorithm is run iteratively, at each iteration assigning a value to each page. We will arrange the entire collection of values into a huge vector v (i.e., there is one such for each iteration). To start the process we must assign some initial value to each page (we will later consider the effect of this choice on the final result, for now we will simply assign every page the same initial value). The objective is to end up with a final vector consisting of one number for each web page, where these numbers give the importance rank of the pages (the bigger the number, the more important the page).

The idea behind the algorithm is that the importance of a page is judged on the incoming links. Roughly speaking, if a page is important, people will link their pages to it. More subtly, if it is important, other important pages will link to it. So essentially a page gets a vote from each linking page, but high ranked pages votes count for more.

The question is, how to implement this. Since importance depends on the importance of neighbours (whose importance may well depend on that of the original page), there is a question of existence and uniqueness of solution, not to mention convergence of any concrete algorithm.

Another way of thinking about it which helps with this is to imagine someone browsing the web 'forever'. Which ever page they are on at time t, they step to one of the linked pages at time $t + 1$. Now run this process for a hugely long time, and ask: over all that time, what is the total amount of time spent at each page (adding up all visits). The more important the page, the more often it will be visited. Although other outcomes can be imagined, you will see that it is possible that the *proportion* of the total time of the experiment spent at any given page may eventually settle down to a steady

figure. Again the question is, from this idea, how do we get to an actual numerical ranking?

Let v^n be the vector of PageRank values for each web page, at the n^{th} iteration, so that v_i^n is the value for page i. The iteration is

$$v_i^n = (1-p) + p \sum_{j \in \text{pages}} \frac{W_{ji} v_j^{n-1}}{\sum_{k \in \text{pages}} W_{jk}}.$$

Note that for each page j which links to i we have W_{ji} nonzero, so that this page makes a contribution to v_i^n, with the size of this contribution determined by the ranking of j itself at the previous iteration. (The denominator scales down the weight of these provisional ranked votes by the number of outgoing links the voting page has. The idea of this is so that, overall, it casts a total weight of votes, across all linked pages, proportional to its provisional rank.)

If and when the algorithm settles down (i.e. stops changing the values between successive iterations), we may say that it has assigned each rank based on the actual rank of that page's voters.

A number of questions arise. In particular:
How can we implement this algorithm in practice?
How can we tell if the algorithm settles down?
To answer these questions we can usefully recast our problem in the formalism of Stochatic Processes.

2.2 Stochastic Processes

Let M be a matrix, v a column vector, and $()^t$ the transpose operation. Consider the elementary fact of matrix multiplication

$$Mv = v' \qquad \Rightarrow \qquad v^t M^t = (v')^t$$

This 'duality' implies that M and M^t contain essentially the same information, and any property of the rows of M can be states as a property of the columns of M^t. If we wish to manipulate equations of the form above, the

use of M or M^t depends simply on whether we prefer to use row or column vectors. Of course having made a choice it is necessary to be consistent within any given calculation.

A matrix may be called *(column) stochastic* if its column sums are all 1, and all the entries are probabilities (i.e. non-negative). [2]
A matrix is called row stochastic if it is the transpose of a column stochastic matrix.
Different authors use different conventions as to whether the term *stochastic matrix* means row or column stochastic. As noted above, the difference is simply a matter of transposition (although we must be careful to be consistent).
Note that it is possible to be both row *and* column stochastic.
Exercise 2.1. Give distinct examples of each of the following: row stochastic matrix; column stochastic matrix; row and column stochastic matrix.

Suppose that the value of some variable (perhaps the price of a unit of pork bellies on the Chicago stock exchange) evolves randomly through a discrete series of time steps. If the probability of taking value x at time $n+1$ depends only on the value at time n, then this process is called a Markov chain. Suppose further that there are only finitely many values which the variable can take. Then we have a discrete time, finite state Markov process. Note that this process is determined by the set of transition probabilites between the various possible values. We arrange these into a matrix M, so that M_{ij} is the probability of taking value j at time $n+1$, given a value of i at time n. This means in particular that $\sum_j M_{ij} = 1$, since the probability of the variable taking a value, summed over all values, at time $n+1$ is 1.

Suppose we run this process for a long time. If it happens that the proportion of the time spent at each value settles down (irrespective of the initial value) then the vector ν of these proportions is called an invariant measure. If we arrange it as a row vector it will satisfy

$$\nu M = \nu$$

[2] Brzezniak and Zastawniak, Basic Stochastic Processes, Springer 1999.

(in fact no stochastic matrix can have an eigenvalue with absolute value greater than 1; and they all obviously have 1 as an eigenvalue).

Our random walk on the web would simply choose to follow one of the links out of the present page at random. If we write δ for the diagonal matrix whose m-th diagonal entry is the number of links *out* of page m, then the appropriate stochastic matrix is

$$M = \delta^{-1}W.$$

It is possible that only a subset of all web pages can be reached following outgoing links from some particular starting point. To avoid getting trapped in this way we will also allow a $1-p$ probability of simply ignoring the local links and jumping randomly to any point on the web. (We wouldn't want to do this totally random action any more than necessary, which is why we choose p fairly close to 1.) The stochatic matrix appropriate for this random jump mode on its own is simply the matrix f in which every entry is $1/\sigma$, where σ is the total number of pages on the web. Thus the combined matrix, allowing for the probability of chosing the random mode, is

$$M = (1-p)f + p\delta^{-1}W.$$

The totally random component makes sure that M does not break up into blocks which (via such beautiful ideas as the Peron–Frobenius theorem (see later)) ensures that the solution to the unit eigenvalue problem is unique (once the eigenvector is normalised so that the entries add to 1).

Let ι be the *vector* with all entries 1. Then $\nu^n\sigma f = \iota$ for ν^n any probability distribution row vector (exercise). It follows that, applying M to some probability distribution ν^n:

$$\nu^n M = \nu^n((1-p)f + p\delta^{-1}W) = \frac{(1-p)}{\sigma}\iota + p\nu^n\delta^{-1}W = \nu^{n+1}$$

confirming that M is the transition matrix for this process. The distribution is stable at ν:

$$\nu\left(1 - p\delta^{-1}W\right) = \frac{1-p}{\sigma}\iota$$

so

$$\nu = \frac{1-p}{\sigma}\iota + p\nu\delta^{-1}W$$

This means that the page rank vector is the invariant measure for the above random walk.

Since this is the eigenvector for the largest eigenvalue of the stochastic matrix we may compute it by starting with an (almost) arbitrary vector and simply repeatedly multiplying this by the stochastic matrix.

2.3 Examples

Model 1: Consider the very simple model of the web consisting of three pages, call them A,B and C, with A linking to B linking to C linking to A. This model has matrices

$$W = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \qquad \delta = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Then we have

$$M = (1-p)\left(\frac{1}{3}\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}\right) + p\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

This model has an obvious symmetry under permuting any two of the pages, so they must all be equally 'important'. This tells us that the invariant measure must be given by a vector with all entries equal. We can readily confirm this:

$$\left(\frac{1}{3}\begin{pmatrix} 1 & 1 & 1 \end{pmatrix}\right) M = \frac{1-p}{3}\begin{pmatrix} 1 & 1 & 1 \end{pmatrix} + \frac{p}{3}\begin{pmatrix} 1 & 1 & 1 \end{pmatrix} = \left(\frac{1}{3}\begin{pmatrix} 1 & 1 & 1 \end{pmatrix}\right)$$

(Note that we could have found the invariant measure by repeated multiplication on an arbitrary initial probability vector. In this case the steps in the iteration, although not the final answer, would have depended on p. Thus

the rate of convergence to the final answer can depend on p. For an extreme example, considering the initial vector $\begin{pmatrix} 1 & 0 & 0 \end{pmatrix}$ and $p = 1$ we see that this *never* converges!)

Model 2: Now consider what happens when B introduces a link back to A:

$$W = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \qquad \delta = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

so

$$M = (1-p)\left(\frac{1}{3}\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}\right) + p\begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

This model is connected so we can usefully consider $p \to 1$, whereupon

$$M = \begin{pmatrix} 0 & 1 & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} \\ 1 & 0 & 0 \end{pmatrix}$$

By the argument above we may determine the (relative) PageRanks by repeatedly multiplying this matrix into an initial positive matrix. (To get the absolute ranks we need to normalise this initial matrix as a matrix of probabilities, but this normalisation is just a fixed overall factor so we will not worry about it for now.) Consider

$$\begin{pmatrix} 1 & 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} \\ 1 & 0 & 0 \end{pmatrix}^n = \begin{pmatrix} 1.5 & 1 & .5 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} \\ 1 & 0 & 0 \end{pmatrix}^{n-1}$$

$$= \begin{pmatrix} 1 & 1.5 & .5 \end{pmatrix} M^{n-2} = \begin{pmatrix} 1.25 & 1 & .75 \end{pmatrix} M^{n-3} = \begin{pmatrix} 1.25 & 1.25 & .5 \end{pmatrix} M^{n-4}$$

$$= \begin{pmatrix} 1.125 & 1.25 & .625 \end{pmatrix} M^{n-5} = \begin{pmatrix} 1.25 & 1.125 & .625 \end{pmatrix} M^{n-6} = \ldots$$

Can you see where this is going? Consider

$$\begin{pmatrix} x & x & y \end{pmatrix} M = \begin{pmatrix} x & x & y \end{pmatrix}$$

giving $x = \frac{1}{2}x + y$, $y = \frac{1}{2}x$, so putting $2x + y = 1$ (for probabilities) we have $x = \frac{2}{5}$, $y = \frac{1}{5}$.

Now explain this in terms of the linking and importance of the pages! At first site, A and B are clearly more important than C, but A gets votes from both B and C, so you might think it beats B. However, B votes for both A and C, so its vote for A is diluted, while A always votes entirely for B which, in this model, locks their importance levels together.

Exercise 2 *What happens if we make $p < 1$?*

Exercise 3 *Consider the model with four pages, A,B, C and D, and matrix*

$$W = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Work out the PageRanks in case $p = .85$.

Exercise 4 *(Harder) Do a Google search for the common name "Paul Martin". Qualitatively explain the first page of results using PageRank.*

2.3.1 More exercises

Every simple loop free digraph is a representation of some model of the web.

Every $n \times n$ matrix with zeros down the diagonal and either 1 or 0 in each offdiagonal position is the adjacency matrix of some such digraph. Let A_n denote the set of such matrices. Evidently $|A_n| = 2^{n(n-1)}$. However, many of these matrices represent the same digraph up to isomorphism. (For example, any two such matrices containing precisely one nonzero element are isomorphic.)

A complete list of adjacency matrices of representative elements of isomorphism classes of 3 vertex simple loop free digraphs containing at most 2

edges is:

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

We can obtain a 3 edge digraph by taking a 2 edge digraph and adding an edge. Starting with the first 2 edge digraph above we get

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

but no others (up to isomorphism). Starting with the second 2 edge digraph we get one new digraph (up to isomorphism)

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

Starting with the third 2 edge digraph we get one new digraph (up to isomorphism)

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

This is a complete list up to three edges.

We want to restrict attention to matrices with nonzero row sums. There are only two such in our list so far.

Exercise 5 *Compute the page rank vector (invariant measure) for each of these two cases. (Take $p = .85$ or another appropriate value of your choice.)*

Exercise 6 *Continuing with the three vertex case, list a complete set of representative elements with 4 or more edges, such that the matrix row sums are all nonzero. Compute page rank for every element of your list. (Take $p = .85$ or another appropriate value of your choice.)*

Exercise 7 *Give an example of a model of the web with 8 pages in which you can easily compute page rank (and compute it!).*

In order to study and compute with finite state Markov processes in general, and with our applications in particular, we see that we need familiarity with basic matrix theory. Here is a quick review.

2.4 Elementary Matrix Theory

Consider the eigenvalue equation for matrix M

$$Mv = \lambda v$$

The set of eigenvalues is the set of roots of the *characteristic equation*

$$P_M(\lambda) := |M - \lambda \mathbb{I}| = 0$$

Two matrices A, B are *similar* if they are related by a similarity transformation, i.e.

$$A = M^{-1}BM$$

for some M.

Exercise 2.2. Show that two similar matrices have the same characteristic equation, and hence the same eigenvalues.

In particular the trace and determinant of a matrix are not changed by similarity transformation.

Theorem 2.3. *[Cayley–Hamilton]*

$$P_M(M) = 0$$

It follows that M^n can be expressed as a linear combination of lower powers of M.

2.4.1 Norms

Definition 2.4. A norm on a vector space V is a real function $||v \in V||$ such that $||v|| \geq 0$; $||v|| = 0 \Rightarrow v = 0$; $||kv|| = k||v||$; $||v + w|| \leq ||v|| + ||w||$.
Example 2.5. The Euclidean norm is the $r = 2$ case of $||v||_r = +\sqrt[r]{\sum_i |v_i|^r}$, and is a norm.

Definition 2.6. A matrix norm is a vector norm as above extended by the condition on conformable matrices M, N: $||MN|| \leq ||M||.||N||$.
Examples:

Definition 2.7. The Frobenius norm $||M||_F$ of a matrix M is defined by

$$||M||_F = +\sqrt{\sum_{i,j} |M_{ij}|^2} = +\sqrt{\text{Trace}((A^*)^t A)}$$

Exercise 2.8. (Optional) Show that the Frobenius norm is a matrix norm.

If $|| - ||$ is a vector norm on n-component column vectors then we get an 'induced' matrix norm on $n \times n$ matrices by

$$||M|| \quad = \quad \max_{||v||=1} \quad ||Mv||$$

(NB, you need to convince yourself that the maximum exists!).

The matrix norm induced from $|| - ||_2$ is called the matrix 2–norm. Assume for a moment that M is real. Then to determine $||M||_2$ we need to determine the maximum value of

$$f(v) = ||Mv||_2^2 = v^t M^t M v$$

subject to $g(v) := v^t v = 1$. Form

$$h = f - \lambda g$$

(Lagrange multipliers). The system got by differentiating wrt each v_i is

$$(M^t M - \lambda \mathbb{I})v = 0$$

so λ must be such that $(M^tM - \lambda\mathbb{I})$ is singular (i.e. $P_{M^tM}(\lambda) = 0$). Thus

$$v^t(M^tMv) = \lambda v^t v = \lambda$$

and

$$||M||_2 = \max_{||v||=1} ||Mv|| = \max_{||v||^2=1} ||Mv||$$
$$= +\sqrt{\max_{v^tv=1} v^tM^tMv} = +\sqrt{\lambda_{max}}$$

where λ_{max} is the biggest such λ. Of course this is just the biggest eigenvalue of M^tM.

Definition 2.9. The spectral radius of a square matrix M is

$$\rho(M) = \max_{\lambda \in S(M)} |\lambda|$$

where $S(M)$ is the set of eigenvalues of M.

2.4.2 Jordan form

Let $S(M) = \{\lambda_1, .., \lambda_r\}$ be the set of eigenvalues of M, with multiplicities n_i. Let U_n be the $n \times n$ matrix with all entries zero except for those immediately above the main diagonal.

$$U_3 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Then $J_n(\lambda) = \lambda\mathbb{I}_n + U_n$ is called a Jordan block. Every $n \times n$ matrix is similar to a matrix of form

$$AMA^{-1} = \bigoplus_j \bigoplus_i J_{n_{i,j}}(\lambda_j)$$

where $\lambda_j \in S(M)$ and $\sum_i n_{i,j} = n_j$.

For the study of Markov processes we are interested in the behaviour of (certain) matrices when raised to a high power. Let us start by considering Jordan blocks.

Exercise 2.10. Show that if $J_n(\lambda)$ is a Jordan block with $n \geq 2$ then $(J_n(\lambda)^k)_{11} = \lambda^k$ and $(J_n(\lambda)^k)_{12} = k\lambda^{k-1}$. Determine the complete form of the k-th power.

If $\lambda < 1$ the limit $\lim_{k\to\infty}(J_n(\lambda))^k$ is the zero matrix.
By the exercise above, the limit will not exist, indeed the matrix will diverge (certain entries grow bigger and bigger in magnitude as k increases) if $|\lambda| > 1$, or if $|\lambda| = 1$ and $n > 1$.
If $\lambda \neq 1$ while of unit magnitude and $n = 1$ then the diagonal term will oscillate, so that (although every power is finite) again there is no limit. The case $\lambda = 1$, $n = 1$ is obvious.

Note that for any transform A

$$AM^kA^{-1} = AMM^{k-1}A^{-1} = AMA^{-1}AM^{k-1}A^{-1} = (AMA^{-1})^k$$

Comparing these observations we see that $\lim_{k\to\infty} M^k$ will not exist unless $|\lambda_i| \leq 1$ for all i, and if $|\lambda_i| = 1$ for some k then $n_{ik} = 1$ for all i.

On the other hand, if M is stochastic then so is M^k for any k (in particular all entries remain in the probablistic interval). We deduce that a stochastic matrix has no eigenvalue with magnitude greater than 1. This is because, if M^k is finite then so is AM^kA^{-1} for any finite A, including the transform taking M (and hence also M^k) to Jordan form, so that if the Jordan form of M^k diverges (i.e. has entries of unboundedly large magnitude) we know M^k cannot be finite. By the same token we know that $n = 1$ in any Jordan block with $|\lambda| = 1$, so that each eigenvalue with magnitude 1 has an independent eigenvector associated to it.

2.5 The Perron–Frobenius Theorem

A matrix is *positive* if all its entries are positive.

The Perron–Frobenius theorem states that a finite positive matrix has a unique eigenvalue of largest magnitude, and this eigenvalue is positive; and

that this eigenvalue has an eigenvector with all positive entries. [3]

A matrix M is *positivizable* if M^n is positive for some natural number n. It will be evident that the theorem applies to such matrices.

Let us prove the theorem in the special case of a matrix M in which the row sums are 1. The idea of this proof will be to consider $\min_k M^n_{kj}$ and $\max_k M^n_{kj}$ and show that these converge to the same thing as n gets large (which would force M^n_{ij} to settle down to a value independent of i). First we show that $\min_k M^n_{kj}$ (which we may take as zero for $n = 0$) increases with n:

$$M^{n+1}_{ij} = \sum_k M_{ik} M^n_{kj} \geq \min_k M^n_{kj} \sum_k M_{ik} = \min_k M^n_{kj}$$

Similarly

$$\max_k M^{n+1}_{kj} \leq \max_k M^n_{kj}$$

Now impose that M is positive. Let $e > 0$ be the smallest M_{ij}. Then

$$M^{n+1}_{ij} = \sum_k M_{ik} M^n_{kj} = \sum_k [M_{ik} - e M^n_{jk}] M^n_{kj} \quad + e \sum_k M^n_{jk} M^n_{kj}$$

$$= \sum_k [M_{ik} - e M^n_{jk}] M^n_{kj} \quad + e M^{2n}_{jj}$$

$$\geq \min_k M^n_{kj} \sum_k [M_{ik} - e M^n_{jk}] \quad + e M^{2n}_{jj} = (1 - e) \min_k M^n_{kj} \quad + e M^{2n}_{jj}$$

Since the RHS doesn't depend on i we have

$$\min_k M^{n+1}_{kj} \geq (1 - e) \min_k M^n_{kj} \quad + e M^{2n}_{jj}$$

Similarly

$$\max_k M^{n+1}_{kj} \leq (1 - e) \max_k M^n_{kj} \quad + e M^{2n}_{jj}$$

and hence

$$\max_k M^{n+1}_{kj} - \min_k M^{n+1}_{kj} \leq (1 - e)(\max_k M^n_{kj} - \min_k M^n_{kj})$$

[3] A proof of this theorem can be found, for example, in P P Martin, Potts models and related problems in statistical mechanics, World Scientific 1991.

so the sequence of maxima and the sequence of minima have the same limit. Let us call it π_j. For any i

$$\min_k M^n_{kj} \leq M^n_{ij} \leq \max_k M^n_{kj}$$

so

$$M^\infty_{ij} = \pi_j > 0$$

independent of i.

We have a matrix of form

$$M^\infty = \begin{pmatrix} \pi_1 & \pi_2 & \pi_3 \\ \pi_1 & \pi_2 & \pi_3 \\ \pi_1 & \pi_2 & \pi_3 \end{pmatrix}$$

and

$$M^\infty M = M^\infty$$

so in particular

$$\begin{pmatrix} \pi_1 & \pi_2 & \pi_3 \end{pmatrix} M = \begin{pmatrix} \pi_1 & \pi_2 & \pi_3 \end{pmatrix}$$

giving us our invariant measure.

The trace of M^∞ is $\sum_i \pi_i = 1$. This is the sum of all eigenvalues of magnitude 1, but if there were any such eigenvalues not equal to 1 the limit would not exist. Indeed the rank of M^∞ is 1, so all it's eigenvalues except one have value zero.

Exercise 2.11. Find the eigenvalues and eigenvectors for each of the following:

$$\frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \qquad \frac{1}{4}\begin{pmatrix} 1 & 2 & 1 \\ 1 & 1 & 2 \\ 2 & 1 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & \\ & & & 1 \\ 1 & & & \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & \\ & & & 1 \\ 0 & 1 & & \end{pmatrix}$$

Chapter 3

Preliminaries

3.1 Sets

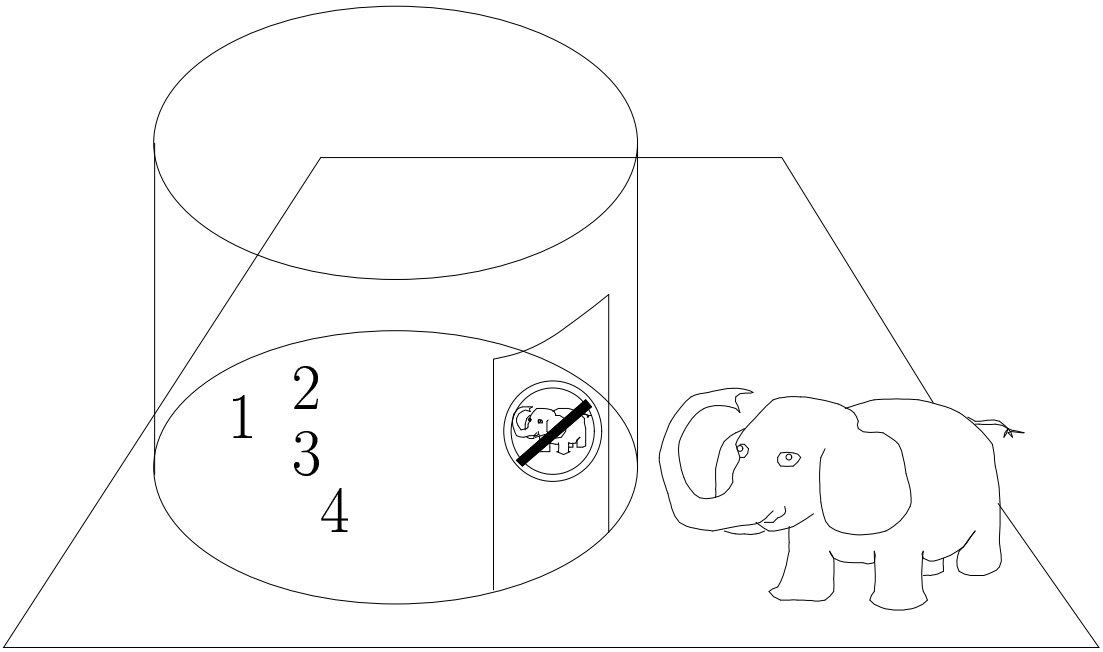
- A SET is a collection of objects.
- A specific set is 'defined' by any means which unambiguously tells us how to determine whether an arbitrary object is in the set or not.
- The objects in a set are called the ELEMENTS of the set. We write $x \in S$ in case x is an element of set S. We write $x \notin S$ otherwise.

Example 1 *Suppose we write* $S = \{1, 2, 3, 4\}$. *Then* S *is a set,* $1 \in S$, *and* $2 \in S$, *but* $5 \notin S$, *and of course* $[\mathfrak{My}\ \mathfrak{pet}\ \mathfrak{E}lephanT] \notin S$ *(see figure).*

Example 2 *Suppose* $T = \{x\ \textit{an integer} \mid x^2 < 27\}$. *This is another set (here* $\mid$ *means 'such that'). We have* $-1 \in T$, $6 \notin T$, $-6 \notin T$, $0 \in T$, *and so on.*

Example 3 *Suppose* $V = \{0, 1, 2, 3, 4, 5, -1, -2, -3, -4, -5\}$. *This is also a set. The order in which we write the elements in a set is not important.*

Definition 3.1.[SUBSET] A set S is a subset of a set T if and only if every element of S is an element of T.



A *mathematical notation* representation of this definition is:

$$S \subseteq T \iff (x \in S \Rightarrow x \in T).$$

Make sure you understand what each symbol means, and how to read this line as a sentence in ordinary language! For example, $\subseteq$ is the symbol for subset; $\iff$, also written *iff*, means 'if and only if'; and $\Rightarrow$ is the symbol for 'implies'. The brackets here are a guide to the eye, containing a statement within the sentence which is a composite of other statements.

Example 4 *Comparing S from example 1 and T from example 2 we see that $S \subseteq T$.*

Example 5 *Let $\mathcal{S}$ be the set of playing cards in a 52 card deck of playing cards. Then the set of all 'club' cards is a subset $\mathcal{S}_\clubsuit$ of $\mathcal{S}$. Suppose that a card dealer deals out the pack into 4 equal hands (i.e. 13 cards each). Each of these hands is a subset of $\mathcal{S}$.* What is the probability that one of these hands is $\mathcal{S}_\clubsuit$?

A set $S \subseteq T$ is called a PROPER subset of T (written $S \subset T$) provided at least one element of T is not in S.

We write $S = T$ if $S \subseteq T$ and $T \subseteq S$.

Example 6 *Comparing T from example 2 and V from example 3 we see that $T = V$.*

Exercise 8 *Write down five sets — call them S_1, S_2, S_3, S_4, S_5, say — with the property that $S_i \subset S_{i+1}$ for $i = 1, 2, 3, 4$ (i.e. $S_1 \subset S_2$, and so on).*

Exercise 9 *Show that for A, B, C sets, if $A \subset B$ and $B \subset C$ then $A \subset C$.*

The general procedure for solving this kind of problem is as follows:

State what is to be done in mathematical notation; *if* the solution is very long (not the case here, as we will see!) give a one sentence overview of your plan of attack; convert the known information into mathematical notation (expanding up all terms to their full definitions) and rearrange to achieve the required result....

Solution 9.1 *We need to show that $x \in A$ implies $x \in C$, and that there is some $y \in C$ such that $y \notin A$. Suppose that $A \subset B$ and $B \subset C$. Since $A \subset B$ then $x \in A$ implies $x \in B$. Further since $B \subset C$ then $x \in B$ implies $x \in C$. Altogether then $x \in A$ implies $x \in C$, which shows that $A \subseteq C$. But $A \subset B$ also implies that there exists $y \in B$ such that $y \notin A$, and since $y \in B$ implies $y \in C$ then $A \subset C$. QED.*

3.1.1 Sets built from other sets

In what follows, S, T are two sets:

Definition 3.2.[INTERSECTION] We define a new set, the 'intersection of S and T', written $S \cap T$, by

$$S \cap T = \{x | x \in S \text{ and } x \in T\}.$$

For example, if $S = \{1, 2, 4\}, T = \{1, 3, 4, 5, 6\}$, then $S \cap T = \{1, 4\}$.

The EMPTY set, denoted $\emptyset$, is the set containing no objects. For example,

$$\{1, 3, 5\} \cap \{2, 4, 6\} = \emptyset.$$

Definition 3.3.[DISJOINT] We say that two sets A, B are disjoint in case $A \cap B = \emptyset$.

Example 7 *Let W be the set of all those ancient Egyptian pyramids under whose northernmost foundation stone is hidden evidence that aliens once visited the Earth. It is true to say that there is a set E such that $W \supseteq E$, since $W \supseteq \emptyset$ and $W \supseteq W$. But is it true that there is a set E such that $W \supset E$?*

Definition 3.4.[UNION] We define a new set

$$S \cup T = \{x | x \in S \text{ or } x \in T\}.$$

N.B. The 'or' here is the *inclusive or*.

For example, if $S = \{1, 2, 4\}, T = \{1, 3, 4, 5, 6\}$, then $S \cup T = \{1, 2, 3, 4, 5, 6\}$.

Exercise 10 *Verify that $S \cup (T \cup V) = (S \cup T) \cup V$ for all sets S, T, V.*

From this exercise we see that we may speak unambiguously of the union of several sets (i.e. not just two sets).

Definition 3.5.[POWER SET] The power set of a set S, denoted $\mathcal{P}(S)$, is the set of all subsets of S.

Example 8 $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$. *Notice how careful one must be with the brackets for this to make any sense.*

In SET THEORY it is useful to have a notion of 'all possible objects' which might be collected together to form sets. Unfortunately this notion is really too vague as it stands. In practice we define a UNIVERSAL set U to be a set containing all possible objects *under discussion* (with the kind of object under discussion being determined, perhaps implicitly, by the context). We

usually specify a universal set *for a given problem* as some set which, at least, contains as subsets all the sets in which we are currently interested.

The COMPLEMENT of a set S (with respect to some such universal set U) is written S', and means the set of all objects in U NOT in S.

3.1.2 Cartesian product

Definition 3.6.[CARTESIAN PRODUCT] The Cartesian product of two nonempty sets S and T, written $S \times T$, is the set $S \times T$ given by

$$S \times T = \{(a, b) | a \in S \text{ and } b \in T\}$$

where $(a, b) \in S \times T$ is a constructed object made from the ordered pairing of a and b.

For example,

$$\{1, 2, 3\} \times \{x, y\} = \{(1, x), (1, y), (2, x), (2, y), (3, x), (3, y)\}.$$

Note that the order in which we write the pair $(1, x)$ (say) is important. This pair is a single element of the Cartesian product. The pair $(x, 1)$ is NOT an element of the Cartesian product in our example (but it would be an element of $\{x, y\} \times \{1, 2, 3\}$, so obviously $S \times T \neq T \times S$ in general!).

Example 9 *Let $H = \{A, 2, 3, 4, 5, 6, 7, 8, 9, 10, J, Q, K\}$ — the set of values on the cards in a 52 card deck of playing cards. Then the set $\mathcal{S}$ from example 5 may be written*

$$\mathcal{S} = H \times \{\clubsuit, \heartsuit, \spadesuit, \diamondsuit\}$$

where $(2, \clubsuit)$ represents the two of clubs, and so on. In this notation we might write $\mathcal{S}_\clubsuit = H \times \{\clubsuit\}$ (it might be safer to write $\cong$ instead of $=$, see later). We may similarly introduce $\mathcal{S}_\heartsuit = H \times \{\heartsuit\}$, and so on. Note that $\mathcal{S}_\heartsuit \cap \mathcal{S}_\clubsuit = \emptyset$; and $\mathcal{S}_\heartsuit \cup \mathcal{S}_\clubsuit \cup \mathcal{S}_\spadesuit \cup \mathcal{S}_\diamondsuit = \mathcal{S}$.

3.1.3 Aside on the subsets of the set of real numbers

We will discuss the topic of real numbers later, but in order to introduce some notation we here note that the set of real numbers, denoted $\mathbb{R}$, has a sequence of subsets:

$$\emptyset \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

Exercise 11 *Explain the meaning of each of these symbols.*

The set of NATURAL NUMBERS, denoted $\mathbb{N}$, satisfies *Peano's axioms*:
(a) $1 \in \mathbb{N}$;
(b) for each $n \in \mathbb{N}$ there exists a unique $n' \in \mathbb{N}$ called 'the successor of n', written $(n+1)$;
(c) 1 is not the successor of any $n \in \mathbb{N}$;
(d) if $n' = m'$ then $n = m$;
(e) if $S \subseteq \mathbb{N}$ and $1 \in S$ and if $n \in S$ implies $(n+1) \in S$, then $S = \mathbb{N}$.
Let us see what we get using these axioms:

$$\mathbb{N} = \{1, (1+1), ((1+1)+1), (((1+1)+1)+1), ((((1+1)+1)+1)+1), ...\}.$$

Of course we have a shorthand for this:

$$\mathbb{N} = \{1, 2, 3, 4, 5, ...\}.$$

Exercise 12 *Give an example of a set $\overline{\mathbb{N}}$ which satisfies all of Peano's axioms except axiom (c): 1 is not the successor of any $n \in \overline{\mathbb{N}}$.*

Solution 12.1 *Without this axiom we could allow, for example,*

$$(((((1+1)+1)+1)+1)+1) = 1.$$

Then

$$\overline{\mathbb{N}} = \{1, 2, 3, 4, 5\}$$

(and + doesn't have its usual meaning!).

We have lots more to say about sets and numbers. We will come back to them later.

3.2 Relations and Functions

Let S and T be nonempty sets. A RELATION from S to T is any subset of $S \times T$.

For example, if S is the set of Mathematicians, and T is the set of Statisticians, then we might define a relation ρ by writing

$$\rho = \{(a, b) \in S \times T | a \text{ is older than } b\}.$$

It is often convenient to write $a\rho b$ (and say 'a has the relation ρ with b', or 'a stands in relation ρ to b', or in this case simply 'a is older than b') in case $(a, b) \in \rho$.

Note in particular than in this example (and in general) $a\rho b$ does not imply $b\rho a$!

Suppose we have a relation $\rho \subseteq S \times T$. Then

Definition 3.7.[DOMAIN] The domain of ρ, written $dom\ \rho$, is the set of elements of S which appear as the left hand sides of pairs which are elements of ρ.

For example, if $\rho = \{(1, x), (2, x)\}$ then $dom\ \rho = \{1, 2\}$.

Definition 3.8.[RANGE] The range of ρ, written $ran\ \rho$, is the set of elements of T which appear as the right hand sides of pairs which are elements of ρ.

In our example, $ran\ \rho = \{x\}$.

Definition 3.9.[INVERSE] The inverse of ρ, written ρ^{-1}, is the set obtained by reversing the order of each pair in ρ.

In our example $\rho^{-1} = \{(x, 1), (x, 2)\}$.

Let ρ be a relation from S to T. Then it is also a relation from $dom\ \rho$ to T.

Exercise 13 *Show that ρ is also a relation from S to $ran\ \rho$.*

Solution 13.1 *This is an example of a simple kind of 'proof' of a claim, where we simply have to insert the definitions of the terms and rearrange a little:*

We have to show that $(a, b) \in \rho$ *implies* $b \in ran\ \rho$. *But the definition of* $ran\ \rho$ *says that it is the set of* all *right hand sides of such pairs, so certainly it includes this one!*

Exercise 14 (compulsory) *By similar means:*

1) Show that a relation ρ *is also a relation from dom* ρ *to any* Q *such that* $Q \supset ran\ \rho$.

2) Show that a relation ρ *is NOT a relation from dom* ρ *to any* P *such that* $P \subset ran\ \rho$.

Definition 3.10.[FUNCTION] A function is a relation in which each element of the domain appears exactly once as the left hand side of a pair.

Thus $\{(1, x), (2, x)\}$ is a function, but $\{(x, 1), (x, 2)\}$ is not. To generate some more examples let us consider $A = \{a, b, c, d\}$, $B = \{r, s, t, u, v\}$. Then:
(i) $\{(a, t), (c, r), (d, s), (c, v)\}$ is not a function from A to B because c appears twice;
(ii) $\{(a, u), (b, r), (c, s), (d, u)\}$ is a function;
(iii) $\{(a, c), (a, u), (b, s), (c, r), (d, t)\}$ is *not* a function;
(iv) $\{(a, u), (b, u), (c, u), (d, u)\}$ is a function;
(v) $\{(a, r), (b, s), (c, t), (d, u)\}$ is a function.

Recall that we can think of the set of real numbers $\mathbb{R}$ as the set of points on the x-axis of a Cartesian x, y frame. Then the set $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ may be represented by the points on the whole plane (i.e. with "coordinates" $(x, y) \in \mathbb{R}^2$). It follows that any subset of the points of the plane is a relation! In particular any line drawn on the plane gives a relation. We are familiar with the representation of functions from $\mathbb{R}$ to $\mathbb{R}$ by this means. On the other hand, we know that only certain lines drawn on the plane correspond to a function (an arbitrary scribble, while giving a perfectly good relation, would not normally be a function). You should compare your intuitive understanding of this with the definition above!

Since each element of the domain appears exactly once in a function, we have the opportunity for a new and neater notation. The right hand side

of each pair in the function is uniquely given by the left hand side. We can recognise this by writing the pair $(x, f(x)) \in f$, say. Of course we then often go on to specify the right hand side "as a function of" the left hand side explicitly, arriving at the more familiar notation for functions, for example:

$$f(x) = 1 + x^2.$$

Altogether we give the concrete definition of a specific function as follows. First we specify the name of the function, and the domain, and the CODOMAIN (which is any set containing the range - this definition may seem rather arbitrary at first, but it is quite convenient, as we will soon see). For example if f is the function, A is the domain and $B \supseteq ran\ f$ we write

$$f : A \to B$$

and say "the function f maps the set A into the set B". Then we write

$$f : x \mapsto f(x)$$

which means that the action of f on a specific element $x \in A$ is to take it to $f(x) \in B$. In practice at this point we may be able to give $f(x)$ explicitly. For example we might write, altogether,

$$f : \mathbb{R} \to \mathbb{R}$$

$$f : x \mapsto x^3 + 3x - 2.$$

This may seem like a lot of fuss over nothing! It isn't, and you should take care to study it very carefully. There will be examples shortly. First, here are some refinements:

Definition 3.11.[ONTO] A function $f : A \to B$ is called onto (or SURJECTIVE) if $ran\ f = B$.

Note that examples (ii),(iv) and (v) above are NOT onto.

Definition 3.12.[ONE-TO-ONE] A function is one-to-one (or INJECTIVE) if

$$(\ (a, b) \in f \ \text{ and } \ (a', b) \in f\ ) \ \text{ implies } \ a = a'.$$

That is, distinct elements in A have distinct "images" in B ($f(a) \in B$ is called the "image of a under f"). Note that examples (ii) and (iv) above are not one-to-one, but that example (v) is one-to-one.

A function which is not one-to-one is called MANY-TO-ONE.

Definition 3.13.[BIJECTION] A function which is both one-to-one *and* onto is called a bijection.

Exercise 15 *Give three examples of bijections.*

There are various useful pictorial representations of functions. These will be discussed in class.

Definition 3.14.[IDENTITY FUNCTION] For each set A there is a function from A to A, called the identity function, denoted 1_A, and given by

$$1_A : A \to A$$

$$1_A : a \mapsto a.$$

Two functions h and g are said to be EQUAL (written $h = g$) if they have the same domain and codomain, and $h(x) = g(x)$ for all x in the domain. For example, if h, g are two functions from $\mathbb{R}$ to $\mathbb{R}$ given by $h(x) = x + x$ and $g(x) = 2x$, then $h = g$.

The *restriction* of a function f to a subset of the domain is the function on that subset obtained by applying f to it.

3.2.1 Composition of functions

Let $f : A \to B$ and $C \supseteq ran\ f$ and $g : C \to D$. Then

Definition 3.15.[COMPOSITE FUNCTION] The composite function $g \circ f$ is defined by

$$g \circ f : A \to D$$

$$g \circ f : a \mapsto g(f(a)).$$

We write $(g \circ f)(a) = g(f(a))$.

For a relation ρ we understand $\rho(a)$ to be the *set* of objects b such that $a\rho b$. For S a subset of the domain of ρ we understand $\rho(S)$ to be the union of sets $\rho(s)$ over every $s \in S$. Relations are then composable in much the same way as functions.

Although every relation has an inverse (and hence every function has an inverse *as a relation*), not every function has an inverse which is itself a function.

Exercise 16 *Show that the inverse of a function is a function if and only if the function is a bijection.*

Exercise 17 *For $f : A \to B$ a bijection, show that*

$$f \circ f^{-1} = 1_B$$

and

$$f^{-1} \circ f = 1_A.$$

3.2.2 Permutations

If the number of elements in a set is a natural number (i.e. if it is finite, since then it is certainly a non-negative whole number!) then the set is called a finite set. For example, $A = \{a, b, c, d, e, f, g\}$ is a finite set, as it has 7 elements; meanwhile $\mathbb{R}$ is not a finite set. We will return to this point later.

Definition 3.16.[ORDER] The order (or degree) of a finite set A, denoted $|A|$, is the number of elements in the set.

Denoting the set of all finite sets by F, then the 'order' operation is a function

$$\text{Order} : F \to \mathbb{N}$$

i.e.

$$\text{Order} : A \mapsto |A|.$$

For example, if $B = \{a, b, c, d\}$ then $\text{Order}(B) = |B| = 4$.

Definition 3.17.[PERMUTATION] A bijection $f : A \to A$ on a finite set A is called a permutation of A.

For example, if $S = \{1, 2, 3, 4\}$ then f given by $f(1) = 2$, $f(2) = 3$, $f(3) = 4$, $f(4) = 1$ is a permutation. Permutations may be written in the form

$$\begin{pmatrix} a & b & c & ... & x \\ f(a) & f(b) & f(c) & ... & f(x) \end{pmatrix}.$$

This one then becomes

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

Exercise 18 *Verify that any $f : A \to A$ is 1–to–1 if and only if it is onto.*

Let A be a finite set of degree n, and f be a permutation of A. If repeated composition of f with itself produces the identity function after $|A|$ compositions and not before (or, equivalently, if for any $x \in A$ we have that $\{x, f(x), (f \circ f)(x), (f \circ (f \circ f))(x), ...\} = A$) then the permutation is called a CYCLE of A, or n–CYCLE. More generally, if f restricts to a cycle of B for some $B \subset A$, and acts as $f(x) = x$ for all $x \notin B$, then f is a $|B|$–cycle. (Note that there are no permutations of A which are p-cycles with $p > n$.)

Exercise 19 *Show that the f defined in the example above is a cycle. Give an example of a bijection $g : S \to S$ which is not a cycle.*

Exercise 20 *Let A be the set of letters in the alphabet, together with the hyphen symbol – (so $|A| = 27$). Let A' be the subset of these symbols occuring at least once in the word* gerbil–brain. *Write down A'.*

Let $f : A' \to \mathbb{N}$ be the alphabetical ordering of these symbols (so $f(a) = 1$, $f(b) = 2$, $f(e) = 3$, and so on) with $f(-) = 9$. Note that $|ran\ f| = 9$. What is the word obtained by applying the inverse of f to the sequence of elements of ran f given by 1653791643281?

3.3 Equivalence Relations

Let ρ be a relation from set A to A (i.e. $\rho \subseteq A \times A$). Then

Definition 3.18.[REFLEXIVE/SYMMETRIC/TRANSITIVE] .

1. ρ is reflexive if and only if $a\rho a$ for all $a \in A$.
2. ρ is symmetric if and only if whenever $a\rho b$ then $b\rho a$.
3. ρ is transitive if and only if whenever ($a\rho b$ and $b\rho c$) then $a\rho c$.

Examples:

$\rho =$ "belongs to the same family as" is reflexive, symmetric and transitive;

$\rho =$ "is an ancestor of" is transitive;

$\rho =$ "is the mother of" is none of these!

Definition 3.19.[EQUIVALENCE RELATION] A reflexive, symmetric, transitive relation is an equivalence relation.

Such a relation is often written $\sim$ (as in $a \sim b$) unless it already has a name.

For specific relations, we usually define a pair, consising of the set A together with its equivalence relation: $(A, \sim)$. Thus we have:

(1) $(\mathbb{N}, =)$ given by $a\rho b$ if and only if $a = b$;

(2) $(\mathbb{Z}, \sim)$ given by $a \sim b$ if and only if $5|(a-b)$ (here we have introduced the following

Definition 3.20.[DIVIDES] For $n, m \in \mathbb{Z}$ we say p divides m, and write $p|m$ (*not* to be confused with p/m), in case the equation $m = pn$ is solved by some $n \in \mathbb{Z}$.

for example here $11 \sim 1$ (i.e. $5|(11-1)$) since $11 - 1 = 5.2$ - see later). Let's check these:

In (1) we have $a = a$ for any number a, so the relation is reflexive; if $a = b$ then certainly $b = a$, so it is symmetric; and if $a = b$ and $b = c$ then $a = c$, so transitive;

(2) is more of a challenge, we have $(a - a) = 0$ and $5|0$, so reflexive; we have $(a-b) = -(b-a)$, so if $5|(a-b)$ then $5|(b-a)$, so symmetric; and finally

if $(a-b)=5k$ (say) and $(b-c)=5l$ (with $k,l\in\mathbb{Z}$) then $(a-c)=5(k-l)$, so transitive!
The relation (2) is sometimes written $a\equiv b$ (mod.5).

3.3.1 Equivalence classes

Definition 3.21.[EQUIVALENCE CLASS] Given a pair $(A,\sim)$ we define the equivalence class containing $a\in A$ to be the set

$$[a]=\{x\in A\ :\ x\sim a\}.$$

Note that $[a]\subseteq A$; $a\in[a]$; and if $b,c\in[a]$ then $a\sim b, c\sim a$ and indeed $b\sim c$ (i.e. *any* two elements of the same class are equivalent).

Theorem 3.22.*[On equivalence classes] Let $\sim$ be an equivalence relation on a set A and let $[a]$ be the equivalence class of $a\in A$. Then for any $a,b\in A$*

(i) $[a]=[b]$ if and only if $a\sim b$;

(ii) if $[a]\neq[b]$ then $[a]\cap[b]=\emptyset$.

Proof: The theorem may be broken into three parts. Firstly, the 'if' part of (i):

We can write this part $[a]=[b]\Leftarrow a\sim b$, so this is what we need to show. In other words we must show that if we *assume* $a\sim b$, then $[a]=[b]$ follows, so.... Let $a\sim b$. Then by definition $a\in[b]$. Then again, $[a]\subseteq[b]$, since if $x\in[a]$ then $x\sim a$, but $a\sim b$ and so by transitivity $x\sim b$, that is $x\in[b]$. Similarly $[b]\subseteq[a]$, so finally $[a]=[b]$.
Now the 'only if' part of (i) (i.e. to show $[a]=[b]\Rightarrow a\sim b$):

If $[a]=[b]$ then since $b\sim b$ we have $b\in[a]$ and so $b\sim a$;
Lastly, part (ii):

We will prove this by CONTRADICTION. This means we assume the *opposite* to what is required, and prove this must be false (if the opposite is false, then logically the statement itself must be true). The trick here is to figure out what the opposite of the statement is! This is not always obvious, but in our case the opposite would be:

a and b can be found such that $[a] \neq [b]$ but $[a] \cap [b] \neq \emptyset$.

Let's assume *this* statement true, and see what happens. Consider such an a and b, and consider any $x \in [a] \cap [b]$. If it exists (the last ingredient of the statement says it does!) then this means $x \sim a$ and $x \sim b$. This then implies $a \sim b$ by symmetry and transitivity. But part (i), which is already proved, says that *this* can only happen when $[a] = [b]$ — a contradiction between the consequences of the first and second ingredients of the statement. The only resolution is that there can be no such x — that is, $[a] \cap [b] = \emptyset$. QED.

There will be more examples of this kind of proof shortly.

Definition 3.23.[PARTITION] Given a set A, if there exists a set I and a collection of nonempty subsets $\{X_i \mid i \in I\}$ of A such that

(i) $x \in A$ implies $x \in X_i$ for some $i \in I$;

(ii) $X_i \cap X_j = \emptyset$ unless $i = j$,

then the collection $\{X_i \mid i \in I\}$ is said to form a partition of A.

So BY THEOREM 1 an equivalence relation $\sim$ on a set A defines a partition of A into its equivalence classes.

Example 10 $(\mathbb{Z}, \sim)$ *where* $a \sim b$ *iff* $(a - b)$ *divisible by 5.*

We have

$$[0] = \{...., -10, -5, 0, 5, 10, 15, ...\}$$

$$[1] = \{...., -9, -4, 1, 6, 11, 16, ...\}$$

$$[2] = \{...., -8, -3, 2, 7, 12, 17, ...\}$$

and $[3], [4]$ *similarly (exercise). Altogether there are five classes partitioning the integers* $\mathbb{Z}$. *Sometimes we write these classes simply as* $0, 1, 2, 3, 4$ *'modulo 5' (or mod 5). Note that* $[0] = [5] = [10] = ...$, *and* $[3] = [8] = [13] = ...$ *and so on.*

The SET OF EQUIVALENCE CLASSES here has five elements and is written $\mathbb{Z}_5$ - sometimes called the set of 'residues' mod 5.

We can do 'mod 5' arithmetic, as in

$$4 + 3 = 2 \qquad mod\ 5.$$

This makes sense in as much as the sum of any element of [4] with any element of [3] is always some element of [2]. (For example $9 + 8 = 17$. Now check it in the general case!). Multiplication also works on residues, in a similar way (check it!).

This can be done for residue classes modulo any integer. For example we have a complete arithmetic 'mod 3':

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

.

Special things happen when the integer is *prime* as here. See later.

Conversely, given a partition of A we can define an equivalence relation on A by $a \sim b$ iff a, b belong to the same set X_i of the partition. For example: Let $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 0\}$ with partition $\{1, 2, 0\}, \{3\}, \{4, 5, 7\}, \{6, 8\}, \{9\}$; then the corresponding equivalence relation is

$$\{(1,1),(2,2),(3,3),(4,4),(5,5),(6,6),(7,7),(8,8),(9,9),(0,0),(1,2),(2,1),(1,0),$$

$$(0,1),(2,0),(0,2),(6,8),(8,6),(4,5),(5,4),(4,7),(7,4),(5,7),(7,5)\}.$$

3.4 Countability

Consider the collection A of all sets. (We could say the set of all sets. This is a potentially dangerous notion — see [Cohn] on *Russell's Paradox* — but the dangers need not concern us here.) For X, Y sets let $X \sim Y$ iff there exists a bijection $f : X \to Y$. Note

(i) $1_X : X \to X$, so $\sim$ is reflexive;

(ii) If $f : X \to Y$ is a bijection, then $f^{-1} : Y \to X$ is a bijection, so $\sim$ is symmetric;

(iii) $f : X \to Y$ and $g : Y \to Z$ bijections implies $(g \circ f) : X \to Z$ is a bijection, so $\sim$ is transitive.

Altogether then, we have an equivalence relation.

In some sense (and precisely for the finite sets) each equivalence class contains all the sets with the same 'number of elements'.

For a set A the equivalence class $[A]$ is written $Card\ A$ ('Cardinal A'). $Card\ A = Card\ B$ iff A, B are 'numerically equivalent'.

For *finite* sets the equivalence class of all sets containing n elements is sometimes written simply as n. This n is called a 'cardinal number' (in general such numbers are the numbers associated with set sizes - but the finite cardinal numbers are the natural numbers $n \in \mathbb{N}$).

A set in $Card\ \mathbb{N}$ is called COUNTABLY INFINITE. A *countable set* is either finite or infinite. A set is countable, it 'can be counted', if when one sets out to count the elements (i.e. assign a distinct number to each of them from 1,2,3,...) there is a way of doing this such that any given element of the set eventually gets counted. N.B. This is not the same as saying that *all* the elements will be counted in finite time. $Card\ \mathbb{N}$ is sometimes denoted $\aleph_0$ ('aleph zero').
Example:

$$E = \{2, 4, 6, 8, 10, 12, ...\} \subset \mathbb{N}$$

what is the cardinality of E? Well,

$$f : \mathbb{N} \to E$$

$$f : x \mapsto 2x$$

is a bijection (check it!), so $Card\ E = \aleph_0$.

Obviously $\aleph_0$ is not any finite cardinal number. In a sense it is *bigger*. In a similar sense, as we will see shortly, there are still bigger infinite numbers (i.e. there are infinite sets too big to have a bijection with $\mathbb{N}$)! We call $\aleph_0$ a TRANSFINITE NUMBER. We have the following transfinite arithmetic:

$$2\ \aleph_0 \quad = \quad \aleph_0$$

(since naively we threw away half the elements of $\mathbb{N}$ to get E, and yet it didn't change the cardinality)

$$\aleph_0 + \aleph_0 = \aleph_0$$

$$\aleph_0 + 1 = \aleph_0$$

....so, is every infinite set countable? Well, what sets do we know which are bigger than $\mathbb{N}$? Obviously we have the rational numbers - even the set $\mathbb{Q}_+$ of positive rational numbers obeys $\mathbb{Q}_+ \supset \mathbb{N}$, but in fact:

Proposition 3.24. *Card* $\mathbb{Q}_+ = \aleph_0$

Proof: We will list the elements of $\mathbb{Q}_+$ in such a way that a bijection with $\mathbb{N}$ (i.e. a way of 'counting' the elements such that any given element is eventually counted) can be explicitly given.

We organise the elements of $\mathbb{Q}_+$ as follows:

$$1/1 \quad 1/2 \quad 1/3 \quad 1/4 \quad 1/5 \quad ...$$

$$2/1 \quad 2/2 \quad 2/3 \quad 2/4 \quad 2/5 \quad ...$$

$$3/1 \quad 3/2 \quad 3/3 \quad 3/4 \quad 3/5 \quad ...$$

$$...$$

(here many elements are counted more than once, but at least we can be sure that eventually any given element does appear on the grid). Now suppose we consider an arbitrary element, which is of the form $x = p/q$ by definition. Each South-East diagonal of the grid gives all the numbers with fixed $p + q$. We will count through the grid starting from the top left and then counting up each such diagonal in turn (i.e. running through the diagonals in order $p + q = 2, 3, 4, 5, ...$). That is, our bijection will be:

$$f(1/1) = 1$$

$$f(2/1) = 2$$

$$f(1/2) = 3$$

$$f(3/1) = 4$$

(2/2 has already been counted as 1/1)

$$f(1/3) = 5$$

$$f(4/1) = 6$$

and so on. QED.
You should check that you *understand* how the one-to-one and onto conditions are satisfied here.
Corollary 3.25.*[Exercise] Card* $\mathbb{Q} = \aleph_0$.

3.4.1 Uncountability

So we still havn't found any bigger 'numbers' than $\aleph_0$, even though $\mathbb{Q}$ contains $\mathbb{N}$ and much much more. What about the even bigger set $\mathbb{R}$?
Proposition 3.26. *Card* $\mathbb{R} \neq \aleph_0$.

Proof: We will prove the proposition by contradiction! In other words we will assume that $\mathbb{R}$ is countable, and prove that this must be wrong.

If we assume that $\mathbb{R}$ is countable then any subset must also be countable (if every element can be counted, then every element of a subset can be counted). Let us consider the set $(0, 1) \subset \mathbb{R}$, which is the set of real numbers between 0 and 1. Our assumption implies that $(0, 1)$ is countable, so that each $x \in (0, 1)$ may be numbered distinctly by some function f, a bijection onto the natural numbers. Since it is a bijection it has an inverse f^{-1}, i.e. for each natural number n there is a unique real number $f^{-1}(n)$ in the interval $(0, 1)$.

Now consider an $x \in (0, 1)$ written in decimal form. This form may be familiar to you. For example $x = .7 = .70000...$ (recurring 0s) or $x = .76582342222....$ (recurring 2s), or $x = \pi - 3 = .1415926...$ (no recuring pattern!). Note that to avoid duplicating values x we can avoid recurring 9s. To see why recurring nines are redundant consider, say, .79999... (recurring

9s) and .80000... (recurring 0s). The calculation $9 \times .79999... = (10 \times .79999...) - .79999... = 7.9999... - .79999... = 7.2$ shows that $.79999... = .8$. Now consider a particular decimal

$$y = .a_1 a_2 a_3 a_4 ....$$

(e.g. $y = .2343479....$, so each $a_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$). Suppose that for all i, the i^{th} decimal place - a_i - is chosen to be *different from* the i^{th} decimal place of the real number $f^{-1}(i)$. For example a_1 is different from the first decimal place of $f^{-1}(1)$; a_2 is different from the first decimal place of $f^{-1}(2)$; and so on.

By this construction y differs from each and every element of the list of images of f^{-1} in at least one decimal place. But of course if two numbers are the same then (excluding the situation with recurring 9) they must be the same in every decimal place, so y is actually a different number from each and every element of the list. But it is of the form $y = .a_1 a_2 ....$, so certainly $y \in (0, 1)$. But then f^{-1} is not onto, so it is not a bijection, so neither is f, which is then a CONTRADICTION of the original assumption.

We conclude that the assumption must be wrong, that is $(0, 1)$ is 'uncountable'. Then $\mathbb{R}$ is uncountable. QED.

Now we can introduce a new 'number': $Card\ \mathbb{R}$, which is often written C for 'continuum'.

This raises some intriguing questions. For example: Are there any cardinal numbers 'between' $\aleph_0$ and C? Are there numbers bigger than C? The mathematician CANTOR has thought a lot about these problems, with limited success. For the first question we have 'Cantor's continuum hypothesis', in which he claims that there are no cardinal numbers between $\aleph_0$ and C. What do you think?.....

For the second question - let us recall the notion of power set $\mathcal{P}(S)$ - the set of all subsets of S.

Exercise 21 *Verify that for finite sets*

$$|\mathcal{P}(S)| = 2^{|S|}.$$

In general considering $Card\ \mathcal{P}(S)$ (which we may abuse notation to write as $2^{Card\ S}$) is a reasonable way of trying to generate new cardinals. Cantor proved that $Card\ \mathcal{P}(S) > Card\ S$ continues to hold for transfinite numbers, so there exist infinitely many transfinite cardinals:

$$\aleph_0, 2^{\aleph_0}, 2^{2^{\aleph_0}}, ...$$

Exercise 22 (Difficult) *Prove that* $Card\ \mathcal{P}(\mathbb{N}) = 2^{\aleph_0} = C$.

Definition 3.27.[$\aleph_1$] We define $\aleph_1$ to be the next bigger cardinal after $\aleph_0$. This raises the question: Is $\aleph_1 = C$? What do you think?...

3.5 Orderings

Let P be a non-empty set.

Definition 3.28.[Partial Order Relation] A partial order relation on P, usually written $\leq$, is a relation with the following properties:

(i) $x \leq x$ for all $x \in P$ (reflexivity);

(ii) $x \leq y$ and $y \leq x$ implies $x = y$ ('anti-symmetry');

(iii) $x \leq y$ and $y \leq z$ implies $x \leq z$ (transitivity).

Then the pair $(P, \leq)$ is called a partially ordered set, or just a poset for short.

Examples:

(1) $(\mathbb{N}, \leq)$ where $\leq$ means 'less than or equal to' is a poset.

(2) $(\mathbb{N}, <)$ is NOT a poset (it fails reflexivity test).

(3) $(\mathbb{Z}, a$ divides $b)$ is NOT a poset (1 divides -1, and -1 divides 1).

(4) $(\mathbb{N}, a$ divides $b)$ is a poset.

(5) For X any set then $(\mathcal{P}(X), \subseteq)$ is a poset.

Let us check this one:

Reflexivity: $A \subseteq A$ for any set A, so OK.

Anti-symmetry: $A \subseteq B, B \subseteq A$ implies $A = B$, again for any two sets.

Transitivity: $A \subseteq B, B \subseteq C$ implies $A \subseteq C$, so OK.

(6) For X a nonempty set, the set of all real valued functions $f : X \to \mathbb{R}$, with relation $f \leq g$ iff $f(x) \leq g(x)$ for all $x \in X$, is a poset.

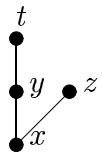
3.5.1 Diagrammatic representation of posets: Hasse diagrams

In a Hasse diagram we take advantage of the definition to represent a poset as follows. We draw a 'node' or spot for each element of the set, and a bond between nodes x and y (say) if either $x \leq y$ or $y \leq x$ (if there is some z such that $x \leq z \leq y$ we only draw bonds between x and z and between z and y, since this automatically creates a connection for us between x and y). We draw y ABOVE x on the page if $y \geq x$.

For example: (1) $S = \{x, y\}$ with $x \leq y$ then the diagram is

where $x \leq x$ and $y \leq y$ are to be understood implicitly.

(2) $S = \{x, y, z, t\}$ with $x \leq y, y \leq t, x \leq z$ (and $x \leq x, y \leq y, z \leq z, t \leq t$ and $x \leq t$ implicitly) is



We will give some more examples in the lecture.

Definition 3.29.[Comparability] In a poset $(P, \leq)$ two elements $x, y \in P$ are said to be comparable iff $x \leq y$ or $y \leq x$ (i.e. if joined in the Hasse diagram).

For example, in $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$ the elements $\{1\}$ and $\{2\}$ are NOT comparable, but $\{1\}$ and $\{1, 2\}$ are comparable.
Then again in $(\mathbb{N}, m$ divides $n)$ we have that 4 and 6 are not comparable but 3 and 6 are comparable.

Definition 3.30.[Total Ordering] A poset in which every pair of elements is comparable is called a total ordering, or a linear ordering, or a CHAIN.

For example $(\mathbb{N}, \leq)$ is a chain; $(\mathcal{P}(X), \subseteq)$ is not a chain; and $(\mathbb{N}, a$ divides $b)$ is not a chain.

A linear ordering $\leq$ on a set P in which every non-empty subset has a LEAST ELEMENT (i.e. an element l such that $l \leq x$ for all x in the subset) makes $(P, \leq)$ a WELL ORDERED SET.

Proposition 3.31.*[Exercise]*

1. $(\mathbb{N}, \leq)$ *is well ordered.*
2. *Every finite chain is well ordered.*
3. $(\{x \in \mathbb{Q} \ : \ x \geq 0\}, \leq)$ *is NOT well ordered.*

Definition 3.32.[BOUNDEDNESS] A poset $(P, \leq)$ in which there exists an element, $\bot$ (say), such that $\bot \leq x$ for all $x \in P$, and an element, $\top$ (say), such that $x \leq \top$ for all $x \in P$ is said to be BOUNDED.

For example:

1. $(\mathcal{P}(S), \subseteq)$ is bounded (even when S is infinite). Exercise: What are $\bot$ and $\top$ here?

2. $(\{1, 2, 3, 4, 6, 9\}, a$ divides $b)$ has no $\top$, so is not bounded (exercise: draw the diagram).

Definition 3.33.[MAXIMAL/MINIMAL ELEMENTS] In a poset $(P, \leq)$ an element $x \in P$ is MAXIMAL iff $y \geq x$ implies $y = x$ (i.e. x is not $\leq$ any *other* element).

Similarly for MINIMAL elements.

e.g.1. in $(\{1, 2, 3, 4, 6, 9\}, a$ divides $b)$ the elements 4,6,9 are maximal.

e.g.2. in a bounded poset $\top$ (also called 'the top element') is the unique maximal element, and $\bot$ (also called 'the bottom element') is uniquely minimal.

Definition 3.34.[LOWER BOUND] In $(P, \leq)$ let A be a nonempty subset of P. Then $x \in P$ is a LOWER BOUND of A if $x \leq a$ for all $a \in A$.

Definition 3.35.[GREATEST LOWER BOUND / INFIMUM] With A as above, x is a GLB (or 'inf') of A if $x \geq$ every lower bound of A.

Exercise 23 *If $inf\ A$ exists it is unique. Prove it!*

Similarly, y is an UPPER BOUND of A if $y \geq a$ for all $a \in A$, and y is a LEAST UPPER BOUND (or SUPREMUM, or 'sup') if it is $\leq$ every upper bound of A.

Example: $(\mathbb{N}, \text{is a factor of})$ - let $A = \{4, 6\}$, then 12,24,36,... are all upper bounds for A; 1,2 are lower bounds.

Sup $A = 12$ (Lowest Common Multiple (LCM) of 4 and 6)

Inf $A = 2$ (Highest Common Factor (HCF) of 4 and 6).

Proposition 3.36.*[Zorn's Lemma (see later)] A poset P in which every chain has an upper bound has a maximal element.*

There are some more advanced notes on posets (specifically on LATTICES) to be found in the version of these notes published on the maths web pages. Of course, looking at these additional notes is optional.

3.6 Sets with Binary Operations

A (closed) binary operation $*$ on a non-empty set S is a function

$$* : S \times S \to S.$$

If $*((x, y)) = z$ we usually write $x * y = z$.

Note that $x * y$ is defined for all $x, y \in S$ and that $x * y = z \in S$.

Examples:

1. $(\mathbb{N}, +)$, i.e. the natural numbers with operation given by addition;
2. for L a lattice both $(L, \vee)$ and $(L, \wedge)$ give binary operations;
3. $(\mathbb{N}, \times)$, ...muliplication of natural numbers is closed;
4. $(\mathbb{N}, -)$ is NOT closed (here $* : \mathbb{N} \times \mathbb{N} \to \mathbb{Z}$, since, for example, $3 - 4 = -1 \notin \mathbb{N}$), and:
5. $(\mathbb{Z}, -)$: $-$ on $\mathbb{Z}$ is a closed binary operation.

Definition 3.37.[ASSOCIATIVITY] An operation $*$ on S is associative iff

$$(x * y) * z = x * (y * z)$$

for all $x, y, z \in S$.

For example addition in $\mathbb{N}$ is associative:

$$(1+2)+5 = 1+(2+5)$$

(note that this *example* does not constitute a *proof* of associativity on its own), but subtraction is not associative:

$$(1-2)-5 \neq 1-(2-5).$$

With assocative operations we usually write just xyz for $x*(y*z)$.

Definition 3.38.[COMMUTATIVITY] A binary operation $*$ is commutative iff

$$(x*y) = (y*x).$$

For example $1+3 = 3+1$ (and so on), $a \wedge b = b \wedge a$, but $2-3 \neq 3-2$. We DO NOT assume commutativity.

Definition 3.39.[IDENTITY] The pair $(S, *)$ has a (two sided) identity (usually denoted by e) iff there exists $e \in S$ such that for all $x \in S$

$$e*x = x*e = x.$$

Proposition 3.40. *If $*$ is a closed binary operation with identity then the identity is unique.*

Proof: Assume e, f two identities, then $f = e*f = e$ by definition. QED! Examples:

1. in $(\mathbb{Z}, +)$ the identity is $e = 0$;
2. in $(\mathcal{P}(X), \cup)$ then $e = \emptyset$;
3. in $(\mathcal{P}(X), \cap)$ then $e = ?$ (exercise);

Definition 3.41.[IDEMPOTENT] Any $x \in S$ obeying $x*x = x$ is called an idempotent.

Definition 3.42.[INVERSES] Let $(S, *)$ be a set with a closed binary operation and identity e. An element y is an inverse of x iff $x*y = e = y*x$ (so x is also an inverse of y).

Examples: $(\mathbb{Z}, +)$, inverse of 3 is -3;

$(\mathbb{Q}, \times)$, 1 is the identity and the inverse of 3 is $1/3$.

Proposition 3.43. *For a closed associative binary operation $(S, *)$ with identity e, if x has an inverse then the inverse is unique.*

Proof: Let y, z be inverses of x. Then $x * y = e$ and $z * x = e$ so

$$(z * x) * y = e * y = y$$

and

$$z * (x * y) = z * e = z$$

so $y = z$ by associativity. QED.

As a notation, if we write xy for $x * y$ then we write x^{-1} for the inverse of x.

3.6.1 Groups

Definition 3.44.[GROUP] A group $(G, *)$ is a set G with a closed associative binary operation $*$ such that:

1. there exists an (unique) identity;
2. there exists an (unique) x^{-1} for each $x \in G$.

Examples: $(\mathbb{Z}, +)$ is a group;

$(\mathbb{Q}, \times)$ is NOT a group (0 has no inverse); but $(\mathbb{Q} - \{0\}, \times)$ is a group;

$(L, \vee)$ is not a group.

Definition 3.45.[ABELIAN] A group $(G, *)$ with $*$ commutative is called a commutative or abelian group.

Such groups are often written $(G, +)$ even though the operation may not be the usual addition (but in particular $(\mathbb{Z}, +)$ is abelian).

$(\mathbb{Z}_3, +)$ is an abelian group (see the table at the end of section 4), but $(\mathbb{Z}, \times)$ is not a group (because 0 does not have an inverse, again see the end of section 4);

Proposition 3.46. *Let S_n be the set of permutations of a set A consisting of n objects (recall, from definition 18, that this is the set of bijections f :*

$A \to A$), and let $\circ$ be the binary operation given by composition of functions, then $(S_n, \circ)$ is a group.

Proof: We have to check that the operation is closed and associative, that there is an identity, and that each element has an inverse.

Firstly, the composition of two bijections from A to A is a bijection from A to A, so we have closure. Secondly

$$f \circ (g \circ h) : A \to A$$

is given by

$$f \circ (g \circ h)x :\mapsto f(g(h(x)))$$

as is $(f \circ g) \circ h$, so we have associativity. The bijection 1_A acts as the identity, and since the functions are bijections they all have inverses as functions which also serve as their group inverses. QED.

Proposition 3.47.*[Exercise] The group $(S_3, \circ)$ is not abelian.*

Definition 3.48.[SUBGROUP] Let $(G, .)$ be a group. Then $(H, .)$ is a subgroup of G iff $H \subset G$ and $(H, .)$ is a group.

Example: Consider the group $(S_3, \circ)$. The set S_3 consists of elements which we can write (as in section 3.2):

$$1_A = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \; ; a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \; ; b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$a \circ b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \; ; b \circ a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \; ; a \circ (b \circ a) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

This is the complete list, since the bottom rows should give all possible permutations of the list $1, 2, 3$, of which there are 6 possibilities (i.e. 3!=3.2.1 possibilities). As an exercise you should check, for example, that $b \circ (a \circ b)$ doesn't give anything new (i.e. check closure).

We have labelled the identity element 1_A, as appropriate. The identity element MUST appear as an element of any subgroup (since the subgroup is also a group). In fact the smallest subgroup would be $(\{1_A\}, \circ)$, that is, the group containing *only* the identity element (which is its own inverse).

Another subgroup is $(\{1_A, a\}, \circ)$. You should check closure. Is this subgroup abelian?

We write $H \leq G$ if H, G are groups (we often supress explicit reference to the binary operation for brevity) and H is a subgroup of G. Note that subgroup is a much stronger condition than subset. H a subgroup of G implies H a subset of G, but NOT the other way round.

For example, $\{a, b\}$ is a subset of S_n, but it is not a subgroup because it is not closed, and does not contain the identity (exercise).

Chapter 4

Graphs

To read this section you will need to know about sets. If necessary, see the section on sets, and return here when you are done.

Graph Theory has applications in Sorting and Searching, Combinatorics, queuing theory, programming, cartography, Physics, systems engineering, representation theory, and a host of other areas. It is aslo interesting (to Mathematicians) in its own right.

4.1 Definitions

(**4.1.1**) A *directed graph* (or digraph) is a pair of sets (V, E) together with a pair of functions i and f from E into V.

The elements of V are the *vertices* of the graph, and those of E are the *edges*. If $i(e) = v_1$ and $f(e) = v_2$ then e is an edge from v_1 to v_2.

Diagrammatically we may represent a digraph as a collection of dots on the page (the vertices), together with a collection of lines (the edges) with direction arrows on them, each starting at some vertex and finishing at some vertex.

A *graph* is similar to a digraph, except that the edges have no direction arrows.

A *simple* (di)graph has no pair of vertices with multiple edges between them.

(**4.1.2**) A *loop* is an edge having the same initial and final point.

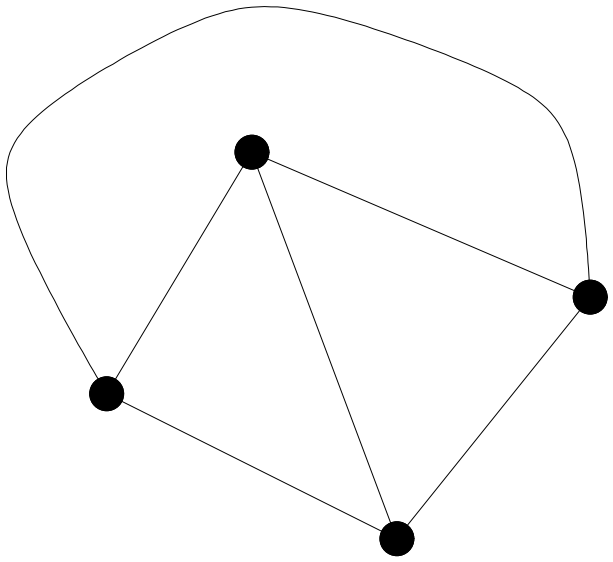
If $G = (V, E)$ and $G' = (V', E')$ are graphs then G' is a subgraph of G if $V' \subseteq V$ and $E' \subseteq E$. A special kind of subgraph is an *induced subgraph*. If G' is an induced sugraph of G then every edge of G for which both endpoints are present in V' is present in E'.

A graph is *connected* if for any two vertices there is a sequence of edges joining one to the other.

A (di)graph is *planar* if it can be represented on the plane in such a way that edges only ever touch at their endpoints (the vertices).

The *degree* of a vertex in a graph is the number of edges incident with that vertex.

The *complete graph* K_n on n vertices is the loop–free graph in which every pair of vertices is connected directly by an edge. For example, K_4 may be represented as:



(**4.1.3**) Execises.

What is the largest n for which K_n is planar?

Discuss the representation of elements of the group S_n as graphs.

(**4.1.4**) A *path* from v_1 to v_2 is a sequence of edges with the first beginning at v_1, each subsequent one beginning where the previous one finished, and with the last one ending at v_2. (On a graph either end of an edge may be regarded as the beginning, whereupon the other end must be *the* end.)

A *circuit* is a path from any vertex x to itself with at least one edge, and no edge occuring twice. For example, a loop is a circuit.

(**4.1.5**) A *tree* is a connected graph without circuits.

(**4.1.6**) Let G be a (di)graph whose vertices are totally ordered. There is a map from the set of such graphs with n vertices to the set of $n \times n$ matrices, as follows. $M_{ij}(G)$ is the number of edges from vertex i to vertex j. (Thus if G is a graph, not a digraph, the matrix is symmetric.)

We say that two (di)graphs, G and G', are *isomorphic* if their vertices can be ordered in such a way that $M(G) = M(G')$.

Note that if, from a given order of the vertices of G we reorder by exchanging two vertices, then $M(G)$ will change by having the corresponding pair of rows interchanged, and the corresponding pair of columns interchanged. Note that this is a similarity transformation (i.e. it can be achieved by conjugating $M(G)$ by an appropriate matrix). Note also that any reordering can be achieved by a sequence of such vertex pair reorderings. (We are back with the symmetric group again!) Hence any reordering acts like a similarity transformation on $M(G)$.

Note also that the order on vertices is not usually deemed to be intrinsic to the graph, so unless an order is specified, any of the versions of $M(G)$ in the same similarity class are equally good representations of G. (Although of course the vertices of G *are distinguishable.*) However, if G and G' are simply different orderings of the same vertex set, let us say by a pair permutation of vertices v and v', and $M(G) = M(G')$, then the graph has a kind of symmetry under swapping v and v'.
For example, if w is an eigenvector of $M(G)$: $wM(G) = \lambda M(G)$, then the entries in w are naturally associated to vertices. If P is the similarity trans-

form matrix which interchanges v and v' then $M(G) = PM(G')P^{-1}$, and with the symmetry: $M(G) = PM(G)P^{-1}$. Thus $wM(G)P = w(PM(G)P^{-1})P = wPM(G) = \lambda wP$, so wP is an eigenvector of $M(G)$ with the same eigenvalue. Note that wP is related to w simply by exchanging the entries corresponding to the vertices v and v'. Then if, for example, the eigenvector associated to the eigenvalue λ is know to be unique (up to scalar multiplication, as usual), we have that the entries corresponding to the vertices v and v' must be *the same*.
These observations can be useful in computing PageRank-like properties of graphs.

Exercise 24 *What do matrix addition and multiplication correspond to at the level of graphs?*

4.2 Colouring

(**4.2.1**) Let C be any set (for example, but not necessarily, a set of colours). A colouring of a loop–free graph G with C is a function f from V to C such that if there is an edge between any v_1 and v_2 then $f(v_1) \neq f(v_2)$.
(Note that the restriction to loop–free graphs is not really necessary in this definition, but there is *no* colouring of a graph with a loop, since the loop imposes the unsatisfiable condition that the corresponding vertex is coloured differently from *itself*!)

For any loop–free graph its 'chromatic number' is the smallest degree of C such that there exists a colouring of G with C. For example, the chromatic number of K_n is n (exercise!).

Exercise 25 *Let G be a graph and let $C_G(Q)$ denote the number of ways of colouring G with at most Q colours. (For example, $C_{K_2}(Q) = Q(Q-1)$.) Show that $C_G(Q)$ may be expressed as a polynomial in Q for every graph G.*

For graphs G and G' having no vertices in common, let $G \cup G'$ denote the natural disconnected composite graph. For a graph G with distinct vertices

v and v' connected by an edge e, let G_e denote the subgraph differing from G only in the absence of edge e, and let $G_{vv'}$ denote the graph obtained from G by identifying v and v' and discarding e.
Note that the transformation $G \mapsto G_e$ (any e) takes a simple graph to a simple graph, but the transformation $G \mapsto G_{vv'}$ does not necessarily do so. For example, picking any e in K_3 we have that $(K_3)_{vv'}$ is a graph like K_2 but with two edges instead of one.

Exercise 26 *Verify the polynomial identity* $C_G(Q) = C_{G_e}(Q) - C_{G_{vv'}}(Q)$.

Hint: note that G and G_e have the same vertex sets. Pick a suitable example and consider which colourings of G_e become 'illegal' when e is re-inserted. How can we count the number of such colourings using $G_{vv'}$?

A more mundane hint is to start by considering some examples.
If $G = K_2$ then $(K_2)_e$ is $K_1 \cup K_1$ (suitably interpretted), and $(K_2)_{vv'} = K_1$, so the claim is that $C_{K_2}(Q) = Q^2 - Q$, which is correct (see above).
Suppose G is like K_2, but with the edge tripled! Then removing one edge does not change the number of possible colourings, i.e. $C_G(Q) = C_{G_e}(Q)$. But identifying the two vertices leaves two edges which are now loops, even after removing the edge e, so $C_{G_{vv'}}(Q) = 0$ and the identity holds.

(**4.2.2**) Example application — Scheduling. Suppose various jobs are to be done in an industrial process producing some product. Suppose that it is possible to perform some of the jobs simultaneously, but not others (perhaps they require the *same* piece of machinery). A schedule for the jobs may be obtained as follows. The set of jobs is represented as vertices in a graph, joining any two if and only if they CANNOT be peformed at the same time. A *colouring* of this graph by a set of *times* then effectively assigns times for performance of jobs in such a way that jobs which cannot be performed simultaneously *are* not scheduled together.

4.3 Planar graphs

(**4.3.1**) Consider the plane with its natural metric topology. We will call a subset of the plane *open* if it is open with respect to this topology. (For example, consider a circle drawn in the plane — the set of all those points interior to, but not actually touching, the circle is an open subset.) An open subset of the plane is *connected* if it cannot be cut into two non–empty open pieces (roughly, it is an open region with the property that we may move continuously from any point within it to any other without leaving the region). Suppose that a graph G has a representation in the plane. A *face* of this representation is a bounded maximal connected region of the plane disjoint from the vertices and edges representing the graph.

An edge is *external* if it has a face on at most one side of it.

Proposition 4.1. *Let finite non–empty connected planar graph G have vertex set V, edge set E, and a planar representation with face set F. Then*

$$|V| + |F| - |E| = 1.$$

Proof: By induction on $|E|$. The base $|E| = 0$ is trivial. Assume the result true for all graphs with $|E| < n$ and let $G = (V, E)$ have n edges (and face set F). Without loss of generality let e be any external edge of G, with ends v_1 and v_2. If the subgraph G' got by removing e is connected then the inductive hypothesis applies to it. It has the same number of vertices, one fewer edge and (since e was external) one fewer face than G. Thus, in this case, the hypothesis holds on G.

If on the other hand removing e separates G into disconnected components then we have two subgraphs (V', E') and (V'', E''), say, with $V' \cap V'' = \emptyset$, $E' \cap E'' = \emptyset$, $V' \cup V'' = V$, $E' \cup E'' \cup \{e\} = E$, and similarly $F' \cap F'' = \emptyset$, and $F' \cup F'' = F$. Both sugraphs must obey the inductive hypothesis, so

$$|V| + |F| - |E| = |V'| + |V''| + |F'| + |F''| - (|E'| + |E''| + 1) = 1 + 1 - 1 = 1$$

as required. □

(**4.3.2**) The famous 4 colour theorem asserts that any finite planar graph can be coloured with no more than 4 colours. It is clear that there are planar graphs requiring at least 4 colours (see K_4 above). The fact that no more are required is one of the most intriguing and tantalising results in Graph Theory. The known proof is very complicated, although many authors (including the present one) have expended much effort in trying to produce a slicker one. For our purposes it will suffice to prove a weaker result.

Proposition 4.2. *Any finite loop–free planar graph can be coloured with no more than 5 colours.*

Proof: We may assume G to be simple and connected. Proceed by induction on the number of vertices. If there are 5 or fewer vertices then the result follows trivially, so the base is clear. Now assume all graphs with fewer vertices than G may be coloured with 5 or fewer colours. We will show that G must have a vertex of degree ≤ 5 and build a 5 colouring of G around such a vertex, thus establishing the inductive step.

Let M be the number of pairs (e, f) where e is an edge of face f. Each edge bounds at most 2 faces, so

$$M \leq 2|E|$$

and each face contributes at least 3 to M since G is simple, so

$$M \geq 3|F|.$$

Thus

$$|E| \leq |E| + (2|E| - 3|F|) = 3|V| - 3$$

(using Euler's formula from proposition 4.1 at the last). Let V_i be the number of vertices of G of degree i, then

$$2|E| = \sum_i iV_i$$

and so

$$\sum_i iV_i \leq 6|V| - 6$$

giving

$$\sum_{i=1}^{5}(6-i)V_i \geq 6 + \sum_{i=7}^{k}(i-6)V_i$$

where k is the maximum degree in G. In particular

$$\sum_{i=1}^{5}(6-i)V_i \geq 6$$

and at least one of V_1, V_2, V_3, V_4, V_5 is non-empty!

Now let P be a vertex of degree ≤ 5. Let G' be the induced subgraph of G on $V \setminus \{P\}$. Graph G' is still planar and has fewer vertices, so it can be 5 coloured by hypothesis. Consider such a 5 colouring of G'. We will show how to modify this colouring so that a colouring of the whole of G is possible.

If less than 5 colours are used for the neighbours of P in the colouring of G' then we can colour P with the fifth colour, so assume that P has degree 5 and its neighbours use all 5 colours. (Obviously we have to make a modification so that only 4 are used, while preserving the colouring of G'.) Label the neighbours by number clockwise around P. Suppose there is a path from 1 to 3 using only vertices coloured with two colours (red and blue, say); then there can be no such path from 2 to 4 (any path from 1 to 3 cuts a path from 2 to 4, since the graph is planar). Thus we may assume that at least one of these pairs does not have a two colour path between them. Without loss of generality, then, let 1 and 3 be a pair without a two colour path between them. Now let us say red is the colour of 3, and blue is the colour of 1. To colour the graph G *including* P, colour P red, and change the colour of 3, and any vertex in a red–blue path from 3, to the other one of these two colours.

To see that this works, it remains to check that we still have a colouring of G'. Both 1 and 3 are now blue, but they are not adjacent. All the red–blue paths of changed vertices starting at 3 are still consistent with colouring (red–blue–red becomes blue–red–blue, and so on). Further, there is no vertex adjacent to, but not on, any of these paths which is coloured either red or

blue (else it *is* on a path and so changed to be consistent by construction). □

4.4 Exercises

Exercise 27 *You are in a game show on TV. The host shows you three closed doors. Behind one of the doors is a prize. You have to guess which door leads to the prize. There are no clues, so you guess at random, but after you have guessed the host opens one of the other doors and shows that there is* not *a prize behind that door. She then asks if you would like to change your guess, or stay with your original guess.*

Is it better to change, or stay, or does it make no difference to your probability of success?

Draw a graph which illustrates the relevant probabilities and hence gives the answer to this well-known old puzzle.

Exercise 28 *Show that isomorphism is an equivalence relation on the set of all graphs.*

Exercise 29 *Up to isomorphism, how many different simple, loop-free graphs are there with 2 vertices? How many are there with 3 vertices? How many are there with 4 vertices?*

Exercise 30 *Up to isomorphism, how many different simple, loop-free graphs are there with n vertices and $\frac{n(n-1)}{2} - 1$ edges? How many are there with n vertices and $\frac{n(n-1)}{2} - 2$ edges?*

Exercise 31 *If we have a planar representation of a graph, then this 'restricts' to a planar representation of any subgraph (by simply erasing the relevant vertices and edges). However, it is not always possible to extend a planar representation of a subgraph to a planar representation of a planar graph by adding appropriate objects. Give an example to show this.*

An *Euler tour* of a graph is a walk that uses each edge of the graph once.

Euler's theorem states that if connected graph G has an Euler tour then there are either no vertices of odd degree, or two vertices of odd degree. Conversely, if there are no vertices of odd degree then there is an Euler tour, and it may start at any vertex but must end at the same vertex; while if there are two vertices of odd degree then there is an Euler tour, it must start at one of the vertices of odd degree and end at the other one.

Exercise 32 *(Harder) Prove Euler's theorem.*

A *spanning tree* for a connected graph G is a tree which is a subgraph of G whose vertex set coincides with that of G.

Exercise 33 *Construct an algorithm which takes a graph G as input and produces a spanning tree of G as output.*

Chapter 5

Sorting and Permutation

As we will see, the process of sorting is very much in the realm of pure discrete mathematics. However, even to say what *is* sorting, and why it is worth doing, become complex philosophical questions when viewed in a purely mathematical light. One advantage of coupling with the issue of sorting as a computing problem is that this gives us a collection of applications which serve to put these questions on a more concrete footing. Thus we will proceed, as far as possible, with reference to the mathematical and computational aspects *at the same time*.

The definitive text on sorting is, perhaps, Knuth [8].

5.1 Introduction

What is sorting? According to the WordNet online dictionary *to sort* is "to arrange or order by classes or categories" (that is, to put things together which are of the *same sort*). It is convenient to add to this that the classes then be put into some order, and we will usually assume that this means a total order. Indeed, this second part of sorting may also achieve the first since, if we have a hierarchical classification scheme and a total order of all (sub)classes then lexicographic ordering automatically arranges objects into a sequence consisting of runs of objects in the same class (just as a dictionary

order groups together all words beginning with A).

Why sort? Arranging objects into classes has many uses. In particular it helps with searching. Depending on the nature of the search either a total order or a classification may be the more useful. For example, if I am looking for a book in a library it is useful if the books are totally ordered. If I am looking for *information* in a library it may be more useful to have all the books on my subject grouped together, for browsing.

Exercise: Let $\{R_i \mid i = 1, 2, 3, ..., n\}$ be a row of books on a shelf. Let us say that the books are labelled each by an integer (representing a book title!). Thus the order of the books on the shelf may be represented as a sequence of integers. Give an algorithm to sort the first 5 of these book into non–descending order of their labels.

An answer: Let $\{I_i \mid i = 1, 2, 3, 4, 5\}$ denote the current list (i.e. possibly after reordering). For $i = 1, ..., 4$ compare I_i, I_{i+1} and swap if $I_i > I_{i+1}$. Iterate this loop until there is no further change.

Example:

$$43521 \to 34521 \to 34251 \to 34215$$

$$\to\to 32415 \to 32145 \to\to 23145 \to 21345 \to\to 12345$$

Q1. Does this process converge in general?
A1. Yes. Note that in each loop the largest numbered book not yet in its correct position is moved to its correct position.
Q2. Is it optimal?
A2. This is the interesting question, but it is not yet well posed, since different algorithms require different operations to be performed. Before we can ask a better question we need some more algorithms for comparison. The above procedure is called "Exchange Sort".

We could also do:

"Insertion Sort": Construct a new sequence as follows. Locate an empty shelf (hopefully very nearby!). Put R_1 somewhere in the middle to start a new sequence. Then for $i = 2, 3, 4, 5$ insert R_i in the correct position relative

to the existing form of the new sequence. Example

$$4\rangle 34\rangle 345\rangle 2345\rangle 12345$$

"Selection Sort": Locate the lowest numbered book and put it on the left on a new shelf. Then locate the lowest numbered remaining book and put it on the new shelf to the immediate right of the previous addition, and iterate.

"Enumeration Sort": For each R_i count the number of R_js which should be to its left. The final list of numbers so obtained gives the order in which to arrange the books on a new shelf. Example:

$$\begin{array}{c} 43521 \\ 32410 \end{array}$$

We now have enough algorithms to play with. To decide on optimality we need to know relatively how much effort is required for each of their component operations, and of course how many times (typically) each operation would have to be performed. The first of these data will depend on the system to be sorted (light books/ heavy books etc.). The second can be well addressed in the framework of pure combinatorics. In particular, at the heart of Exchange Sorting is the act of permuting elements of a list. The set of possible acts of permutation form a *group* under composition, and the study of this group can be seen to inform much of the theory of sorting. Accordingly we will start with (and here concentrate mainly on) a study of this group.

We begin by recalling the basic algebraic structures we will use.

5.2 Preliminaries

Before proceeding you will need to have read the section on groups in chapter 3. A good reference book for our purposes might be the Schaum Outline Series volume on *Groups* (but the following is abstracted in part from works of Knuth, Jacobson[6], Cohn[4, 3], Maclane and Birkoff[9], Bass[2], and Green[5]).

5.2.1 Algebraic systems

There follows a list of definitions in the form
ALGEBRAIC SYSTEM $A = (A$ a set, $n-$ ary operations), axioms.
Extended examples are postponed to the relevant sections.

(**5.2.1**) SEMIGROUP $S = (S, \Box)$, $\Box$ closed associative binary operation on S.

(**5.2.2**) MONOID $M = (M, \Box, u)$, $(M, \Box)$ a semigroup, u a unit ($au = a = ua$).
Example: $(\mathbb{N}_0, +, 0)$.

(**5.2.3**) GROUP $G = (G, ., u)$, G a monoid, $\forall a \in G \exists a'$ such that $aa' = u = a'a$.

(**5.2.4**) ABELIAN GROUP $G = (G, +, 0)$, G a group, $a + b = b + a$.

(**5.2.5**) RING $R = (R, +, ., 1, 0)$, $(R, +, 0)$ abelian group, $(R, ., 1)$ monoid, $a(b + c) = ab + ac$, $(a + b)c = ac + bc$.

(**5.2.6**) INTEGRAL DOMAIN K, K a ring, . commutative, $0 \neq 1$, $mn = 0$ implies either $m = 0$ or $n = 0$.

(**5.2.7**) FIELD F, F integral domain, every $a \neq 0$ has multiplicative inverse.

Exercise 34 *Show that the complex numbers are a field when taken with the usual binary operations of addition and multiplication.*

In fact the complex numbers are almost the only example of a field which we will need in this course. If you don't like the idea of fields, just replace all reference to them with a reference to the system of complex numbers!

Before we forget about general fields altogether though, consider the following exercises.

Exercise 35 *Show that the system of arithmetic mod 3 introduced in Chapter 3 is a field.*

Exercise 36 *Construct the addition and multiplication tables for the system of arithmetic mod 2 (generalising those introduced in Chapter 3). Show that this is a field.*

We will call these systems $\mathbb{F}_3$ and $\mathbb{F}_2$ respectively.

Exercise 37 *Verify that the definition of group above coincides with that given in Chapter 3.*

5.2.2 Categories

(**5.2.8**) A CATEGORY A is a collection of 'objects' (the possible failure of this collection to be a set will not concern us here), together with a non–empty set $A(M,N)$ of 'morphisms' for each ordered pair (M,N) of objects, and an associative composition

$$A(M,N) \times A(L,M) \to A(L,N)$$

such that there are identities $1_M \in A(M,M)$.

Example: Let **Set** be the collection of all sets, and for $M, N \in$ **Set** let **Set**(M,N) be the set of maps from M to N. The usual composition of maps is associative and has identities, so this is a category.

Let **Ab** be the collection of all abelian groups and **Ab**(M,N) the set of group homomorphisms from M to N. This is a category.

$f \in A(M,N)$ is an ISOMORPHISM if there exists $g \in A(N,M)$ such that $gf = 1_M$ and $fg = 1_N$.

(**5.2.9**) The DUAL CATEGORY A^o has the same objects and composition is reversed $(A(M,N) = A^o(N,M))$.

(**5.2.10**) A (covariant) FUNCTOR $F : A \to B$ is a map on objects together with a map on morphisms which preserves composition and identities.

A CONTRAVARIANT FUNCTOR from A to B is a functor from A^o to B (examples later).

5.3 Groups and representations

For F a field let $\mathfrak{GL}_n(F)$ denote the set of invertible $n \times n$ matrices over F. These matrices form a group under matrix multiplication.

Exercise 38 *Verify this explicitly for $F = \mathbb{C}$ in case $n = 2$.*

Exercise 39 *Write down* all *elements of $\mathfrak{GL}_2(\mathbb{F}_2)$.*

(**5.3.1**) A group homomorphism is a map $\rho : G \to H$ between groups such that $\rho(xy) = \rho(x)\rho(y)$.

Exercise 40 *Construct a group homomorphism between the groups $\mathfrak{GL}_2(\mathbb{C})$ and $\mathfrak{GL}_3(\mathbb{C})$.*

Put $\ker \rho = \{g \in G \mid \rho(g) = e\}$ (where e is the group identity element); and $\operatorname{im} \rho = \{\rho(g) \mid g \in G\}$.

(**5.3.2**) A SUBGROUP S of a group G is a group which is a subset of G. A NORMAL subgroup N of a group G (denoted $N \trianglelefteq G$) is a subgroup which is a union of conjugacy classes of G (thus $n \in N$ implies $gng^{-1} \in N$ for all $g \in G$).

(**5.3.3**) For S any subgroup of G we may partition G into LEFT COSETS OF S as follows. For $g \in G$ the coset

$$Sg = \{sg \mid s \in S\}$$

and the set of left cosets is denoted G/S.

Proposition 5.1. *If $N \trianglelefteq G$ then G/N is a group with multiplication $(Na)(Nb) = N(ab)$, and there is a natural group epimorphism $\pi : G \to G/N$ given by $\pi(g) = Ng$.*

Proof: We need to show that if $a' \in Na$ and $b' \in Nb$ then $N(a'b') = N(ab)$. WLOG put $a' = n_1 a$, $b' = n_2 b$ with $n_i \in N$, then $an_2a^{-1} \in N$ by the definition of normal subgroup, and so

$$N(a'b') = Nn_1an_2b = Nan_2b = Nan_2a^{-1}ab = Nab$$

□

(**5.3.4**) Let $\phi : G \to H$ be a group homomorphism. Then $\operatorname{im}\phi$ is a subgroup of H and $\ker\phi$ is a normal subgroup of G. There is a factorisation $\phi = \phi' \circ \pi$ where $\pi : G \to G/\ker\phi$ is as in proposition 5.1 and $\phi' : G/\ker\phi \to \operatorname{im}\phi$ is the isomorphism $\phi'(\ker\phi g) = \phi(g)$.

(**5.3.5**) A REPRESENTATION of a group G over a field F is a homomorphism $\rho : G \to \mathfrak{GL}_n(F)$ for some n.

A finite group is a group which is a finite set.

(**5.3.6**) A group G ACTS on a set W if there is a map from $G \times W$ to W (denoted $(g, w) \mapsto gw$) such that $1w = w$ and $g(hw) = (gh)w$.

5.4 The symmetric group

(**5.4.1**) A PERMUTATION p of a finite set S is a bijection from S to $\{1, 2, \ldots, |S|\}$, that is to say, an arbitrary total ordering of S. We may represent a permutation by listing the elements of S in the order $p = (p^{-1}(1), p^{-1}(2), \ldots)$.

(**5.4.2**) Let $\mathcal{P}_n$ denote the set of $n \times n$ matrices whose row vectors are a permutation of the standard ordered basis of $\mathbb{C}^n$. These matrices form a group under matrix multiplication, denoted S_n.

The set of bijections of any set T of degree n to itself form a group under composition of bijections, and this group is isomorphic to S_n (the identity bijection maps to the identity matrix). We will confuse the two groups willy–nilly under the name SYMMETRIC GROUP.
It is convenient to use $T = \{1, 2, \ldots, n\}$.

(**5.4.3**) There is a useful pictorial representation of S_n, obtained by tracking the timelines in a sort of some notionally ordered set. We see from figure 5.1 that each act of permutation may be viewed as a collection of trajectories between two rows of vertices (representing the objects in the set before and after rearrangement). Composition is then by juxtaposition of such diagrams.

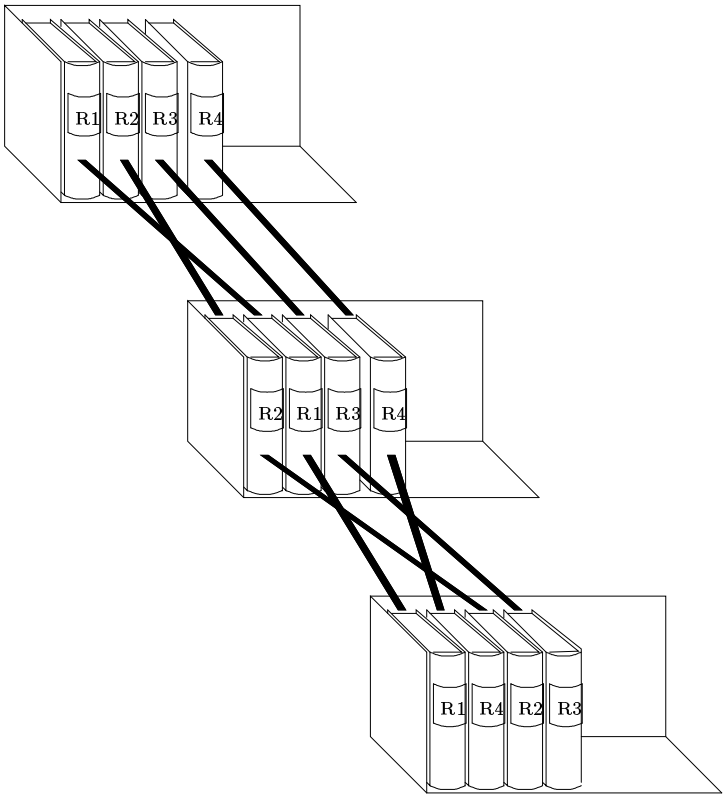


Figure 5.1: An act of permutation as a rearrangement of books on a library shelf. The first step permutes an adjacent pair of books; the second step is a more complicated rearrangement.

(**5.4.4**) Abstract to diagrams (i.e. discard the books and keep the trajectories). These form a group isomorphic to S_n. The multiplication of diagrams is to juxtapose them top to bottom (just as they are juxtaposed in the figure, once the books are removed), and then to equate diagrams which realise the same connections from top to bottom.

Exercise: Familiarise yourself with these diagrams and their multiplication. Given the diagram for some $f \in S_n$, what does the diagram for f^{-1} look like?

(**5.4.5**) In CYCLE notation a permutation p of $T' \subseteq T$ is interpreted as an element f of S_n by

$$\begin{aligned} f(i) &= \quad i \quad && (i \notin T'), \\ f(p_{|T'|}) &= \quad p_1 \quad && \text{and} \\ f(p_i) &= \quad p_{i+1} \quad && \text{otherwise.} \end{aligned}$$

We will call such an element a cycle of length $|T'|$.

There is a SHUFFLE action on the set of cycles of T' obtained by taking

$$p \mapsto (p_2, p_3, \ldots, p_{|T'|}, p_1).$$

The orbits of this action may be represented by the elements in which the numerically lowest element of T appears first. Note that two different cycles may produce the same element of S_n — in particular they do so iff they are in the same shuffle orbit.

Note also that only a subset of elements of S_n are produced this way. However

Proposition 5.2. *A cycle on T' commutes with a cycle on $T'' \subseteq T$ if $T' \cap T'' = \emptyset$.*
Each $f \in S_n$ is a product of such disjoint cycles.

We will write such products so that a longer cycle comes before a shorter one. If we also arrange for the lowest element of each cycle to be written first, and in the case of a tie on length for the cycle with the lowest first element to be written first, then such products are in bijection with S_n. The

cycle structure λ of $f \in S_n$ is then the list $(\lambda_1, \lambda_2, \ldots)$ of cycle lengths in the given order (and hence a PARTITION OF n — we write $\lambda \vdash n$, and denote the set of partitions of n by Λ_n).

Proposition 5.3. *Two elements of S_n are in the same conjugacy class iff they have the same cycle structure.*

Exercise: Prove this proposition (hint: draw the diagram for a non–trivial conjugation and so determine the effect of conjugation on a cycle).

5.4.1 Matrix representations

(**5.4.6**) Consider the list of all possible initial orderings of the row of books in figure 5.1. For n distinguishable books there are $n!$ orderings. Let us consider writing out all these orderings as a list (for $n = 3$ we would have 123, 132, 213, 231, 312, 321). A particular act of permutation, such as illustrated in the figure, takes each one of these orderings to a different one. We can encode its effect on the complete list as a matrix as follows.

To begin let us consider the first (upper) act of permutation in the figure (and neglect its effect on the last book, $R4$). In cycle notation the element of the permutation group S_4 in question is (12). Its action takes 1234 to 2134, and in particular *restricts* to take 123 to 213. If the initial ordering had been 1342, say, instead of 1234, the same action would have taken 1342 to 3142 (that is, we have the act of permutation permuting the objects in certain positions, rather than permuting objects with certain labels). Altogether we find that $(123, 132, 213, 231, 312, 321)$ is taken to $(213, 312, 123, 321, 132, 231)$.

We can realize this reordering by matrix multiplication. Specifically, consider the vector space with basis this list of orderings, and the matrix which transforms a 6–tuple whose entries are the basis elements in the original order

into one in the new order:

$$(123,132,213,231,312,321)\begin{pmatrix}001000\\000010\\100000\\000001\\010000\\000100\end{pmatrix}=(213,312,123,321,132,231).$$

Again ignoring $R4$, the rearrangement whose cycle notation is (23) is captured similarly by

$$(123,132,213,231,312,321)\begin{pmatrix}010000\\100000\\000100\\001000\\000001\\000010\end{pmatrix}=(132,123,231,213,321,312).$$

In this way we build a matrix $R(x)$ for each element $x \in S_n$. If we now discard the vectors, we find that the matrices give us a representation of S_n (Exercise: Explain exactly how this works).

(**5.4.7**) Further, if some of the books are duplicates we still get a representation (exercise). We thus have a plethora of representations. Our next job is to bring some order to this situation.

Until further notice we will concern ourselves with complex representations (i.e. where the field of the matrix entries is $\mathbb{C}$).

(**5.4.8**) Suppose M is a representation of a group G. Then conjugating every representation matrix by a fixed (complex) matrix gives another representation isomorphic to the first. For example

$$M(x)M(y)=M(xy)\Rightarrow(A^{-1}M(x)A)(A^{-1}M(y)A)=(A^{-1}M(xy)A).$$

Isomophism is an equivalence relation. The set of representations isomorphic to a given representation is its equivalence class.

(**5.4.9**) Suppose M_1 and M_2 are two representations of G. For each $g \in G$ construct the *matrix direct sum* of $M_1(g)$ and $M_2(g)$. This set of matrices forms a new representation of G.

If a representation is isomorphic to a representation formed in this way then it is said to be REDUCIBLE, otherwise it is IRREDUCIBLE.

(**5.4.10**) Since every representation can be built up simply from irreducible representations, the most important aspect of the study of a group (at least from the point of view of modelling) is the study of its IRREDUCIBLE representations.

(**5.4.11**) A handy indicator is:

Proposition 5.4. *If any matrix A which is not a multiple of the identity matrix obeys $AM(g) = M(g)A$ for every $M(g)$ in a representation then the representation is reducible.*

Exercise: Prove it. Hints:

1. Note that every matrix which is the image of a group element in some representation is necessarily invertible. Thus it has maximal rank, and so a maximal number of eigenvectors. Thus it is diagonalisable.

2. Start by proving that: Two diagonalisable matrices can be simultaneously transformed into diagonal form (i.e. by the *same* transformation) iff they commute.

Exercise: Prove that every irreducible representation of an abelian group is 1–dimensional.

(**5.4.12**) Let g be any element of G. Then the set of elements of G which commute with g (such as e and g) form a subgroup of G (called the normaliser of g).

Let $[g]$ denote the class of g.

Proposition 5.5. *For $g \in G$, $\{gh \mid h \in G\} = G$.*

Proof: Let $f \in G$ be arbitrary. Then $f \in \{gh\}$ since $f = g(g^{-1}f)$. Done.

(**5.4.13**) Consider the K–vector space with basis G. The group multiplica-

tion may be extended K–linearly to a multiplication on this space, whereupon it is called the K–group algebra of G, denoted KG. A subalgebra is a subset closed as a space and under this multiplication. A K–representation of G gives rise to a representation of KG (and any subalgebra) by the obvious K–linear extension.

Proposition 5.6. *The number of equivalence classes of irreducible representations of a group G is equal to the number of classes of G.*

We will prove this fundamental result shortly. First we need to do some preparatory work.

(**5.4.14**) Write $G = \{g_i \mid i = 1, 2, \ldots, N\}$ and $|[g]| = N_{[g]}$. Consider the elements $g_j g g_j^{-1} \in [g]$ as g_j runs over G. If g_j is in the normaliser G_g of g then $g_j g g_j^{-1} = g$. Indeed elements $g_j \in G$ in the same coset of G_g give the same conjugate of g; and elements $g_j \in G$ in different cosets of G_g give different conjugates of g. Altogether, then, as we run over all possible choices of g_j in $g_j g g_j^{-1}$, we visit each member of $[g]$ precisely $\frac{N}{N_{[g]}}$ times. Therefore, in the group algebra

$$\sum_{j=1}^{N} g_j g g_j^{-1} = \frac{N}{N_{[g]}} \sum_{g' \in [g]} g'.$$

Indeed, let us use $[g]$ in the group algebra to denote the sum of all the elements in the class, and say that an element of the group algebra is a linear function of classes if it is a linear combination of such basic class sums. We have

Proposition 5.7. *$x \in \mathbb{C}G$ commutes with all $g \in G$ iff x is a linear function of classes.*

Proof: (if) It is enough to show that g commutes with every basic class sum. We have

$$g \left(\sum_{g' \in [h]} g' \right) g^{-1} = \frac{N_{[h]}}{N} g \left(\sum g_j h g_j^{-1} \right) g^{-1} = \frac{N_{[h]}}{N} \left(\sum g g_j h (g g_j)^{-1} \right) = \sum_{g' \in [h]} g'$$

by proposition 5.5.

(only if) If $x = \sum_i k_i[g_i]$ commutes with all $g \in G$ then

$$x = \frac{1}{N}\sum_j g_j x g_j^{-1} = \frac{1}{N}\sum_i k_i \sum_j g_j g_i g_j^{-1}$$

which is a linear function of classes. Done.

(**5.4.15**) *Proof of proposition 5.6* A matrix representation R of G is also a representation of the subalgebra generated by the basic class sums. Since this latter is commutative every element can simultaneously be written in diagonal form. If R is reducible then it is isomorphic to a representation in which the matrices for all elements of G have the same block diagonal structure (exhibiting the irreducible content). In this representation the block components for matrices representing elements of the class sum subalgebra are scalar multiples of the (block) unit matrix (by proposition 5.4). That is, different diagonal terms in these matrices correspond to different irreducible representations.

Since a class function depends on the choice of a free parameter for each class, the representation matrix can depend on at most this many parameters (depending on whether the representation is faithful or not). Thus there can be up to this many different diagonal terms (precisely this many if R is faithful), and thus there are this many inequivalent irreducible representations of G. Done.

(**5.4.16**) For example, there are seven irreducible representations of S_5, corresponding to the seven classes (corresponding in turn to the seven partitions of 5, which are $\{(5), (4,1), (3,2), (3,1,1), (2,2,1), (2,1,1,1), (1,1,1,1,1)\}$).

(**5.4.17**) EXERCISES.

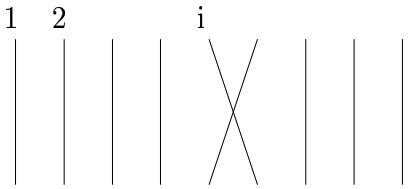
Write down the two irreducible representations of S_2 (corresponding to the partitions of 2, which are $\{(2), (1,1)\}$). Now try to figure out the three irreducible representations of S_3!

Prove proposition 5.2. Hint: ...

5.4.2 Sorting

(**5.4.18**) A group G is GENERATED by a subset S if every element of the group is expressible as a 'product' of one or more of these elements.

(**5.4.19**) Examples. Let us write σ_i for the 'elementary transposition' $(i\ i+1) \in S_n$. That is, as a diagram:

$\sigma_i =$ 

We have

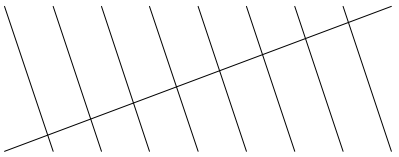
$$\sigma_i\sigma_i = 1 \tag{5.1}$$

$$\sigma_i\sigma_{i\pm1}\sigma_i = \sigma_{i\pm1}\sigma_i\sigma_{i\pm1} \tag{5.2}$$

$$\sigma_i\sigma_j = \sigma_j\sigma_i \qquad\qquad j \neq i \pm 1 \tag{5.3}$$

and $\{\sigma_i \mid i = 1, 2, ..., n-1\}$ generates S_n. (Exercise: Verify this by considering diagrams. More surprisingly, the equations 5.1–5.3 are sufficient for abstract objects $\{\sigma_i \mid i = 1, 2, ..., n-1\}$ to generate a group isomorphic to S_n even if we don't know anything else about them!)

Let $t_n = (12...n)$, i.e. $t_n == \sigma_{n-1}\sigma_{n-2}...\sigma_1 =$

$(12...n) =$ 

Then $\{(12), (12...n)\}$ generates S_n. (To see this note $(t_n)^n = 1$ so $t_n^{-1} = (t_n)^{n-1}$ and

$$t_n^{-1}\sigma_1 t_n = \sigma_2$$

and so on. Thus we reduce to the previous problem.

(**5.4.20**) If $S \subset G$ generates G then the matrices $R(S)$ completely determine a representation R of G.

(**5.4.21**) We can now consider how many elementary transpositions are required to sort an arbitrary permutation. Since each $\sigma_i = \sigma_i^{-1}$ the number required is equal to the minimum number of σ_is required to be multiplied together to achieve that permutation (starting, as it were, from the 'trivial' permutation). It will be evident that the number of σ_is required to build $g \in S_n$ is not unique (e.g. $1 = \sigma_i\sigma_i = \sigma_i\sigma_i\sigma_j\sigma_j$ etc.). However, there is a well defined minimum number required, which we will call $\mathrm{len}(g)$ (pronounced 'length g') — we normally say $\mathrm{len}(1) = 0$; then $\mathrm{len}((23)) = 1$ and so on.

The length of g is equal to the number of crossings of lines in the diagram of g, provided all the lines are drawn straight (and the rows of vertices are slightly agitated randomly so that no more than two lines ever intersect at the same point). Alternatively, the minimum number can be read off from the permutation in a way directly analogous to the "bubble" sort of the permutation (a kind of exchange sort — see Knuth).

For an example let us consider the permutation

$$\begin{pmatrix} 12345678 \\ 32658714 \end{pmatrix} = (458)(1367).$$

How can this be expressed minimally as a product of elementary transpositions? One (non–unique) way is illustrated in figure 5.2. We first locate the object which should be permed into 'last place', and move it into last place by a sequence of elementary transpositions. Then repeat for the object which should be in next to last place, and so on. (nominal bubble sort pictures some of the elementary transpositions occuring in parallel, if they commute, but this does not change the number of elementary transpositions required). Note that this construction ensures that no two lines cross each other more than once, and hence, provided the required 'perm' is achieved (!), that the number of elementary transpositions is minimal.

We can see from this that the maximum number of factors which could

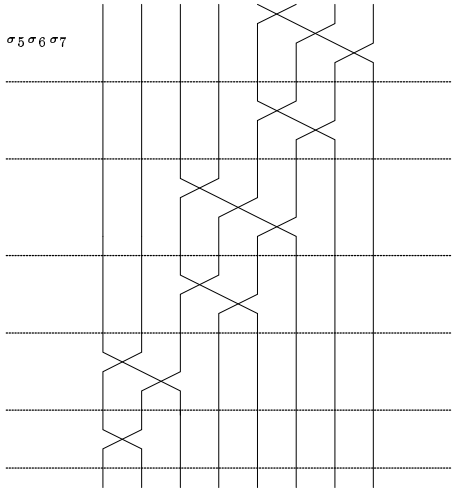


Figure 5.2: An act of permutation as a product of elementary transpositions, organised following the 'bubble' sorting algorithm.

be required is

$$(n-1)+(n-2)+\ldots+1=\frac{n(n-1)}{2}$$

and that this is only achieved by, for example,

$$\begin{pmatrix} 12345678 \\ 87654321 \end{pmatrix} =: w_0.$$

5.4.3 Exercises

1. Determine the mean and a median for the length of elements of S_n. That is, determine the average number of elementary transpositions required to sort an arbitrary permutation of n objects into a specific total order. (Hint: If you are stuck you should try to determine the lengths of all elements of S_n for $n = 1, 2, 3, 4$ and then consider how to generalise your findings.)

2. (Non–compulsory, for 10 bonus points) Determine the modal length(s) of elements of S_n.

3. Determine all one–dimensional representations of S_n. Give a non–trivial relationship between one of these representations and the len function.

4. Determine if the following gives a representation of S_3

$$\sigma_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\sigma_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

and if so, determine if that representation is irreducible.

5. Show that the set L of all elements of the form $(i\ j)$ $(i < j,\ i, j \in \{1, 2, ..., n\})$ generates S_n. Describe an algorithm to sort a permutation of n objects using this set. Discuss the practical differences between using this set to sort books (in the library at Alexandria) and using the set of elementary transpositions. Define a length function on S_n appropriate for the set L, and relate this to the normal length function.

Chapter 6

Hardware

This component of the course is lab based. We will attempt to separate and identify within an arbitrary PC the following components: Motherboard; Processor (CPU); BIOS chip; RAM; Hard disk; Floppy disk; IO ports; Network capability; Video subsystem; HCI devices (keyboard, mouse etc.). We will discuss the role of these components and their relationship with the operating system and other software. We will attempt to reassemble the system and, if functional (!), to install an operating system. If *this* can be done we will attempt to create a LAN (local area network) with another such PC, by installing appropriate Network Interface Cards, cables, and hubs, and configuring these devices in software (both at the driver level and at the Internet Protocol level).

Exercise 41 *Make sure you can physically identify the core modular components (as listed above) of a generic PC.*

Exercise 42 *Draw a graph encoding the modular structure of a typical PC.*

Exercise 43 *Draw a graph encoding the structure of a typical small LAN.*

Exercise 44 *Under what circumstances might a single PC contain two NICs?*

Bibliography

[1] F Ayres Jr, *Theory and problems of Matrices*, Schaum's outline, Schaum - McGraw-Hill, London, 1974.

[2] H Bass, *Algebraic K–theory*, Benjamin, New York, 1968.

[3] P M Cohn, *Algebra*, vol. 1, Wiley, New York, 1982.

[4] ———, *Algebra vol.2*, Wiley, New York, 1982.

[5] J A Green, *Polynomial representations of* GL_n, Springer-Verlag, Berlin, 1980.

[6] N Jacobson, *Basic Algebra II*, Freeman, 1980.

[7] H F Mattson Jr., *Discrete mathematics with applications*, Wiley, Singapore, 1993.

[8] D E Knuth, *Sorting and searching*, 2 ed., The Art of Computer Programming, vol. 3, Addison Wesley, 1998.

[9] S Maclane and G Birkoff, *Algebra*, Collier Macmillan, New York, 1979.

[10] M R Spiegel, *Advanced calculus*, Schaum's Outline, McGraw Hill, 1988.

[11] G Stephenson, *Mathematical methods for science students*, 2 ed., Longman, 1973.