

Combinatorial Enumeration: Theory and Practice

Gordon Royle

Semester 1, 2004

Combinatorial Structures

Combinatorics is the study of finite sets of objects defined by certain specified properties – *combinatorial structures* – such as:

- ▶ Subsets of a finite set

$$\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}$$

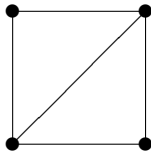
- ▶ Partitions of a number

$$4 = 1 + 1 + 1 + 1 = 1 + 1 + 2 = 1 + 3 = 2 + 2$$

- ▶ Words over a finite alphabet

aaa, aab, aba, abb, baa, bab, bba, bbb

► Graphs



► Latin squares

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

Combinatorial Questions

For any particular combinatorial structure, a number of (related) questions can be asked:

- ▶ Existence
Are there *any* combinatorial structures of this type?
- ▶ Enumeration
How many combinatorial structures of this type are there?
- ▶ Generation
List all the combinatorial structures of this type.

Existence

An *existence* question can be answered in different ways:

- ▶ Constructively, by giving
 - ▶ An *explicit example*, or
 - ▶ An *algorithm* to construct an example.
- ▶ Non-constructively, by giving an existence proof that does not yield an actual example.

A *constructive proof* is regarded as being “better” than a non-constructive one.

Enumeration

There are even more ways in which an enumeration question can be answered, including:

- ▶ Exactly

A set of size n has $\binom{n}{k}$ subsets of size k .

- ▶ Approximately

The number $L(n)$ of Latin squares of order n satisfies $\log L(n) = n^2 \log n + O(n^2)$.

- ▶ Implicitly

The n 'th Fibonacci number F_n is the coefficient of x^n in the expansion of

$$\frac{1}{1 - x - x^2}$$

as a power series (about 0).

Enumeration cont.

- ▶ Bijectively

The number of switching classes of graphs is equal to the number of Eulerian graphs.

- ▶ Computationally

If all else fails, it may only be possible to produce a short list of the numbers of small combinatorial structures by direct computer generation. For example, the number of *Steiner triple systems* on n points for $n = 1, \dots, 19$ is

1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 2, 0, 80, 0, 0, 0, 11084874829.

Generation

Algorithms for the generation of combinatorial structures are often called *combinatorial algorithms*.

Such an algorithm should generate every combinatorial structure of a particular type – for example, we might want to generate all the subsets of a given set. Other considerations include:

- ▶ Efficiency

The algorithm should be efficient in both space and time terms.

- ▶ Ordering

The order in which the structures are output may be significant — a specific order may be required by the user, or a cleverly chosen order may reduce the amount of work required.

Ranking

Given a set X of n combinatorial structures, a *ranking function* is a bijection

$$r : X \rightarrow \{0, \dots, n-1\}$$

where $r(x)$ is the *rank* of the structure x .

A ranking function specifies an order from the first structure (the one with rank 0) to the last (the one with rank $n-1$).

With this definition, counting starts at 0 which is usually the most convenient for computation. Mathematically, it is probably more natural to have a ranking function defined to be a function

$$r : X \rightarrow \{1, \dots, n\}$$

and we will freely use this whenever appropriate.

Successors

If we have a ranking on a set X , then for any structure x with $r(x) < n - 1$ the *successor* of x is the structure y such that

$$r(y) = r(x) + 1.$$

The *predecessor* of a structure x is defined analogously provided $r(x) > 0$.

A generation algorithm can often be described simply by giving an explicit successor function (that is, a rule for computing the successor of x directly from x). This is extremely useful because it means that the corresponding generation algorithm does not need to maintain large lists of structures.

Unranking

The inverse of a ranking function is called an *unranking* function.
That is, a function

$$u : \{0, \dots, n-1\} \rightarrow X$$

such that $ru = e$ (where e is the identity function).

Any ranking function *implicitly* defines an unranking function, but having an *explicitly* defined unranking function is extremely useful.

Sampling

For most types of combinatorial structure, there is an enormously rapid increase in their number as their size increases — the *combinatorial explosion*.

In this case, exhaustive generation is impossible, but we often wish to perform tests or collect statistical data by *sampling* the structures uniformly at random.

If we have an explicit unranking function u then getting a sample structure from a set X is very easy.

- ▶ Generate a (pseudo-)random number i between 0 and $|X| - 1$
- ▶ Calculate $u(i)$

Subsets

The simplest of the classical combinatorial structures are the *subsets* of a set.

Recall the notation used for sets:

$A \subseteq B$ A is a subset of B .

$A \subset B$ A is a proper subset of B .

\emptyset The empty set.

$A \cap B$ The intersection of A and B .

$A \cup B$ The union of A and B .

2^A The set of all subsets of A (the *powerset* of A)

$\mathcal{P}(A)$ Another common notation for 2^A .

The powerset $2^{\{1,2,3,4\}}$

$$\{1, 2, 3, 4\}$$

$$\{1, 2, 3\} \quad \{1, 2, 4\} \quad \{1, 3, 4\} \quad \{2, 3, 4\}$$

$$\{1, 2\} \quad \{1, 3\} \quad \{1, 4\} \quad \{2, 3\} \quad \{2, 4\} \quad \{3, 4\}$$

$$\{1\} \quad \{2\} \quad \{3\} \quad \{4\}$$

$$\emptyset$$

Counting all subsets

The *existence* of subsets of a set is not in doubt, so we only need to consider enumeration and generation.

Theorem

If A is a set of size n , then 2^A has size 2^n .

Proof.

If $A = \{a_1, \dots, a_n\}$ then a subset of A is determined by specifying for each $i = 1, \dots, n$ whether a_i is included or excluded. These n choices are independent and hence there are 2^n possibilities. ■

Representing subsets

Representing these n choices with 0s (for excluded) and 1s (for included) yields a useful representation of a subset as a binary n -tuple.

For example, if $A = \{1, 2, 3, 4, 5\}$ then we can specify the subset $\{2, 3, 5\}$ as follows:

5	4	3	2	1
5	4	3	2	1
1	0	1	1	0

If we view this binary n -tuple as the binary representation of an integer, then we obtain a very convenient ranking function r . For our example subset we have

$$r(\{2, 3, 5\}) = 10110_2 = 16 + 4 + 2 = 22.$$

Unranking

The corresponding unranking function merely involves computing the binary representation of an integer i .

Each successive binary digit (from the least significant) is obtained by checking to see if i is odd and then replacing i by the quotient when i is divided by 2. For example, if $i = 29$ and $n = 5$ then

i	$i \bmod 2$	$i/2$
29	1	14
14	0	7
7	1	3
3	1	1
1	1	0

Reading the second column upwards we conclude that

$$29_{10} = 11101_2 \text{ corresponding to } \{1, 3, 4, 5\}$$

Ordering

The ordering on subsets determined by this representation is sometimes called *lexicographic ordering*. Unfortunately there are at least two other orderings on the set of all subsets that are also sometimes called lexicographic!

A	n -tuple	$r(A)$
\emptyset	000	0
$\{1\}$	001	1
$\{2\}$	010	2
$\{1, 2\}$	011	3
$\{3\}$	100	4
$\{1, 3\}$	101	5
$\{2, 3\}$	110	6
$\{1, 2, 3\}$	111	7

The powerset $2^{\{1,2,3,4\}}$

$$\{1, 2, 3, 4\} 15$$

$$\{1, 2, 3\} 7 \quad \{1, 2, 4\} 11 \quad \{1, 3, 4\} 13 \quad \{2, 3, 4\} 14$$

$$\{1, 2\} 3 \quad \{1, 3\} 5 \quad \{1, 4\} 9 \quad \{2, 3\} 6 \quad \{2, 4\} 10 \quad \{3, 4\} 12$$

$$\{1\} 1 \quad \{2\} 2 \quad \{3\} 4 \quad \{4\} 8$$

$$\emptyset 0$$

Minimal change algorithms

Under the lexicographic ordering the difference between successive subsets can be very large. For example,

$$\text{succ}(\{1, 2, 3\}) = \{4\}$$

which involves altering the status of all 4 elements (that is, changing all 4 bits).

A *minimal change* algorithm is one where the successor function changes the current structure as little as possible — in the case of generating subsets, we would like to change just *one bit*.

A cyclic ordering of the 2^n binary n -tuples such that each differs from the previous one by a single bit is called a *Gray code*.

Small Gray codes

We can easily find Gray codes for small values of n :

For $n = 1$ we have

0 1

For $n = 2$ we have

00 01 11 10

For $n = 3$ we have

000 001 011 010 110 111 101 100

There is a pattern evident in this last Gray code:

000 001 011 010 110 111 101 100

Existence of Gray codes

The following theorem shows that Gray codes exist for all lengths — it is an example of a constructive proof.

Theorem

Let $G_n = (g_0, g_1, \dots, g_m)$ be an n -bit Gray code (so $m = 2^n - 1$). Then the code

$$(0g_0, 0g_1, \dots, 0g_m, 1g_m, \dots, 1g_1, 1g_0)$$

obtained by listing the words of G_n each preceded by 0, and then the words of G_n in reverse order each preceded by 1 is an $(n + 1)$ -bit Gray code.

Proof.

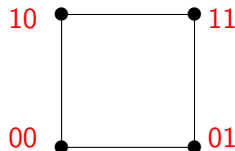
There is a 1-bit change between each of the first 2^n words and each of the last 2^n words, and so we merely need to check the halfway point, where the successor of $0g_m$ is $1g_m$ and that the final word $1g_0$ is one bit different from the first word $0g_0$, both of which are clear. ■

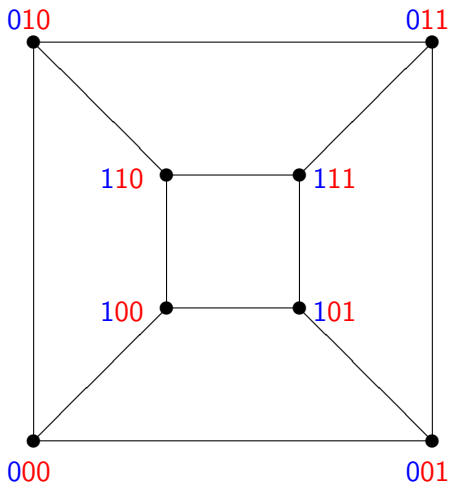
Together with the existence of the Gray code G_1 , this provides an inductive proof that Gray codes of all lengths exist.

Cubes

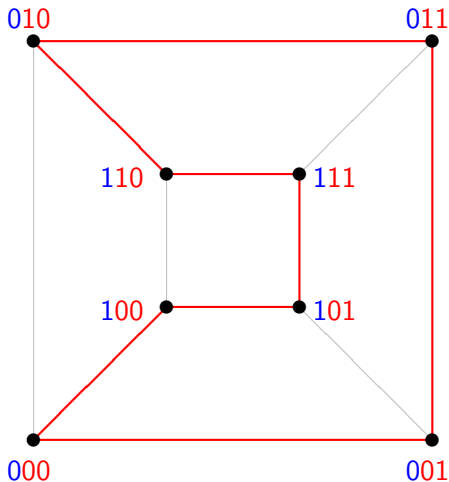
Gray codes are intimately related to a series of graphs known as the k -cubes Q_k .

The vertices of Q_k are the 2^k binary k -tuples, where two k -tuples are adjacent if they differ in exactly one coordinate position.



The cube Q_3 

A Gray code is a Hamilton cycle



Enumeration of Gray codes


An important resource for checking the status of enumeration problems is the *Online Encyclopedia of Integer Sequences* located at

<http://www.research.att.com/~njas/sequences>

This is an online searchable database of sequences of integers that can be used to determine if a given type of structure has been enumerated, or if a given sequence corresponds to a known formula or type of structure.

If we search for “Gray code” we discover that the numbers are known only for $n = 1, \dots, 5$:

1, 1, 6, 1344, 906545760



A screenshot of a web browser window displaying the "On-Line Encyclopedia of Integer Sequences (Look-Up)" page. The browser's address bar shows the URL "http://www.research.att.com/~njas/sequences/index.html". The page features a header with logos for AT&T, "Integer Sequences", and "RESEARCH". The main title is "The On-Line Encyclopedia of Integer Sequences". Below the title, there is a search prompt: "Enter a ☐ sequence, ☒ word, or ☐ sequence number:". A text input field contains the text "gray code". Below the input field are buttons for "Search", "Restore example", and links for "Clear", "Hints", and "Advanced look-up". A section titled "Other languages:" lists various languages including Albanian, Arabic, Bulgarian, Catalan, Chinese (simplified, traditional), Croatian, Czech, Danish, Dutch, Esperanto, Finnish, French, German, Greek, Hebrew, Hindi, Hungarian, Italian, Japanese, Korean, Polish, Portuguese, Romanian, Russian, Serbian, Spanish, Swedish, Thai, and Turkish. Below this list, it says "For information about the Encyclopedia see the [Welcome](#) page." Further down, there are links for "Lookup", "Welcome", "Francais", "Demos", "Index", "Browse", "More", "WebCam", "Contribute new seq. or comment", "Format", "Transforms", "Puzzles", "Hot", "Classics", "More pages", "Superseeker", and "Maintained by N. J. A. Sloane (njas@research.att.com)". At the bottom, it states "[Last modified Tue Feb 17 18:05:31 EST 2004. Contains 91600 sequences.]". A footer section contains links for "home", "people", "projects", "research areas", and "resources", along with "Terms and Conditions", "Privacy Policy", "Copyright 2003 © AT&T. All Rights Reserved.", and "Send comments to Webmaster@research.att.com".

On-Line Encyclopedia of Integer Sequences (Look-Up)

http://www.research.att.com/~njas/sequences/index.html

On-Line Encyclopedia of I...

AT&T Integer Sequences RESEARCH

The On-Line Encyclopedia of Integer Sequences

Enter a ☐ sequence, ☒ word, or ☐ sequence number:

gray code

Search Restore example Clear Hints Advanced look-up

Other languages: Albanian Arabic Bulgarian Catalan Chinese (simplified, traditional) Croatian Czech Danish Dutch Esperanto Finnish French German Greek Hebrew Hindi Hungarian Italian Japanese Korean Polish Portuguese Romanian Russian Serbian Spanish Swedish Thai Turkish

For information about the Encyclopedia see the [Welcome](#) page.

[Lookup](#) | [Welcome](#) | [Francais](#) | [Demos](#) | [Index](#) | [Browse](#) | [More](#) | [WebCam](#)
[Contribute new seq. or comment](#) | [Format](#) | [Transforms](#) | [Puzzles](#) | [Hot](#) | [Classics](#)
[More pages](#) | [Superseeker](#) | Maintained by N. J. A. Sloane (njas@research.att.com)

[Last modified Tue Feb 17 18:05:31 EST 2004. Contains 91600 sequences.]

[home](#) | [people](#) | [projects](#) | [research areas](#) | [resources](#) |

Terms and Conditions. Privacy Policy.
Copyright 2003 © AT&T. All Rights Reserved.
Send comments to Webmaster@research.att.com.

Exercises

1. Write down the 4-bit reflected Gray code.
2. Write down the sequence corresponding to which bit is negated at each step in the reflected Gray code.
3. Write a program (in any language) that produces the n -bit reflected Gray code.
4. Find the ranking function for the reflected Gray code.
5. Find the unranking function for the reflected Gray code.
6. Find all the 3-bit Gray codes.

The mid-levels conjecture

Graph theory and combinatorics abounds with simple-to-state unsolved problems. One of these is the *mid-levels* conjecture:

Conjecture (Mid-Levels Conjecture)

The subsets of size n and $n + 1$ of a set of size $2n + 1$ can be arranged in a cyclic order in such a way that successive elements differ only by a single element.

This is asking for the existence of a hamilton cycle through the subgraph of the $(2n + 1)$ -cube induced by the subsets of size n and $n + 1$. If we draw the $(2n + 1)$ -cube with all the subsets of a given size on one horizontal line, then these form the two middle levels.

Combinatorial Enumeration: Theory and Practice

Gordon Royle

Semester 1, 2004

k -subsets

For many applications we wish to only consider subsets of a fixed size — the k -subsets of an n -set.

There are two common orderings used to list k -subsets, shown here for 2-subsets of a 5-set.

► Lexicographic

12, 13, 14, 15, 23, 24, 25, 34, 35, 45

► Co-lexicographic

12, 13, 23, 14, 24, 34, 15, 25, 35, 45

Note: Here we are using 12 as shorthand for $\{1, 2\}$.

Enumeration

Theorem

The number of k -subsets of an n -set is given by the binomial coefficient

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Proof.

The number of *sequences* of k distinct elements from an n -set is

$$n(n-1)(n-2) \cdots (n-k+1).$$

Every k -subset will occur in $k!$ different orders in this list of sequences, and so the total number of k -subsets is

$$\frac{n(n-1)(n-2) \cdots (n-k+1)}{k!}.$$

Binomial Identities

A significant area of “classical” combinatorics is the discovery and proof of the many *binomial identities* relating appropriate binomial coefficients.

For example,

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$$

Many of these identities can be proved in two ways - an *algebraic* proof or a *combinatorial* proof.

Algebraic Proofs

Algebraic proofs simply involve manipulation of the formulas to get the stated identity.

$$\begin{aligned} & \binom{n}{k-1} + \binom{n}{k} \\ &= \frac{n!}{(n - (k - 1))!(k - 1)!} + \frac{n!}{(n - k)!k!} \\ &= \frac{kn! + (n + 1 - k)n!}{(n + 1 - k)!k!} \\ &= \binom{n + 1}{k} \end{aligned}$$

Combinatorial Proofs

A combinatorial proof aims to *explain* the identity, rather than simply verify it.

Suppose there are $n + 1$ objects, one of which is “distinguished” from the others. Any k -subset of this set either

- ▶ contains the distinguished object, or
- ▶ doesn't contain the distinguished object.

There are $\binom{n}{k-1}$ sets in the first category and $\binom{n}{k}$ in the second category and so the stated identity holds.

A combinatorial proof is usually viewed as conveying more information than an algebraic proof, but there are many situations where only an algebraic proof is known.

Exercise

Find a combinatorial proof of the following identity:

$$\sum_{k=0}^n \binom{n}{k}^2 = \binom{2n}{n}$$

Hint: Consider the $2n$ objects as consisting of two groups of n objects.

The odometer principle

Lexicographic order is related to the “odometer” principle used in a car odometer: increase the least significant digit if possible, and otherwise roll that digit over to 0 and increase the next least significant digit.

1	4	3	2	2
---	---	---	---	---

1	4	3	2	3
---	---	---	---	---

2	3	7	9	9
---	---	---	---	---

2	3	8	0	0
---	---	---	---	---

Representing a k -set

We will represent a k -set T by a sequence (or array) listing its elements in increasing order

$$t_1 < t_2 < \dots < t_k,$$

which we can view as a sort of k -digit odometer

t_1	t_2	\dots	t_k
-------	-------	---------	-------

with strange properties.

Example: 3-subsets of a 7-set

This “odometer” starts at the smallest possible value

1	2	3
---	---	---

because no digits can be repeated.

Using the odometer principle is easy for the first few successors:

1	2	4
1	2	5
1	2	6
1	2	7

Successor of $\{1, 2, 7\}$

We cannot increase the last position any more, so we

- ▶ propagate the increase one position to the left, and
- ▶ put the lowest possible value in the last position.

1	2	7
1	3	4

If the next position over is already in its highest possible position, then the increase must be propagated further to the left:

1	6	7
2	3	4

In GAP

```
nextLex := function(T,n,k) local S,pos,i;
  pos := k;
  while (pos > 0) and (T[pos] = n+pos-k) do
    pos := pos-1;
  od;
  if (pos = 0) then
    S := [1..k];
  else
    S := T;
    S[pos] := S[pos]+1;
    for i in [pos+1..k] do
      S[i] := S[i-1]+1;
    od;
  fi;
  return S;
end;
```

Ranking

A ranking function is much less pleasant to calculate for this ordering — for example, consider finding the rank of $\{2, 5, 7\}$ in the ordering of 3-subsets of a 7-set.

This equivalent to finding the number of sets that occur *before* $\{2, 5, 7\}$ in the ordering, which are the sets of the form:

1	?	?
2	3	?
2	4	?
2	5	6

The key to counting these is to observe that the number of each type is just a binomial coefficient, and in fact we have

$$\binom{6}{2} + \binom{4}{1} + \binom{3}{1} + 1 = 23.$$

Ranking (cont.)

The number of subsets before

$$t_1 t_2 \cdots t_k$$

is the sum of the numbers of subsets that

- ▶ Start with u_1 , where $u_1 < t_1$, or
- ▶ Start with $t_1 u_2$ where $u_2 < t_2$, or
- ▶ Start with $t_1 t_2 u_3$ where $u_3 < t_3$, or
- ▶ ...
- ▶ Start with $t_1 t_2 \cdots t_{k-1} u_k$ where $u_k < t_k$.

Ranking (cont.)

The number of subsets whose i lowest values are

$$t_1 \ t_2 \ \dots t_i$$

is

$$\binom{n - t_i}{k - i}$$

because the remaining positions determine a $k - i$ subset chosen from a set of size $n - t_i$.

Ranking (cont.)

So, the number of subsets that start with u_1 , where $u_1 < t_1$ is

$$\sum_{j=1}^{t_1-1} \binom{n-j}{k-1}$$

with the index j running over all the feasible values for u_1 .
Similarly the number of subsets that start with $t_1 u_2$ is

$$\sum_{j=t_1+1}^{t_2-1} \binom{n-j}{k-2}$$

again with the index j running over all possible values for u_2
(notice that the lowest possible value for u_2 is $t_1 + 1$).

The final expression

The rank of the subset $\{t_1, t_2, \dots, t_k\}$ is

$$\sum_{i=1}^k \left(\sum_{j=t_{i-1}+1}^{t_i-1} \binom{n-j}{k-i} \right)$$

where $t_0 = 0$.

(This is the kind of equation that you derive once, then program in a reusable manner and hope you never have to derive again!)

Colexicographic order

The other ordering on k -sets that is common is called *colexicographic* order. To determine this order, we represent a k -set by a sequence t_1, t_2, \dots, t_k with the property that

$$t_1 > t_2 > \dots > t_k.$$

Set	Representative	Set	Representative
$\{1, 2, 3\}$	321	$\{1, 2, 4\}$	421
$\{1, 2, 5\}$	521	$\{1, 3, 4\}$	431
$\{1, 3, 5\}$	531	$\{1, 4, 5\}$	541
$\{2, 3, 4\}$	432	$\{2, 3, 5\}$	532
$\{2, 4, 5\}$	542	$\{3, 4, 5\}$	543

Colexicographic order (cont)

Colexicographic (colex) order is then defined by listing these representatives in normal lexicographic order:

321, 421, 431, 432, 521, 531, 532, 541, 542, 543

One of the important properties of colex order is that the ordering does not depend on n . More precisely, the colex ordering for the k -subsets of an n -set is the leading portion of the colex ordering for the k -subsets of an $(n + 1)$ -set.

Colex successors

It is quite easy to find a successor function for colex order.

To find the successor of

$$T = \{t_1, t_2, \dots, t_k\}$$

do the following steps:

- ▶ Find the largest index i such that $t_{i-1} \neq t_i + 1$.
- ▶ Increase t_i by 1.
- ▶ Replace t_{i+1}, \dots, t_k by $k - i, \dots, 2, 1$

Example successor

To find the successor of $[8, 5, 4, 3, 2]$ in colex order.

- ▶ The specified index is $i = 2$

$[8, 5, 4, 3, 2]$

- ▶ Increase t_i by 1

$[8, 6, 4, 3, 2]$

- ▶ Replace $t_3 \dots t_5$ with $3, 2, 1$

$[8, 6, 3, 2, 1]$

Colex rank

How many k -sets occur before $T = \{t_1, t_2, \dots, t_k\}$ in the colex order? Once again we can divide them into k groups:

- ▶ Those starting u_1 where $u_1 < t_1$, or
- ▶ Those starting $t_1 u_2$ where $u_2 < t_2$, or
- ▶ Those starting $t_1 t_2 u_3$ where $u_3 < t_3$, or
- ▶ ...
- ▶ Those starting $t_1 t_2 \cdots t_{k-1} u_k$ where $u_k < t_k$.

This sum is much easier to calculate than the corresponding sum for lexicographic order.

Colex rank (cont.)

The number of subsets whose largest element is less than t_1 is simply the number of k subsets of the set $\{1, 2, \dots, t_1 - 1\}$, which is

$$\binom{t_1 - 1}{k}.$$

Similarly, those starting with t_1 but then having no other element larger than t_2 is

$$\binom{t_2 - 1}{k - 1}.$$

Continuing in this fashion we get

$$r(\{t_1, t_1, \dots, t_k\}) = \sum_{i=1}^k \binom{t_i - 1}{k - (i - 1)}.$$

In GAP

```
coLexRank := function(T,k) local rk,i;

  rk := 0;
  for i in [1..k] do
    rk := rk + Binomial(T[i]-1,k-(i-1));
  od;

  return rk;

end;
```

Permutations

A *permutation* is defined to be a one-to-one mapping

$$\pi : \{1, \dots, n\} \rightarrow \{1, \dots, n\}.$$

We can express a permutation by listing the images of each element of the domain under this mapping:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix}$$

It should be clear that the number of permutations of *degree* n is

$$n(n-1)(n-2) \cdots 1 = n!.$$

Permutations of degree 4

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

Image notation

This notation can be condensed a bit by dropping the top line, and simply giving the list of images in order:

$$[\pi(1), \pi(2), \dots, \pi(n)].$$

So the 24 permutations of degree 4 are:

$[1, 2, 3, 4]$ $[1, 2, 4, 3]$ $[1, 3, 2, 4]$ $[1, 3, 4, 2]$ $[1, 4, 2, 3]$ $[1, 4, 3, 2]$
 $[2, 1, 3, 4]$ $[2, 1, 4, 3]$ $[2, 3, 1, 4]$ $[2, 3, 4, 1]$ $[2, 4, 1, 3]$ $[2, 4, 3, 1]$
 $[3, 1, 2, 4]$ $[3, 1, 4, 2]$ $[3, 2, 1, 4]$ $[3, 2, 4, 1]$ $[3, 4, 1, 2]$ $[3, 4, 2, 1]$
 $[4, 1, 2, 3]$ $[4, 1, 3, 2]$ $[4, 2, 1, 3]$ $[4, 2, 3, 1]$ $[4, 3, 1, 2]$ $[4, 3, 2, 1]$

Cycle Notation

Another notation that is frequently used is *cycle notation*. Given a permutation π consider the sequence of values

$$1, \pi(1), \pi^2(1) = \pi(\pi(1)), \pi^3(1), \dots$$

obtained by repeatedly applying the mapping π .

This sequence must eventually return to 1 and the sequence of values obtained is called a *cycle* of the permutation.

For example, if $\pi_1 = [4, 3, 1, 2]$ then we get

$$1 \rightarrow 4 \rightarrow 2 \rightarrow 3 \rightarrow 1$$

which is expressed more succinctly as

$$(1, 4, 2, 3).$$

Cycle Notation (cont.)

The cycle that starts with 1 may not include all the elements of $\{1, 2, 3, 4\}$, but by starting with an unused element we can obtain another cycle. For example, if $\pi_2 = [2, 1, 4, 3]$, then both $(1, 2)$ and $(3, 4)$ are cycles of π_2 .

We can represent a permutation completely by listing all its cycles:

$$\pi_1 = (1, 4, 2, 3) \quad \pi_2 = (1, 2)(3, 4).$$

This representation is not unique, because we could equally well say that

$$\pi_1 = (4, 2, 3, 1)$$

but by convention we express each cycle by putting its smallest element first.

Permutations of degree 4

In cycle notation, the 24 permutations of degree 4 are:

$(1)(2)(3)(4)$	$(1)(2)(3, 4)$	$(1)(2, 3)(4)$	$(1)(2, 3, 4)$
$(1)(2, 4, 3)$	$(1)(2, 4)(3)$	$(1, 2)(3)(4)$	$(1, 2)(3, 4)$
$(1, 2, 3)(4)$	$(1, 2, 3, 4)$	$(1, 2, 4, 3)$	$(1, 2, 4)(3)$
$(1, 3, 2)(4)$	$(1, 3, 4, 2)$	$(1, 3)(2)(4)$	$(1, 3, 4)(2)$
$(1, 3)(2, 4)$	$(1, 3, 2, 4)$	$(1, 4, 3, 2)$	$(1, 4, 2)(3)$
$(1, 4, 3)(2)$	$(1, 4)(2)(3)$	$(1, 4, 2, 3)$	$(1, 4)(2, 3)$

Fixed points

Cycles of length 1 are called *fixed points* and are usually omitted from the cycle notation.

	$(3, 4)$	$(2, 3)$	$(2, 3, 4)$
$(2, 4, 3)$	$(2, 4)$	$(1, 2)$	$(1, 2)(3, 4)$
$(1, 2, 3)$	$(1, 2, 3, 4)$	$(1, 2, 4, 3)$	$(1, 2, 4)$
$(1, 3, 2)$	$(1, 3, 4, 2)$	$(1, 3)$	$(1, 3, 4)$
$(1, 3)(2, 4)$	$(1, 3, 2, 4)$	$(1, 4, 3, 2)$	$(1, 4, 2)$
$(1, 4, 3)$	$(1, 4)$	$(1, 4, 2, 3)$	$(1, 4)(2, 3)$

It is not very convenient having a blank symbol for the identity mapping, so we usually use either $()$ or a symbol such as e or id .

Lexicographic Order

The order used above for the permutations was, once again, lexicographic order on the permutations expressed in image notation.

It is possible to define a successor function for permutations in lexicographic order, but the details are surprisingly complicated, so instead we will just specify a pair of ranking/unranking functions.

These hinge on the observation that the permutations with a fixed value of $\pi(1)$, say $\pi(1) = a$, all have the form

$$[a, \pi(2), \pi(3), \dots, \pi(n)]$$

where $[\pi(2), \pi(3), \dots, \pi(n)]$ is a permutation of $\{1, 2, \dots, n\} \setminus \{a\}$.

Ranking

Therefore the rank of π is equal to the sum of the following two numbers

- ▶ $(a - 1)(n - 1)!$ for the permutations that have $\pi(1) < a$, and
- ▶ The rank of $[\pi(2), \pi(3), \dots, \pi(n)]$ within the list of permutations of $\{1, 2, \dots, n\} \setminus \{a\}$.

If we form π' from $[\pi(2), \pi(3), \dots, \pi(n)]$ by subtracting 1 from every value greater than a , then π' is a permutation of $\{1, 2, \dots, n - 1\}$ and its (normal) rank is the second value above.

Example

The rank of the permutation $[3, 4, 1, 2, 5]$ is equal to

- ▶ $4! \times 2$ for the permutations with $\pi(1) = 1, 2$, plus
- ▶ The rank of $[4, 1, 2, 5]$ within the permutations of $\{1, 2, 4, 5\}$ which is equal to the rank of $[4 - 1, 1, 2, 5 - 1] = [3, 1, 2, 4]$.

Proceeding recursively we see that:

$$\begin{aligned} r([3, 4, 1, 2, 5]) &= 48 + r([3, 1, 2, 4]) \\ &= 48 + 12 + r([1, 2, 3]) \\ &= 60. \end{aligned}$$

Factorial Notation

Unranking a permutation depends on an interesting representation of a number known as the *factorial representation*. A normal decimal number, such as 5476 is a compressed positional notation for

1000s	100s	10s	1s
5	4	7	6

Rather than using the values 10^0 , 10^1 , 10^2 and so on as the values associated with each position, we use $1!$, $2!$, $3!$,

$7!$	$6!$	$5!$	$4!$	$3!$	$2!$	$1!$
1	0	3	3	0	2	0

Uniqueness

If each “digit” d_i in a factorial representation

$$\cdots d_3 d_2 d_1$$

satisfies the condition that $d_i \leq i$, then every natural number has a unique factorial representation!

This is a relatively straightforward but interesting proof, in that it requires us to show

- ▶ Every natural number has *some* factorial representation, and
- ▶ No natural number has *more than one* factorial representation.

Exercise: Prove this.

Unranking

In order to unrank the integer r , we first find its factorial representation. For example

$$60 = 0 \times 5! + 2 \times 4! + 2 \times 3! + 0 \times 2! + 0 \times 1! = 2200.$$

The first digit $d_4 = 2$ tells us that $\pi(1) = 3$, and that the permutation $[\pi(2), \pi(3), \pi(4), \pi(5)]$ has rank $60 - 48 = 12$ among the permutations of $\{1, 2, 4, 5\}$.

We can (recursively) calculate the permutation with rank 12 among the permutations of $\{1, 2, 3, 4\}$ and then transform it to a permutation of $\{1, 2, 4, 5\}$ by incrementing each value that is greater than or equal to 3.

Fixed Points

A classic result in combinatorics is the enumeration of *derangements* — permutations with no fixed points.

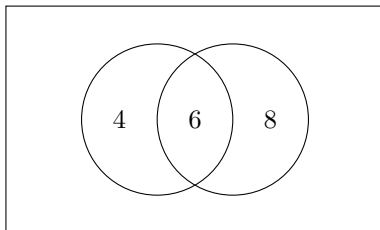
For $n = 4$ there are

- ▶ 9 derangements
- ▶ 8 permutations with 1 fixed point
- ▶ 6 permutations with 2 fixed points
- ▶ 1 permutation with 4 fixed points

Inclusion/Exclusion

Calculating the number of derangements uses an important counting technique called the *principle of inclusion/exclusion*, which we illustrate with a simple example:

- ▶ In a high-school class of 25 children, there are 10 who play cricket, 14 who play football and 6 who play both. How many children play neither sport?



We can calculate the number by calculating separately the number of cricket-but-not-football players ($10 - 6$), football-but-not-cricket players ($14 - 6$) and both-cricket-and-football players (6) and subtracting these from the total.

$$\begin{aligned} 7 &= 25 - (10 - 6) - (14 - 6) - 6 \\ &= 25 - (10 + 14) + 6 \end{aligned}$$

The re-arranged version on the second line shows that we could have obtained the same result by starting with the total number of students, subtracting the football players and the cricket players, and then *adding back* the number who play both.

Inclusion/Exclusion for two or three sets

If A and B are subsets of X , then the number of elements that are not in either A or B is

$$|X| - (|A| + |B|) + (|A \cap B|).$$

If A , B and C are subsets of X , then the number of elements of X that are not in any of A , B or C is

$$|X| - (|A| + |B| + |C|) + (|A \cap B| + |A \cap C| + |B \cap C|) - (|A \cap B \cap C|).$$

Principle of Inclusion/Exclusion

If A_1, A_2, \dots, A_n are all subsets of a set X then for any index set $\mathcal{I} \subseteq X$, define

$$A_{\mathcal{I}} = \bigcap_{i \in \mathcal{I}} A_i$$

(where we take $A_{\emptyset} = X$).

Principle of Inclusion/Exclusion

The number of elements of X that do not belong to any of the sets A_1, A_2, \dots, A_n is given by

$$\sum_{\mathcal{I} \subseteq \{1, 2, \dots, n\}} (-1)^{|\mathcal{I}|} |A_{\mathcal{I}}|.$$

Derangements of degree 4

To count the derangements of degree 4, let X be the set of all permutations of degree 4, and for $1 \leq i \leq 4$, let A_i be the set of permutations that fix i . Then the number of permutations that fix *no* points is equal to:

$$24 - (6 + 6 + 6 + 6) + (2 + 2 + 2 + 2 + 2 + 2) - (1 + 1 + 1 + 1) + 1$$

because

$$|A_i| = 6$$

$$|A_i \cap A_j| = 2$$

$$|A_i \cap A_j \cap A_k| = 1$$

for any choices of distinct i, j and k .

Derangements

It is immediate that the number of derangements of degree n is

$$\sum_{i=0}^{i=n} (-1)^i \binom{n}{i} (n-i)!$$

Expanding the binomial coefficient, this reduces to

$$\sum_{i=0}^{i=n} (-1)^i \frac{n!}{i!} = n! \sum_{i=0}^{i=n} \frac{(-1)^i}{i!}.$$

Is this a *good* answer?

An infinite series

As $n!$ is the total number of permutations we see that the *fraction* of them that are derangements is found by summing the $n + 1$ leading terms of the series

$$\frac{1}{0!} - \frac{1}{1} + \frac{1}{2} - \frac{1}{6} + \frac{1}{24} - \frac{1}{120} + \frac{1}{720} + \dots$$

This series converges quickly:

n	Fraction
2	0.5000
3	0.3333
4	0.3750
5	0.3667
6	0.3681
7	0.3679
8	0.3679

A good answer

Recall that the Taylor series of a suitably differentiable function is

$$f(x) \approx f(0) + xf'(0) + \frac{x^2}{2!}f''(0) + \frac{x^3}{3!}f'''(0) + \cdots + \frac{x^n}{n!}f^{(n)}(0).$$

If we take $f(x) = e^{-x}$ then the derivatives of this function are $-e^{-x}$, e^{-x} , $-e^{-x}$, etc, so by putting $x = 1$, we get

$$e^{-1} = 1 - 1 + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \cdots$$

With a little bit more work we get the final result:

Theorem

The number of derangements of degree n is given by the closest integer to $n!/e$.

The corresponding sequence is given by [OEIS A000166](#)

Using symmetry for enumeration

Cheryl E Praeger

Semester 1, 2004

Multiplying Permutations

Let $X = \{1, 2, 3, 4, 5\}$. Following Cameron, I use g, h, \dots for permutations.

$g = (123)(45)$	$1 \rightarrow 2 \rightarrow 3 \rightarrow 1, \quad 4 \leftrightarrow 5$ so $1g = 2, 2g = 3$ etc
$h = (1)(2345)$ or (2345)	$1 \rightarrow 1, \quad 2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 2$

To compute $g \circ h$: do g first and then h .

$$g \circ h: \quad 1 \leftrightarrow 3, \quad 2 \leftrightarrow 4, \quad 5 \rightarrow 5$$

$$\text{Hence } g \circ h = ((123)(45)) \circ ((2345)) = (13)(24).$$

We usually write $g \circ h$ as gh .

Symmetric group on $X = \{1, 2, \dots, n\}$

$\text{Sym}(X) = S_n$ is the group of all permutations of X under composition.

► **identity** written 1 or 1_X is $(1)(2) \dots (n)$

► **inverses** $g \circ g^{-1} = 1$

For a cycle just reverse the order: $(1234)^{-1} = (4321)$.

Do this to each cycle for general permutations in cycle notation. Note our convention is to write (4321) as (1432) .

$((123)(4897))^{-1} = (321)(7984) = (132)(4798)$

Warning: in general $(g \circ h)^{-1} = h^{-1} \circ g^{-1}$

Permutation group on X is a subgroup G of $\text{Sym}(X)$.

Just a subset closed under composition: $g, h \in G \Rightarrow g \circ h \in G$

Some examples

Take $X = \{1, 2, \dots, n\}$.

$\text{Sym}(X)$ is the largest permutation group on X : $|\text{Sym}(X)| = n!$

Some examples

Take $X = \{1, 2, \dots, n\}$.

$\text{Sym}(X)$ is the largest permutation group on X : $|\text{Sym}(X)| = n!$

Some smaller examples: $\{1, (12)\}$ $\{1, (345), (354)\}$

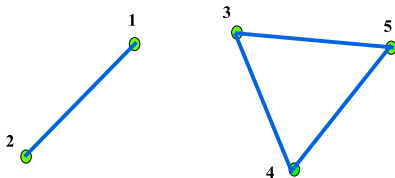
Examples: cont

Take $X = \{1, 2, 3, 4, 5\}$.

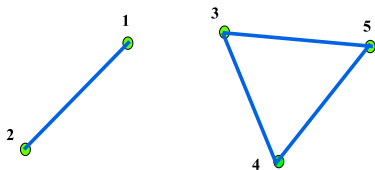
So X is the vertex set
of a graph with edge set

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

Try to spot some **automorphisms** of the graph (edge-preserving permutations of the vertices).

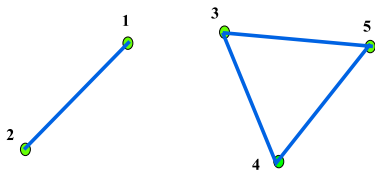


Let $G = \langle (12), (345) \rangle$.
(group given by generators)



Then $G = \{1, (12), (345), (354), (12)(345), (12)(354)\}$.

Let $G = \langle (12), (345) \rangle$.
(group given by generators)



Then $G = \{1, (12), (345), (354), (12)(345), (12)(354)\}$.

We often get permutation groups arising like this in combinatorics.

Can you spot any other automorphisms? If so add them as extra generators. GAP can be used to find the full automorphism group.

Orbits and Stabilisers

$$X = \{1, 2, 3, 4, 5\} \quad \text{and}$$

$$G = \{1, (12), (345), (354), (12)(345), (12)(354)\}.$$

Orbit of $G \leq \text{Sym}(X)$ containing $i \in X$ is $i^G = \{ig \mid g \in G\}$

Orbits and Stabilisers

$$X = \{1, 2, 3, 4, 5\} \quad \text{and}$$

$$G = \{1, (12), (345), (354), (12)(345), (12)(354)\}.$$

Orbit of $G \leq \text{Sym}(X)$ containing $i \in X$ is $i^G = \{ig \mid g \in G\}$

$$1^G = 2^G = \{1, 2\} \quad \text{and} \quad 3^G = 4^G = 5^G = \{3, 4, 5\}.$$

Orbits and Stabilisers

$$X = \{1, 2, 3, 4, 5\} \quad \text{and}$$

$$G = \{1, (12), (345), (354), (12)(345), (12)(354)\}.$$

Orbit of $G \leq \text{Sym}(X)$ containing $i \in X$ is $i^G = \{ig \mid g \in G\}$

$$1^G = 2^G = \{1, 2\} \quad \text{and} \quad 3^G = 4^G = 5^G = \{3, 4, 5\}.$$

Stabiliser in G of i is $G_i = \{g \in G \mid ig = i\}.$

G_i is a subgroup of G (why?)

Orbits and Stabilisers

$$X = \{1, 2, 3, 4, 5\} \quad \text{and}$$

$$G = \{1, (12), (345), (354), (12)(345), (12)(354)\}.$$

Orbit of $G \leq \text{Sym}(X)$ containing $i \in X$ is $i^G = \{ig \mid g \in G\}$

$$1^G = 2^G = \{1, 2\} \quad \text{and} \quad 3^G = 4^G = 5^G = \{3, 4, 5\}.$$

Stabiliser in G of i is $G_i = \{g \in G \mid ig = i\}.$

G_i is a subgroup of G (why?)

$$G_1 = \{1, (345), (354)\} \quad \text{Notice: } |G_1| \cdot |1^G| = 3 \times 2 = 6 = |G|$$

Orbits and Stabilisers

$$X = \{1, 2, 3, 4, 5\} \quad \text{and}$$

$$G = \{1, (12), (345), (354), (12)(345), (12)(354)\}.$$

Orbit of $G \leq \text{Sym}(X)$ containing $i \in X$ is $i^G = \{ig \mid g \in G\}$

$$1^G = 2^G = \{1, 2\} \quad \text{and} \quad 3^G = 4^G = 5^G = \{3, 4, 5\}.$$

Stabiliser in G of i is $G_i = \{g \in G \mid ig = i\}.$

G_i is a subgroup of G (why?)

$$G_1 = \{1, (345), (354)\} \quad \text{Notice: } |G_1| \cdot |1^G| = 3 \times 2 = 6 = |G|$$

$$G_3 = \{1, (12)\} \quad \text{Again: } |G_3| \cdot |3^G| = 2 \times 3 = 6 = |G|$$

Orbit-Stabiliser Theorem

For any $G \leq \text{Sym}(X)$, and any point $i \in X$, $|G_i| \cdot |i^G| = |G|$.

Orbit-Stabiliser Theorem

For any $G \leq \text{Sym}(X)$, and any point $i \in X$, $|G_i| \cdot |i^G| = |G|$.

Proof Write $i^G = \{i_1, \dots, i_r\}$ and $H = G_i = \{h_1, \dots, h_s\}$.

Choose elements $g_1 = 1, g_2, \dots, g_r$ such that $ig_j = i_j$ for each j .

Arrange (some of) the group elements like this.

h_1g_1	h_1g_2		h_1g_r
h_2g_1	h_2g_2		h_2g_r
\vdots	\vdots	\dots	\vdots
h_sg_1	h_sg_2		h_sg_r

Orbit-Stabiliser Theorem

For any $G \leq \text{Sym}(X)$, and any point $i \in X$, $|G_i| \cdot |i^G| = |G|$.

Proof Write $i^G = \{i_1, \dots, i_r\}$ and $H = G_i = \{h_1, \dots, h_s\}$.

Choose elements $g_1 = 1, g_2, \dots, g_r$ such that $ig_j = i_j$ for each j .

Arrange (some of) the group elements like this.

h_1g_1	h_1g_2		h_1g_r
h_2g_1	h_2g_2		h_2g_r
\vdots	\vdots	\dots	\vdots
h_sg_1	h_sg_2		h_sg_r

The elements in column j form the coset Hg_j . Every element in Hg_j maps i to i_j . So this table contains exactly $r \cdot s$ distinct elements of G .

Orbit-Stabiliser Proof continued

Claim: every $g \in G$ appears exactly once in this table.

$h_1 g_1$	$h_1 g_2$		$h_1 g_r$
$h_2 g_1$	$h_2 g_2$		$h_2 g_r$
\vdots	\vdots	\dots	\vdots
$h_s g_1$	$h_s g_2$		$h_s g_r$

Find ig . By definition of orbit, $ig \in i^G$ so $ig = i_j$ for some j .

Compute $h := gg_j^{-1}$. (Remember: g first, and then g_j^{-1} .)

Then $h : i \rightarrow i$ so $h \in H = G_1$.

Hence $g = hg_j$ lies in column j .

Counting:

$|G| = \text{number of elements in the table} = r \cdot s = |i^G| \cdot |G_i|$.

Using the Orbit-Stabiliser Theorem

Let's run through another example: $X = \{1, 2, 3, 4, 5\}$.

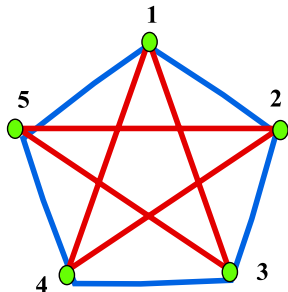
$$G = \langle (12345), (2354) \rangle.$$

$$1^G = \{1, 2, 3, 4, 5\}$$

Just one G -orbit in X :
 G called **transitive**.

Clearly $(2354) \in G_1$ so
 $\langle (2354) \rangle \leq G_1$. Hence $|G_1| \geq 4$.

Use GAP to prove $|G| = 20$.
So $|G_1| = |G|/|1^G| = 20/5 = 4$.
Hence $G_1 = \langle (2354) \rangle$.



Orbit-Stabiliser Theorem for actions

So what's an action? Each element of $G = \langle (12345), (2354) \rangle$

either

$\{ \text{blue edges} \} \leftrightarrow \{ \text{red edges} \}$

or fixes setwise

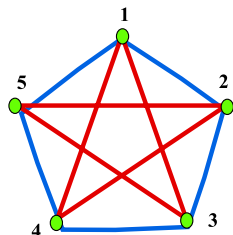
$\{ \text{blue edges} \}$ and $\{ \text{red edges} \}$

Elements of G induce permutations
of $Y = \{ \text{blue edges}, \text{red edges} \}$.

We say that G acts on Y
(unfaithfully).

The Orbit-Stabiliser theorem also works for actions:

$$|G| = |\text{blue edges}|^G \cdot |G_{\text{blue edges}}| = 2 \times 10.$$



Some GAP code for working with permutation groups

```
gap> a := (1, 2);  
(1, 2)  
gap> b := (3, 4, 5);  
(3, 4, 5)  
gap> b^-1;  
(3, 5, 4)  
gap> a * b;  
(1, 2)(3, 4, 5)  
gap> g := Group(a, b);  
Group([(1, 2), (3, 4, 5)])  
gap> Order(g);  
6
```


And GAP code for orbits and stabilisers

```
gap> Orbit(g, 1);  
#This lists the points in the  $g$ -orbit containing 1  
[1, 2]  
gap> Orbits(g); #This list the  $g$ -orbits.  
[[1, 2], [3, 4, 5]]  
We can assign names for lists: gap> o := Orbits(g);  
[[1, 2], [3, 4, 5]]  
and address various entries in the list: gap> o[1];  
[1, 2]  
gap> Length(o[1]);  
2  
gap> g1 := Stabilizer(g, 1);  
#GAP returns a set of generators for  $g_1$ .  
Group([(3, 4, 5)])  
gap> Order(g1);  
3
```

Two ways to verify with GAP the Orbit-Stabiliser Theorem

```
gap> Order(g1) * Length(Orbit(g, 1));
```

```
6
```

```
gap> Order(g1) * Length(Orbit(g, 1)) = Order(g);
```

```
true
```

One more slide to come on the second example.

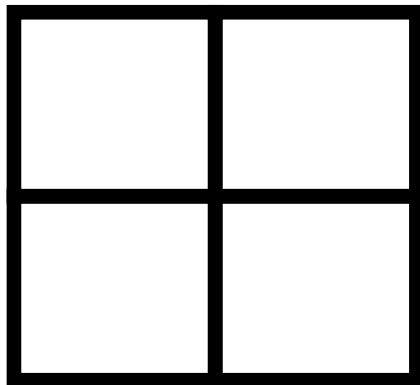
The group on the edge-coloured graph on five vertices

```
gap> a := (1, 2, 3, 4, 5);  
(1, 2, 3, 4, 5)  
gap> b := (2, 3, 5, 4);  
(2, 3, 5, 4)  
gap> G := Group(a, b);  
Group([(1, 2, 3, 4, 5), (2, 3, 5, 4)])  
gap> Order(G);  
20  
gap> IsTransitive(G);  
true  
gap> G1 := Stabilizer(G, 1);  
gap> Order(G1);
```

4 Exercise: Check the Orbit stabiliser Theorem.

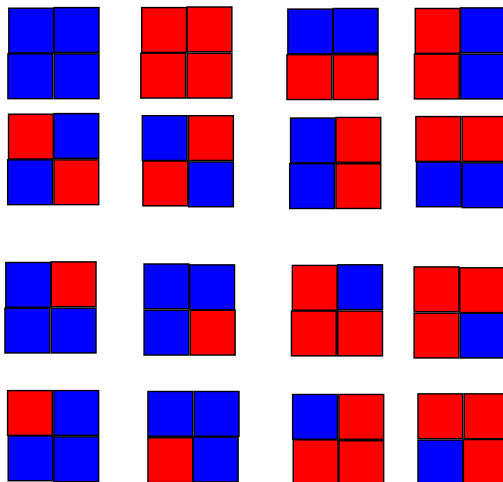
Colouring a grid

In how many different ways can we colour the squares of a 2×2 grid using the colours red and blue?



There are 4 cells and 2 colours; so the number should be $2^4 = 16$.

Here they are



How many coloured grids modulo rotations?

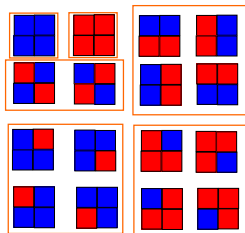
Now suppose that we are allowed to rotate the coloured grids about their centre through $\pi/2, \pi, 3\pi/2, 2\pi$. Some grids will become “indistinguishable from” other grids.

We have just changed the meaning of “different”. Now how many different coloured grids are there?

How many coloured grids modulo rotations?

Now suppose that we are allowed to rotate the coloured grids about their centre through $\pi/2, \pi, 3\pi/2, 2\pi$. Some grids will become “indistinguishable from” other grids.

We have just changed the meaning of “different”. Now how many different coloured grids are there?



Exactly 6. What's going on? How can we compute this number without drawing all 16 coloured grids?

Characters in our drama

Group G consisting of four rotations.

Set S consisting of 16 coloured grids.

G acts on the set S , and

Coloured grids A and B are “indistinguishable” \Leftrightarrow we can map A to B under some rotation in G .

In other words, A and B are “indistinguishable” $\Leftrightarrow A$ and B lie in the same G -orbit in S .

Thus the number of different/indistinguishable coloured grids modulo the rotation group G is equal to the number of G -orbits in S . We would like an easy way to find the number of G -orbits.

Some challenge questions to keep in mind

Suppose you had 3 different colours.

How many coloured grids? $3^4 = 81$

How many different ones up to rotation? i.e. what is the number of orbits under the rotation group?

How many different coloured grids up to rotation if we use k colours?

How many coloured grids up to rotation and/or reflection if we use k colours?

What if we consider $n \times n$ grids in each of these questions?

Orbit Counting Lemma

Let $G \leq \text{Sym}(X)$.

For $g \in G$ let $\text{fix}(g)$ = number of $x \in X$ such that $xg = x$.
i.e. $\text{fix}(g)$ is the number of fixed points of g in X .

Then the number of G -orbits in X

$$\begin{aligned} &= \text{average of } \text{fix}(g) \text{ over all } g \in G \\ &= \frac{1}{|G|} \sum_{g \in G} \text{fix}(g) \end{aligned}$$

Proof of Orbit Counting Lemma

Special Case: G is transitive.

Powerful combinatorial technique:

count pairs (i, g) in two ways ($i \in X, g \in G, ig = i$).

First count: each $g \in G$ paired with $\text{fix}(g)$ points $i \in X$ with $ig = i$

So number of pairs is $\sum_{g \in G} \text{fix}(g)$.

Second count: each $i \in X$ paired with $|G_i|$ elements $g \in G_i$.

So number of pairs is $\sum_{i \in X} |G_i|$.

Orbit Stabiliser Theorem gives: $|G_i| = \frac{|G|}{|iG|} = \frac{|G|}{|X|}$ for each i
(because G is transitive). Hence $\sum_{i \in X} |G_i| = |X| \cdot \frac{|G|}{|X|} = |G|$.

Equate results of first and second counts and get:

$\frac{1}{|G|} \sum_{g \in G} \text{fix}(g) = 1$ (the number of orbits for G transitive).

Proof of Orbit Counting Lemma Continued

General Case: G has $t \geq 2$ orbits X_1, X_2, \dots, X_t .

Let $\text{fix}_i(g)$ = the number of fixed points of g in X_i .

So $\text{fix}(g) = \sum_{1 \leq i \leq t} \text{fix}_i(g)$.

Then G acts on X_i with one orbit (transitive) and since the Orbit Stabiliser Theorem applies to actions, the result for the “Special Case” gives:

$$\frac{1}{|G|} \sum_{g \in G} \text{fix}_i(g) = 1$$

for each i so

$$\frac{1}{|G|} \sum_{g \in G} \text{fix}(g) = \frac{1}{|G|} \sum_{g \in G} \text{fix}_1(g) + \dots + \frac{1}{|G|} \sum_{g \in G} \text{fix}_t(g) = t$$

Revisiting coloured grids

Let R = clockwise rotation through $\pi/2$, and let $G = \{R, R^2, R^3, R^4 = 1\}$.

grids fixed by R	$bbbb$ and $rrrr$	2
grids fixed by R^2	$bbbb, rrrr, brbr, rbrb$	4
grids fixed by R^3	$bbbb$ and $rrrr$	2
grids fixed by $R^4 = 1$	all of them	16
Summing:	$\sum \text{fix}(R^i) =$	24

So $\frac{1}{|G|} \sum_{1 \leq i \leq 4} \text{fix}(R^i) = \frac{1}{4} \cdot 24 = 6$.

Exercises I:

Exercise: Compute the number of different red-blue-green coloured 2×2 grids up to rotation.

Exercise: Find a formula for the number of different red-blue coloured $n \times n$ grids up to rotation (about the centre of the grid).

Exercise: Finish the GAP exercise for the group on the edge-coloured graph on five vertices.

Exercises II

GAP Exercise: Type into GAP: `g := MathieuGroup(11);`
`g` is a permutation group on $X = \{1, 2, \dots, 11\}$.

- ▶ Decide if g is transitive. Also find the order of g .
- ▶ Find g_1 the stabiliser of the point 1. Decide if g_1 is transitive on $X \setminus \{1\}$.
- ▶ Find g_{12} the stabiliser of the points 1 and 2 (or the stabiliser in g_1 of the point 2). Decide if g_{12} is transitive on $X \setminus \{1, 2\}$.
- ▶ Similarly find g_{123} the stabiliser in g_{12} of the point 3. Decide if g_{123} is transitive on $X \setminus \{1, 2, 3\}$.
- ▶ Repeat for the points 4 and 5. Make sense of your answers in terms of the Orbit Stabiliser Theorem.
- ▶ This “remarkable group” was discovered by Mathieu in the 19th century.

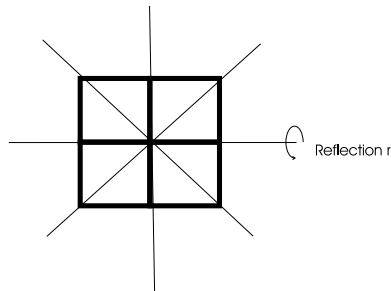
Using symmetry for enumeration II

Cheryl E Praeger

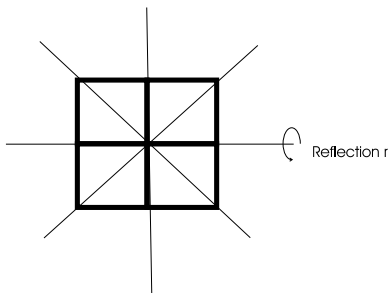
Semester 1, 2004

Dihedral group D_8

Add to the rotation group $G = \{R, R^2, R^3, R^4 = 1\}$ reflections about each of the four axes shown. Take R as anticlockwise rotation by $\pi/2$. Let r be the reflection about the horizontal axis. Then



rR is the reflection
about the SW-NE axis
 rR^2 is the reflection
about the vertical axis
 rR^3 is the reflection
about the NW-SE axis

Dihedral group D_8 continued

Also $R^4 = r^2 = 1$, $rR = R^3r$.

The dihedral group

$$D_8 := \langle R, r \rangle = \{R, R^2, R^3, R^4 = 1, r, rR, rR^2, rR^3\}.$$

General Dihedral Groups D_{2n} 

D20



D12

A regular n -gon is a polygon with n equal length sides and n equal angles.

In this general case take R to be anticlockwise rotation by $2\pi/n$; **reflect** about n axes passing through the midpoints of opposite sides or opposite angles (for n even) or an angle and the midpoint of its opposite side (for n odd). Keeping r as the reflection about the horizontal axis, $R^n = r^2 = 1$, $rR = R^{n-1}r$.

The dihedral group

$D_{2n} := \langle R, r \rangle = \{R, R^2, \dots, R^n = 1, r, rR, rR^2, \dots, rR^{n-1}\}$ has order $2n$. Gordon will be using dihedral groups in his lectures.

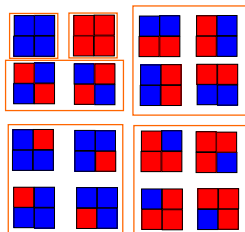
Consider D_8 acting on an $n \times n$ grid

- ▶ First consider D_8 on a single $n \times n$ grid.
- ▶ Next consider D_8 acting on the set of $n \times n$ grids coloured using k colours. There are k^{n^2} of these coloured grids.
- ▶ The number of distinct such grids **modulo rotation and reflection** is the number of D_8 -orbits on this set.

Consider how this new notion of "different" might change the results of our counting.

D_8 on red-blue coloured 2×2 grids

Here are the orbits under the group of four rotations:



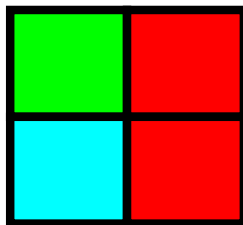
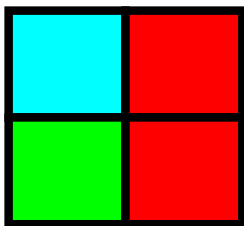
Each of these orbits is fixed setwise by all of the reflections, so there is no change in our concept of “different modulo rotation and reflection” from “different modulo rotation”.

There are still 6 different red-blue coloured grids modulo D_8 . This is not always the case!

D_8 on red-blue-green coloured 2×2 grids

Exercise 1 from last week: you found the number of different red-blue-green coloured 2×2 grids modulo rotation. Answer: 24

Some of these coloured grids can be distinguishable modulo rotations but indistinguishable “modulo rotation and reflection”, that is they can be in different orbits of the rotation group, but in the same orbit of the bigger dihedral group D_8 .



D_8 on red-blue-green coloured 2×2 grids II

Now we want to consider these grids modulo D_8 .

Note: “horizontal reflection” means reflection about the horizontal axis, etc.

grids fixed by R	$rrrr, bbbb$ and $gggg$	3
grids fixed by R^2	$rrrr, \dots, brbr$, etc	9
grids fixed by R^3	$rrrr, bbbb$ and $gggg$	3
grids fixed by $R^4 = 1$	all of them	81
$\sum \text{fix}(R^i) =$		96
horizontal reflection	$rrrr, \dots, rbbr$ etc.	9
vertical reflection	$rrrr, \dots, rrbb$, etc	9
Sw-NE reflection	$rrrr, \dots, rbrg$	27
NW-SE reflection	$rrrr, \dots, rbg b$	27
$\sum_{g \in D_8} \text{fix}(g) =$		168

By the Orbit-Counting Lemma there are $\frac{1}{|D_8|} \cdot 168 = \frac{168}{8} = 21$ different red-blue-green coloured grids modulo D_8 .

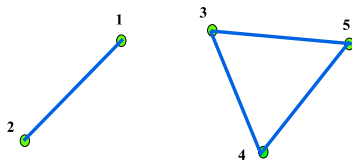
Labelled Graphs

A *labelled graph* $\Gamma = (X, E)$ consists of a “vertex set” X and an “edge set” E , where

$$E \subseteq X^{\{x\}} = \{\{x, y\} \mid x, y \in X, x \neq y\}.$$

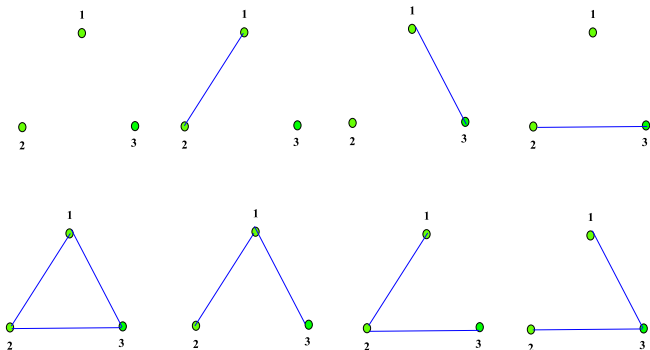
Often we refer to labelled graphs simply as *graphs*.

The graph we saw last week on $X = \{1, 2, 3, 4, 5\}$ is an example. Here $E = \{\{1, 2\}, \{3, 4\}, \{3, 5\}, \{4, 5\}\}$.



Labelled Graphs continued

Here are all the labelled graphs on 3 vertices. Take $X = \{1, 2, 3\}$.



$$\begin{aligned}\text{Number of labelled graphs} &= \text{Number of choices of } E \\ &= \text{Number of subsets of } X^{\{2\}} \\ &= 2^{|X^{\{2\}}|} = 8.\end{aligned}$$

Labelled Graphs continued

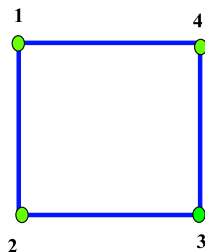
In general if $X = \{1, 2, \dots, n\}$ then we say that the labelled graph $\Gamma = (X, E)$ has *order* n .

Number of labelled graphs of order n

$$= 2^{n(n-1)/2}.$$

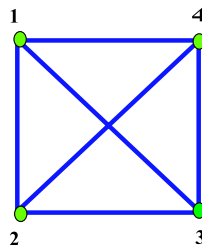
Some useful families of graphs

Cycles C_n



C_4

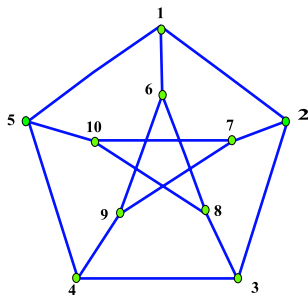
Complete Graphs K_n



K_4

A famous graph — Petersen Graph

A very famous graph: Petersen Graph P of order 10. What is the shortest length of a cycle in P (the *girth* of P)?



How many edges on each vertex (the *degree* or *valency* of each vertex)? — all the same — so P is *regular of valency 3*.

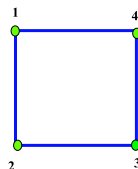
Automorphisms of graphs

An *automorphism* of a labelled graph $\Gamma = (X, E)$ is a permutation $g \in \text{Sym}(X)$ such that g leaves E invariant; that is

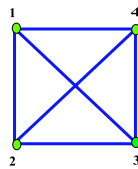
$$\{i, j\} \in E \Rightarrow \{i^g, j^g\} \in E.$$

Example: If $\Gamma = K_n$, then every permutation of $\{1, \dots, n\}$ is an automorphism.

Example: If $\Gamma = C_4$, then rotations, e.g. $g = (1234)$, and reflections, e.g. $g = (13)$ are automorphisms.



C_4



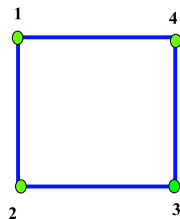
K_4

Automorphism group

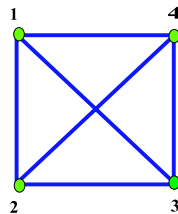
$$\text{Aut}(\Gamma) = \{g \in \text{Sym}(X) \mid g \text{ is an automorphism of } \Gamma\}$$

is a subgroup of $\text{Sym}(X)$ — the *automorphism group* of Γ .

Example: $\text{Aut}(K_n) = S_n$, $\text{Aut}(C_n) = D_{2n}$.



C_4



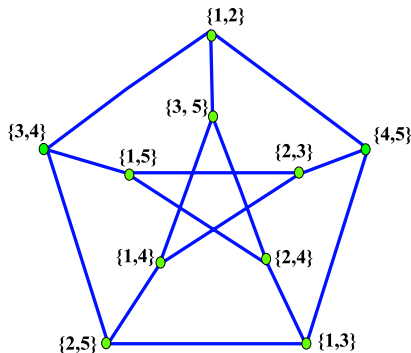
K_4

Automorphism group of Petersen graph

There is a special way of labelling the ten vertices of P :

$$X = \{\{i, j\} \mid 1 \leq i < j \leq 5\}$$

such that vertex $\{i, j\}$ is joined by an edge to vertex $\{a, b\} \Leftrightarrow \{i, j\} \cap \{a, b\} = \emptyset$.



Automorphism group of Petersen graph continued

Any permutation $g \in S_5 = \text{Sym}(\{1, 2, 3, 4, 5\})$ acts as a permutation of X via

$$g : \{i, j\} \longrightarrow \{i^g, j^g\}$$

and maps edges to edges.

Hence $S_5 \subseteq \text{Aut}(P)$. In fact $\text{Aut}(P) = S_5$.

Isomorphism of labelled graphs

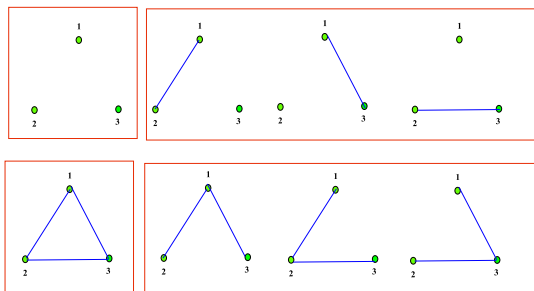
Given $\Gamma_1 = (X_1, E_1)$, $\Gamma_2 = (X_2, E_2)$ with $|X_1| = |X_2| = n$, an *isomorphism* $g : \Gamma_1 \longrightarrow \Gamma_2$ is a bijection $g : X_1 \longrightarrow X_2$ such that

$$\{i, j\} \in E_1 \Leftrightarrow \{i^g, j^g\} \in E_2$$

i.e. edges \longrightarrow edges, and non-edges \longrightarrow non-edges.

- ▶ Γ_1, Γ_2 *isomorphic* if there exists an isomorphism from Γ_1 to Γ_2
- ▶ If $X_1 = X_2 = X = \{1, 2, \dots, n\}$ then an isomorphism is just a permutation $g \in \text{Sym}(X)$ that takes the Γ_1 -edge set onto the Γ_2 -edge set.

Isomorphisms of labelled graphs of order 3

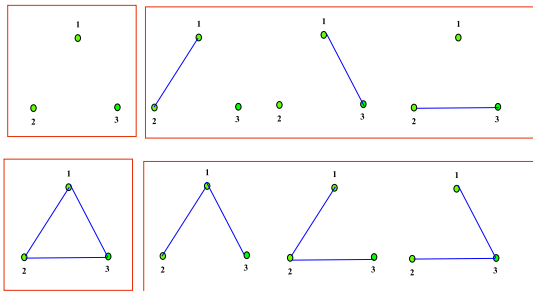


This shows the isomorphism classes of labelled graphs on $X = \{1, 2, 3\}$.

Exercise: For each pair of isomorphic graphs in the diagram write down an isomorphism. When is there more than one choice of an isomorphism?

Action of $\text{Sym}(X)$ on the set of labelled graphs on X

$\text{Sym}(\{1, 2, 3\})$ acts on the labelled graphs on $\{1, 2, 3\}$ and the orbits are the isomorphism classes.



The stabiliser of a labelled graph Γ is $\text{Aut}(\Gamma)$.

Notice how the Orbit Stabiliser Theorem applies here:

$$6 = |\text{Sym}(\{1, 2, 3\})| = |\text{Iso. class of } \Gamma| \cdot |\text{Aut}(\Gamma)|.$$

General rules for this action

$\Gamma = (X, E)$ a labelled graph on $X = \{1, 2, \dots, n\}$

- ▶ $g \in \text{Sym}(X)$; g maps Γ to $\Gamma^g = (X, E^g)$ where $E^g = \{\{i^g, j^g\} \mid \{i, j\} \in E\}$.
- ▶ Stabiliser of Γ is $\text{Aut}(\Gamma)$
- ▶ Size of *isomorphism class* of Γ (the set of all labelled graphs on X that are isomorphic to Γ) is $\frac{n!}{|\text{Aut}(\Gamma)|}$.

Example:

$|\text{Iso. class of Petersen graph}| = \frac{|S_{10}|}{|\text{Aut}(P)|} = \frac{10!}{5!} = 30240$
by the Orbit Stabiliser Theorem.

General rules for this action continued

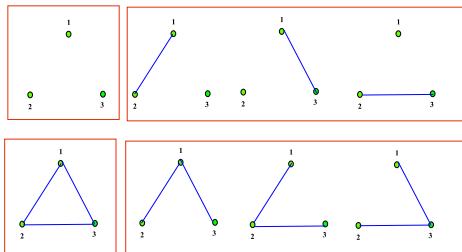
An unlabelled graph on X “is” an isomorphism class of labelled graphs on X .

That is, we “do not distinguish” between graphs Γ_1 and Γ_2 if we can map Γ_1 to Γ_2 by relabelling vertices.

So the number of unlabelled graphs on X = Number of $\text{Sym}(X)$ -orbits on labelled graphs.

E.g. there are 4 unlabelled graphs on $X = \{1, 2, 3\}$.

Using Orbit Counting Lemma



Let $\mathcal{S} = \{\text{labelled graphs on } \{1, 2, 3\}\}$.

g	$\text{fix}(g)$
1	8
(12), (13) or (23)	4
(123) or (132)	2

$$\begin{aligned} \text{Number of unlabelled graphs} &= \frac{1}{|S_3|} \sum_{g \in S_3} \text{fix}(g) \\ &= \frac{1}{6}(8 + 3 \times 4 + 2 \times 2) \\ &= 24/6 = 4. \end{aligned}$$

Automorphism groups are S_3, S_2, S_3, S_2 .

Using Orbit Counting Lemma continued

How to count unlabelled graphs on longer vertex sets

$$X = \{1, 2, \dots, n\}?$$

Let $g \in \text{Sym}(X)$. Then g acts on $X^{\{2\}} = \{\{i, j\} \mid 1 \leq i < j \leq n\}$ by $g : \{i, j\} \longrightarrow \{i^g, j^g\}$.

e.g. $X = \{1, 2, 3, 4\}$, $g = (1234)$, $|X^{\{2\}}| = \binom{4}{2} = 6$.

$$g : \{1, 2\} \rightarrow \{2, 3\} \rightarrow \{3, 4\} \rightarrow \{1, 4\}$$

$$g : \{1, 3\} \leftrightarrow \{2, 4\}$$

So g fixes $\Gamma = (X, E) \Leftrightarrow$

(a) all or none of $\{1, 2\}, \{2, 3\}, \{3, 4\}, \{1, 4\}$ lie in E , and

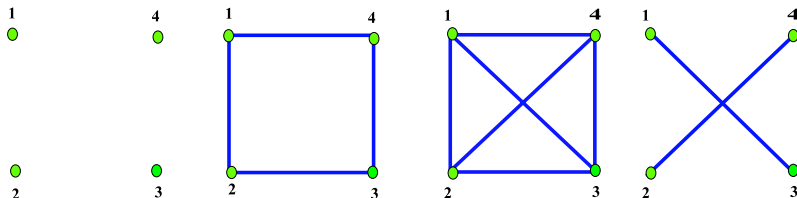
(b) all or none of $\{1, 3\}, \{2, 4\}$ lie in E

$\Leftrightarrow E$ is a union of g -cycles in $X^{\{2\}}$.

Using Orbit Counting Lemma continued

Let $\text{cyc}_2(g) =$ number of g -cycles in $X^{\{2\}}$ (including length 1)

Then g fixes $2^{\text{cyc}_2(g)}$ labelled graphs on X ; in our example $g = (1234)$ fixes exactly the four labelled graphs below.



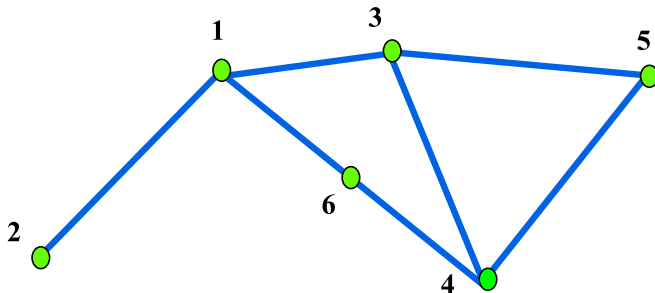
Asymmetric graphs (or rigid graphs)

A labelled graph $\Gamma = (X, E)$ is *asymmetric* (or *rigid*) if $\text{Aut}(\Gamma) = 1$ (no non-trivial automorphisms).

Know: no asymmetric graphs of order 3.

Exercise: show that there is no asymmetric graph of order 4.

Here is an asymmetric graph of order 6. (Why ?)



Is there an asymmetric graph of order 5?

Isomorphism class of asymmetric graph Γ of order n

Has size $\frac{n!}{|\text{Aut}(\Gamma)|} = n!$

While if $\Gamma = (X, E)$ is not asymmetric, then $|\text{Aut}(\Gamma)| \geq 2$, so isomorphism class of Γ has size

$$\frac{n!}{|\text{Aut}(\Gamma)|} \leq \frac{n!}{2}.$$

Summary and Questions

$$X = \{1, 2, \dots, n\}.$$

- ▶ Number of labelled graphs of order $n = 2^{n(n-1)/2}$.
- ▶ Orbit Counting Lemma gives

$$\begin{aligned}\text{Unlab}(n) &= \text{Number of unlabelled graphs of order } n \\ &= \frac{1}{n!} \sum_{g \in S_n} 2^{\text{cyc}_2(g)}\end{aligned}$$

where $\text{cyc}_2(g)$ = number of g -cycles in $X^{\{2\}}$.

- ▶ Order 3: 8 labelled graphs, 4 unlabelled graphs

Summary and Questions continued

$$\begin{aligned} 2^{n(n-1)/2} &= \text{number of labelled graphs of order } n \\ &= \sum_{\text{unlabelled graphs}} |\text{size of iso. class}| \\ &= \sum_{\text{unlabelled graphs}} \frac{n!}{|\text{Aut}(\Gamma)|}. \end{aligned}$$

FACT: Most labelled graphs are asymmetric

Roughly speaking, $\text{Unlab}(n) \sim \frac{2^{n(n-1)/2}}{n!}$.

Lower Bound for $\text{Unlab}(n)$

Let $\text{Asym}(n) = \text{Number of asymmetric labelled graphs of order } n$.

- ▶ Each isomorphism class of these asymmetric graphs has size $n!$
- ▶ So number of isomorphism classes of asymmetric graphs is $\text{Asym}(n)/n!$.
- ▶ There are $2^{n(n-1)/2} - \text{Asym}(n)$ labelled graphs of order n that are not asymmetric.
- ▶ Each isomorphism class of non-asymmetric graphs has size $= \frac{n!}{\text{Aut}(\Gamma)} \leq \frac{n!}{2}$.
- ▶ So Number of isomorphism classes of non-asymmetric graphs is $\geq (2^{n(n-1)/2} - \text{Asym}(n)) \cdot \frac{2}{n!}$.

Lower Bound for $\text{Unlab}(n)$ continued

Hence

$$\begin{aligned}\text{Unlab}(n) &\geq \frac{2}{n!} (2^{n(n-1)/2} - \text{Asym}(n)) + \frac{\text{Asym}(n)}{n!} \\ &= \frac{2^{1+n(n-1)/2}}{n!} - \frac{\text{Asym}(n)}{n!}.\end{aligned}$$

Upper bound for $\text{Unlab}(n)$

$$\text{Unlab}(n) = \frac{1}{n!} \sum_{g \in S_n} 2^{\text{cyc}_2(g)}.$$

Divide $S_n = \text{Sym}(X)$ into 3 classes. Pick even $m \leq n - 2$.

$$C_1 = \{1\}$$

$$C_2 = \{g \in S_n \mid g \text{ moves at most } m \text{ points of } X\}$$

$$C_3 = \{g \in S_n \mid g \text{ moves more than } m \text{ points of } X\}.$$

So

$$|C_1| = 1$$

$$|C_2| \leq \binom{n}{m} m! = n(n-1) \dots (n-m+1)$$

$$< n^m$$

$$|C_3| < n! < n^n.$$

Upper bound for $\text{Unlab}(n)$ continued

We need an upper bound on $\text{cyc}_2(g)$.

For $X = \{1, 2, 3, 4, 5\}$

g	$\text{cyc}_2(g)$	Some g -cycles on pairs
(12)	7	13, 23 14, 24 15, 25 34 35 45 12
(123)	4	—
(1234)	3	15, 25, 35, 45 12, 23, 34, 14 13, 24
(12)(34)	6	—
(12345)	2	—
(123)(45)	2	—

Exercise: Prove that the entries in the last column are correct.

Upper bound for $\text{Unlab}(n)$ continued

For $g \in C_2$, maximum of $\text{cyc}_2(g)$ is for a transposition, so

$$\begin{aligned}\text{cyc}_2(g) &\leq \text{cyc}_2((12)) = \binom{n}{2} - (\text{number of } g\text{-cycles of} \\ &\quad \text{length 2 in } X^{\{2\}}) \\ &= \binom{n}{2} - (n - 2).\end{aligned}$$

Upper bound for $\text{Unlab}(n)$ continued

For $g \in C_3$, maximum of $\text{cyc}_2(g)$ is for

$g = \text{product of } m/2 \text{ cycles of length 2, e.g.}$

$g_0 = (12)(34) \dots (m-1, m).$

$$\text{cyc}_2(g) \leq \binom{n}{2} - (\text{number of } g_0\text{-cycles of length 2 in } X^{\{2\}})$$

$$= \binom{n}{2} - \left((n-m) \cdot \frac{m}{2} + 2 \binom{m/2}{2} \right)$$

$$\leq \binom{n}{2} - \frac{nm}{4}.$$

Upper bound for $\text{Unlab}(n)$ continued

So

$$\begin{aligned}\text{Unlab}(n) &= \frac{1}{n!} \sum_{g \in S_n} 2^{\text{cyc}_2(g)} \\ &< \frac{1}{n!} \left(2^{n(n-1)/2} + |C_2|.2^{n(n-1)/2-(n-2)} \right. \\ &\quad \left. + |C_3|.2^{n(n-1)/2-nm/4} \right) \\ &< \frac{2^{n(n-1)/2}}{n!} \left(1 + \frac{n^m}{2^{n-2}} + \frac{n^n}{2^{nm/4}} \right).\end{aligned}$$

Upper bound for Unlab(n) continued

Combine upper and lower bounds.

$$\frac{2^{1+n(n-1)/2}}{n!} - \frac{\text{Asym}(n)}{n!} \leq \frac{2^{n(n-1)/2}}{n!} \left(1 + \frac{n^m}{2^{n-2}} + \frac{n^n}{2^{nm/4}}\right).$$

Hence

$$\frac{\text{Asym}(n)}{n!} \geq \frac{2^{n(n-1)/2}}{n!} \left(1 - \frac{n^m}{2^{n-2}} - \frac{n^n}{2^{nm/4}}\right).$$

Proportion of labelled graphs of order n that are asymmetric

$$\begin{aligned} &= \frac{\text{Asym}(n)}{2^{n(n-1)/2}} \\ &\geq 1 - \frac{n^m}{2^{n-2}} - \frac{n^n}{2^{nm/4}}. \end{aligned}$$

Upper bound for Unlab(n) continued

Careful choice of m : take $m = \lfloor 8 \log_2 n \rfloor$

Then

$$\begin{aligned} 2^{nm/4} &\geq 2^{2n \log_2 n} = n^{2n} \\ n^m &= (2^{\log_2 n})^m \geq 2^{8(\log_2 n)^2}. \end{aligned}$$

Hence Proportion of asymmetric graphs

$$\begin{aligned} &\geq 1 - \frac{1}{2^{n-2-8(\log_2 n)^2}} - \frac{1}{n^n} \\ &\longrightarrow 1 \text{ as } n \longrightarrow \infty. \end{aligned}$$

Exercises I

Exercise 1: For each pair of isomorphic graphs on $X = \{1, 2, 3\}$ write down an isomorphism. When is there more than one choice of an isomorphism?

Exercise 2: Let $X = \{1, 2, 3, 4\}$.

- a How many labelled graphs are there on X ?
- b Which labelled graphs on X are fixed by
 - (i) (12) , (ii) (123) , (iii) $(12)(34)$, (iv) (1234) ?
- c Use the Orbit Counting Lemma to find the number of unlabelled graphs of order 4.
- d Draw a representative of each isomorphism class of labelled graphs on X .
- e Show there are no asymmetric graphs on X .

Exercise 3: Let $X = \{1, 2, \dots, 6\}$ and $g = (12 \dots 6)$. Find how many labelled graphs on X are fixed by g and sketch them.

Exercises II

Exercise 4: Decide whether or not there is an asymmetric graph of order 5.

(Perhaps use the same process as for Exercise 2.)

Exercise 5: For $g \in \text{Sym}(X)$, $\text{cyc}_2(g)$ = number of g -cycles in $X^{\{2\}}$. Let $X = \{1, 2, 3, 4, 5\}$.

$\text{cyc}_2(g)$ depends on the “cycle type” of g (numbers of cycles of g of each length in X).

Find $\text{cyc}_2(g)$ for

$g \in \{(12), (123), (1234), (12)(34), (12345), (123)(45)\}$.

Exercise 6: Find a way of constructing an asymmetric graph of order n for any $n \geq 6$.

Pólya Counting I

Gordon Royle

Semester 1, 2004

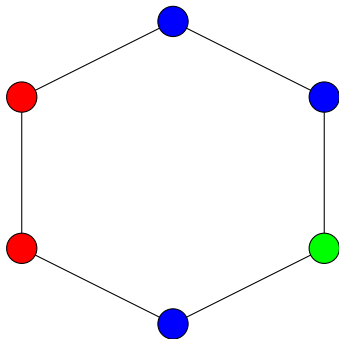
George Pólya (1887 – 1985)

George Polya discovered a powerful general method for enumerating the number of orbits of a group on particular configurations. This method became known as the Pólya Enumeration Theorem, or PET.



Necklaces

Consider a decorative ornament that consists of n coloured “beads” arranged on a circular loop of string.

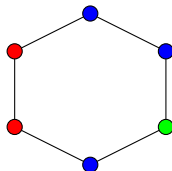
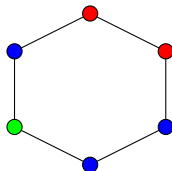
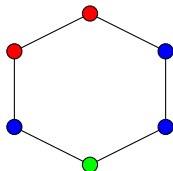


This can be represented simply as a word of length n over a suitable alphabet of colours: *bbgbr*

Rotation

Two words that differ purely by a (cyclic) rotation clearly represent the same ornament, and are called *equivalent*:

$$rbbgbr \equiv rrbgbg \equiv bbgbr r$$



Necklaces

An (n, k) -necklace is an equivalence class of words of length n over an alphabet of size k under rotation. The basic enumeration problem is then:

Necklace Enumeration

For a given n and k , how many (n, k) -necklaces are there?

Equivalently, we are asking how many orbits the cyclic group C_n has on the set of all words of length n over an alphabet of size k .

We will denote this value by $a(n, k)$.

$(6, 3)$ -necklaces

By Burnside's lemma, the number of orbits of C_6 on words of length 6 over an alphabet of size 3 is equal to the average number of words fixed by each element of C_6 .

Element g	$ \text{fix}(g) $
e	3^6
$(1, 2, 3, 4, 5, 6)$	3
$(1, 3, 5)(2, 4, 6)$	3^2
$(1, 4)(2, 5)(3, 6)$	3^3
$(1, 5, 3)(2, 6, 4)$	3^2
$(1, 6, 5, 4, 3, 2)$	3

$$a(6, 3) = \frac{1}{6} \sum_{g \in C_6} |\text{fix}(g)| = 130.$$

$(6, k)$ -necklaces

If we allow k colours, then the computation is the same except that the number of configurations fixed by each element now depends on k .

Element g	$ \text{fix}(g) $
e	k^6
$(1, 2, 3, 4, 5, 6)$	k
$(1, 3, 5)(2, 4, 6)$	k^2
$(1, 4)(2, 5)(3, 6)$	k^3
$(1, 5, 3)(2, 6, 4)$	k^2
$(1, 6, 5, 4, 3, 2)$	k

$$a(6, k) = \frac{1}{6} \sum_{g \in C_6} |\text{fix}(g)| = (2k + 2k^2 + k^3 + k^6)/6;$$

(n, k) -necklaces

The number of words fixed by an element g of C_n is completely determined by the number of cycles in the cycle decomposition of g — in fact, if g has c cycles, then it fixes k^c words.

Now, if $g = (1, 2, \dots, n)$ then the elements of C_n are the n permutations

$$g, g^2, \dots, g^n = e.$$

The order of the element g^i is

$$n / \gcd(n, i)$$

and hence it has $\gcd(n, i)$ cycles in its cycle decomposition.

(n, k) -necklaces

Therefore the number of (n, k) -necklaces is given by

$$a(n, k) = \frac{1}{n} \sum_{i=1}^n k^{\gcd(n, i)}.$$

If p is a *prime number* then this can be substantially simplified, because $\gcd(p, i) = 1$ for all $i < p$, and so we get

$$a(p, k) = \frac{1}{p}((p-1)k + k^p).$$

Euler's ϕ Function

For any positive integer x , let $\phi(x)$ denote the number of integers $1 \leq i \leq x$ such that $\gcd(x, i) = 1$.

This function is sometimes called *Euler's ϕ function* or *Euler's totient function* and its first few values are given below:

x	$\phi(x)$	x	$\phi(x)$
1	1	2	1
3	2	4	2
5	4	6	2
7	6	8	4
9	6	10	4
11	10	12	4

General Result

The following theorem explains the significance of Euler's function for necklaces:

Theorem

For any divisor d of n , there are $\phi(d)$ elements of order d in C_n .

Corollary

The number of (n, k) -necklaces is given by

$$a(n, k) = \frac{1}{n} \sum_{d|n} \phi(d) k^{n/d}.$$

Proof of Theorem

For each possible “greatest common divisor” value $g|n$, how many numbers i are there such that

$$\gcd(n, i) = g?$$

For this to occur, we must have

$$n = n_1 g \quad i = i_1 g$$

where $\gcd(n_1, i_1) = 1$.

Clearly this number is just $\phi(n_1) = \phi(n/g)$, and putting $d = n/g$ we obtain the result.

In GAP

Using GAP's built-in functions, this can be written in a very slick fashion:

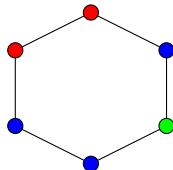
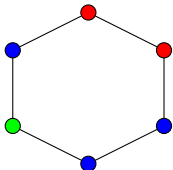
```
neckLaces := function(n,k)
  return Sum(DivisorsInt(n),d->Phi(d)*k^(n/d))/n;
end;
```

Here `DivisorsInt` returns the list of divisors of a number, and `Phi` is Euler's ϕ function. This use of `Sum` with two arguments applies the function given as the second argument to every element of the list in the first argument and sums the resulting values.

Bracelets

Some of these ornaments can be freely turned over (for example, if the beads are just spherical), but sometimes they cannot, and so whether we consider configurations that are mirror-images to be equivalent or not depends on the application.

An (n, k) -*bracelet* is an equivalence class of words of length n under rotation *and* reflection.



Counting Bracelets

In order to determine $b(n, k)$ – the number of bracelets of length n over an alphabet of size k , we need to find the number of orbits of the *dihedral group* D_{2n} on k -ary n -tuples.

Exercise

Determine $b(n, k)$.

Hint: Experiment first with GAP and small dihedral groups. The final expression will differ according to whether n is even or odd, so examine carefully the differences.

Representatives

A necklace was defined to be an equivalence class of words under rotation. For example, if $n = 3$ and the alphabet is $\{0, 1, 2\}$ then the following set is an example of a necklace:

$$\{010012, 100120, 001201, 012010, 120100, 201001\}.$$

Any one of these words suffices to determine the necklace, and so we represent a necklace by using the *lexicographically least* word that it contains. Thus the necklace

$$\{010012, 100120, \textcolor{red}{001201}, 012010, 120100, 201001\}$$

is represented by the word

$$001201.$$

Generation

We could generate all necklaces by generating all the k^n words using the odometer principle and then discarding all the ones that are *not* the lexicographically least in their class.

This is not an efficient way to generate necklaces because it generates k^n words for approximately k^n/n necklaces, thus doing about n times too much work.

An interesting algorithm to generate necklaces was found by Frederickson, Kessler and Maiorana and is therefore known as the *FKM algorithm*.

FKM Algorithm

To generate all (n, k) -necklaces over the alphabet $\{0, 1, \dots, k-1\}$, consider the following rule to generate a list of words (which will include both necklaces and some non-necklaces) in increasing lexicographic order from the first word $0^n = 000\dots 0$ to the last word $(k-1)^n$.

For any word $\alpha = a_1 a_2 \dots a_n$ other than $(k-1)^n$, the successor of α is obtained as follows:

- ▶ Let i be the largest value such that $a_i < (k-1)$,
- ▶ Let $\beta = a_1 a_2 \dots a_{i-1} (a_i + 1)$,
- ▶ Then $\text{succ}(\alpha)$ is the first n characters of $\beta\beta\beta\dots$; this word is a necklace if and only if i is a divisor of n .

Example

Suppose we are generating $(6, 3)$ -necklaces; then the FKM algorithm starts as follows:

0	0	0	0	0	0	
0	0	0	0	0	1	
0	0	0	0	0	2	
0	0	0	0	1	0	← reject
0	0	0	0	1	1	
0	0	0	0	1	2	
0	0	0	0	2	0	← reject
0	0	0	0	2	1	
0	0	0	0	2	2	
0	0	0	1	0	0	← reject

Example (cont.)

At some later stage of the algorithm, it continues

0	1	2	2	2	2	
0	2	0	2	0	2	
0	2	0	2	1	0	← reject
0	2	0	2	1	1	
0	2	0	2	1	2	
0	2	0	2	2	0	← reject
0	2	0	2	2	1	
0	2	0	2	2	2	
0	2	1	0	2	1	

Pre-necklaces

The set of words produced by the FKM algorithm is actually the collection of *pre-necklaces* — that is, words that can occur at the beginning of a k -ary necklace of some possibly larger length.

Proving this, and the fact that the necklaces occur precisely when i is a divisor of n is not extremely difficult, but does require some careful analysis of the structure of necklaces.

Binary Necklaces

Binary necklaces (i.e those with $k = 2$) can be produced by the FKM algorithm:

0 0 0 0 0 0 0	0 0 0 1 1 0 1	
0 0 0 0 0 0 1	0 0 0 1 1 1 1	0 0 1 1 1 1 1
0 0 0 0 0 1 1	0 0 1 0 0 1 1	0 1 0 1 0 1 1
0 0 0 0 1 0 1	0 0 1 0 1 0 1	0 1 0 1 1 1 1
0 0 0 0 1 1 1	0 0 1 0 1 1 1	0 1 1 0 1 1 1
0 0 0 1 0 0 1	0 0 1 1 0 1 1	0 1 1 1 1 1 1
0 0 0 1 0 1 1	0 0 1 1 1 0 1	1 1 1 1 1 1 1

Unsolved Problem

Is there a list containing representatives of all of the binary n -bit necklaces (for odd n) such that successive elements differ in only one place? (In other words, a Gray code for binary necklaces).

Cycle Index

Given a permutation g of degree n , let $c_i(g)$ be the number of cycles of length i in its cycle decomposition.

Then the *cycle index* of a permutation group is a polynomial that summarizes the information about the cycle types of all the elements of the group.

$$Z_G(X_1, X_2, \dots, X_n) = \frac{1}{|G|} \sum_{g \in G} X_1^{c_1(g)} X_2^{c_2(g)} \dots X_n^{c_n(g)}$$

Examples

The cycle index of the group C_6 is given by

$$Z_{C_6}(X_1, X_2, \dots, X_6) = \frac{1}{6}(X_1^6 + X_2^3 + 2X_3^2 + 2X_6).$$

Notice that the number of $(6, k)$ -necklaces is given by

$$a(6, k) = Z_{C_6}(k, k, k, k, k, k)$$

Pólya's Enumeration Theorem

Now we state a simple version of Pólya's Enumeration Theorem.

Pólya's Enumeration Theorem (PET)

Let A and B be two finite sets, and suppose that group G acts on A . Then the number of orbits of G on the set B^A of functions

$$f : A \rightarrow B$$

is given by

$$Z_G(|B|, |B|, \dots, |B|).$$

Necklaces

PET applies directly to necklaces, because if we take

- ▶ $A = \{1, 2, \dots, n\}$,
- ▶ $B = \{0, 1, \dots, k-1\}$, and
- ▶ $G = C_n$.

then a function from $A \rightarrow B$ corresponds to a word of length n over the alphabet $\{0, 1, \dots, k-1\}$, and the orbits of these words under C_n are precisely the necklaces.

So, we get

$$a(n, k) = Z_{C_n}(k, k, \dots, k)$$

as we have (almost) already seen.

Proof of PET

The proof of PET follows directly from Burnside's lemma.

A function $f : A \rightarrow B$ is fixed by a permutation $g \in G$ if and only if f is constant on each of the cycles of g . Therefore if g has $c(g)$ cycles altogether, then there are

$$|B|^{c(g)}$$

functions fixed by g .

Now g makes a contribution to Z_G of

$$X_1^{c_1(g)} X_2^{c_2(g)} \dots X_n^{c_n(g)}$$

and if we substitute $X_i = |B|$ then we get

$$|B|^{c_1(g)+c_2(g)+\dots+c_n(g)} = |B|^{c(g)}.$$

Partitions and Permutations

Gordon Royle

Semester 1, 2004

Partitions

The word *partition* is shared by (at least) two different concepts, although both refer to the process of dividing an object into smaller sub-objects.

- ▶ Integer Partitions

A partition of an integer n is a way to write it as a sum of smaller integers, such as

5, $4+1$, $3+2$, $3+1+1$, $2+2+1$, $2+1+1+1$, $1+1+1+1+1$.

- ▶ Set Partitions

A partition of a *set* is a way to divide it into a number of subsets, such as

$\{1, 2, 3\}$, $\{1, 2\}\{3\}$, $\{1, 3\}\{2\}$, $\{1\}\{2, 3\}$, $\{1\}\{2\}\{3\}$

Lexicographic order

We will represent a partition of an integer n by a sequence $a_1 a_2 \dots$, where $a_1 \geq a_2 \geq \dots > 0$. Thus the partitions of 7 would be represented as follows.

1111111	211111	2211
2221	3111	3211
322	331	4111
421	43	511
52	61	7

In this table the partitions are given in *lexicographic order*.

Reverse Lexicographic Order

The simplest algorithm to generate partitions actually generates them in *reverse lexicographic order*, starting with the partition n and ending with

- Find the largest index i such that $a_i \neq 1$; suppose that $a_i = a + 1$ so that

$$\alpha = \beta(a+1)11\dots 1.$$

- Replace the suffix $(a+1)11\dots 1$ by $aa\dots ar$ where $r < a$, thus obtaining

$$\text{succ}(\alpha) = \beta aa\dots ar.$$

Example 1

What is the successor of $\alpha = 22211$?

- ▶ The largest i such that $a_i \neq 1$ is $i = 3$

a_1	a_2	a_3	a_4	a_5
2	2	2	1	1

- ▶ Replace the suffix 211 with 1111

a_1	a_2	a_3	a_4	a_5	a_6
2	2	2	1	1	
2	2	1	1	1	1

Therefore we get

$$\text{succ}(22211) = 221111.$$

Example 2

What is the successor of $\alpha = 3311$?

- ▶ The largest i such that $a_i \neq 1$ is $i = 2$

a_1	a_2	a_3	a_4
3	3	1	1

- ▶ Replace the suffix 311 with as many 2s as possible, and a remainder if necessary.

a_1	a_2	a_3	a_4
3	3	1	1
3	2	2	1

Therefore we get

$$\text{succ}(3311) = 3221.$$

Fixed number of parts

Suppose we are interested in generating the number of partitions of n into exactly k parts, for example if $n = 11$ and $k = 4$ we get

3332	4322	4331	4421
5222	5321	5411	6221
6311	7211	8111	

Successors

The easiest algorithm for generating partitions of fixed size k starts with the partition

$$(n - k + 1)1111$$

and then computes the successor of $\alpha = a_1 a_2 \dots a_k$ as follows:

- ▶ Let i be the smallest index such that $a_i < a_1 - 1$.
- ▶ Assign $a_i + 1$ to each of a_2, a_3, \dots, a_i and then set a_1 as needed to maintain a partition of n .

The algorithm terminates if there are no values i such that $a_i < a_1 - 1$; in this case each part of the partition is $\lfloor \frac{n}{k} \rfloor$ or $\lceil \frac{n}{k} \rceil$.

Example

Suppose that $n = 15$ and $k = 5$ and we want the successor of $\alpha = 66111$.

- ▶ The smallest index i such that $a_i < 5$ is $i = 3$

a_1	a_2	a_3	a_4	a_5
6	6	1	1	1

- ▶ Set a_2 and a_3 to the value $a_3 + 1$ which is 2

a_1	a_2	a_3	a_4	a_5
*	2	2	1	1

- ▶ Set a_1 to the required value to maintain a partition of $n = 15$

a_1	a_2	a_3	a_4	a_5
9	2	2	1	1

Colex ordering

This ordering of partitions with a fixed number of parts is not *reverse* lexicographic, but rather *colexicographic*.

Lexicographic	Reverse lex	Colexicographic
3322	7111	7111
3331	6211	6211
4222	5311	5311
4321	5221	4411
4411	4411	5221
5221	4321	4321
5311	4222	3331
6211	3331	4222
7111	3322	3322

Conjugate permutations

Suppose that f and g are two permutations in the symmetric group $\text{Sym}(n)$. Then they are said to be *conjugate* if

$$f = h^{-1}gh$$

for some $h \in \text{Sym}(n)$.

Example

The permutations $f = (1, 2, 3)(4, 5)$ and $g = (1, 3, 4)(2, 5)$ are conjugate because

$$(1, 2, 3)(4, 5) = (2, 3, 4) (1, 3, 4)(2, 5) (2, 4, 3)$$

and therefore we may take $h = (2, 4, 3)$ in the above definition.

Conjugacy is an equivalence relation

- ▶ Every permutation is conjugate to itself

$$f = e^{-1} f e$$

- ▶ If f is conjugate to g , then g is conjugate to h

$$f = h^{-1} g h \implies g = h f h^{-1}$$

- ▶ If a is conjugate to b and b conjugate to c , then a is conjugate to c

$$a = h^{-1} b h \text{ and } b = g^{-1} c g \implies a = h^{-1} g^{-1} c g h = (gh)^{-1} c (gh).$$

Conjugacy Classes

This means that the permutations fall into *disjoint* classes called *conjugacy classes* such that two permutations are conjugate if and only if they lie in the same class.

e	$(3, 4)$	$(1, 2)(3, 4)$	$(2, 3, 4)$	$(1, 2, 3, 4)$
	$(2, 3)$	$(1, 3)(2, 4)$	$(2, 4, 3)$	$(1, 2, 4, 3)$
	$(2, 4)$	$(1, 4)(2, 3)$	$(1, 2, 3)$	$(1, 3, 4, 2)$
	$(1, 2)$		$(1, 2, 4)$	$(1, 3, 2, 4)$
	$(1, 3)$		$(1, 3, 2)$	$(1, 4, 3, 2)$
	$(1, 4)$		$(1, 3, 4)$	$(1, 4, 2, 3)$
			$(1, 4, 2)$	
			$(1, 4, 3)$	

Cycle Structure

The *cycle structure* of a permutation is the number of cycles of each length in its cycle decomposition.

Theorem

Two permutations are conjugate in $\text{Sym}(n)$ if and only if they have the same cycle structure.

We need to prove two things

- ▶ If two permutations are conjugate, then they have the same cycle structure, and
- ▶ If two permutations have the same cycle structure, then they are conjugate.

Conjugate permutations have the same cycle structure

If the permutation g maps

$$i \rightarrow ig$$

then $h^{-1}gh$ maps

$$ih \rightarrow igh.$$

Therefore for every cycle

$$(a, b, \dots, c)$$

in the cycle decomposition of g , there is a corresponding cycle

$$(ah, bh, \dots, ch)$$

in the cycle decomposition of $f = h^{-1}gh$.

Permutations with the same cycle structure are conjugate

If two permutations f and g have the same cycle structure, then we can find a conjugating permutation h such that $f = h^{-1}gh$.

For each cycle

$$(f_1, f_2, \dots, f_k)$$

of f there is a corresponding cycle

$$(g_1, g_2, \dots, g_k)$$

of g .

Then define h by the rule

$$h : g_i \rightarrow f_i.$$

Example

Let

$$f = (1, 4, 5)(2, 7)(3, 6) \quad g = (2, 4, 6)(1, 5)(3, 7)$$

Then define h (in image notation) as follows:

$$h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 4 & 7 & 5 & 6 \end{pmatrix}$$

Then $h = (1, 2)(5, 7, 6)$ and it is easy to check that

$$f = h^{-1}gh$$

and so h is a conjugating permutation.

In GAP

```
gap> f := (1,4,5)(2,7)(3,6);  
(1,4,5)(2,7)(3,6)  
gap> g := (2,4,6)(1,5)(3,7);  
(1,5)(2,4,6)(3,7)  
gap> h := PermList([2,1,3,4,7,5,6]);  
(1,2)(5,7,6)  
gap> h^-1*g*h;  
(1,4,5)(2,7)(3,6)  
gap> f = last;  
true  
gap>
```

Cycle structure

The cycle structure of a permutation can be represented in a number of different ways. One way would be to simply list the lengths of the cycles. For example, if $f \in \text{Sym}(10)$ has cycle decomposition

$$f = (1, 2, 4)(5, 6)(8, 9, 10)$$

then its cycle structure could be written as

$$33211$$

In this representation, the cycle structure of a permutation is simply a partition of n , the degree of the permutation!

Partitions and Conjugacy Classes

We have therefore essentially proved the following:

Theorem

The number of conjugacy classes of $\text{Sym}(n)$ is equal to the number of partitions of n .

For $\text{Sym}(4)$ the correspondence is

Partition	Representative
1111	e
211	$(1, 2)$
22	$(1, 2)(3, 4)$
31	$(1, 2, 3)$
4	$(1, 2, 3, 4)$

Counting partitions

Let $p(n)$ be the number of partitions of n , and let $p_k(n)$ be the number of partitions of n that have k parts.

Then

$$p(n) = \sum_{k=1}^n p_k(n).$$

We can write these numbers out in a triangle reminiscent of Pascal's triangle:

$$\begin{array}{ccccccc} & & & & p_1(1) & & \\ & & & & & & \\ & & & p_1(2) & p_2(2) & & \\ & & p_1(3) & p_2(3) & p_3(3) & & \\ p_1(4) & p_2(4) & p_3(4) & p_4(4) & & & \\ \dots & \dots & \dots & & & & \end{array}$$

Top of the triangle

By direct calculation we see that the triangle starts

$$\begin{array}{ccccccc} & & & & 1 & & \\ & & & & & & \\ & & & 1 & & 1 & \\ & & & & & & \\ & & 1 & & 1 & & 1 \\ & & & & & & \\ & 1 & & 2 & & 1 & & 1 \\ & & & & & & \\ & 1 & 2 & & 2 & & 1 & & 1 \\ & & & & & & \\ 1 & & 3 & & 3 & & 2 & & 1 & & 1 \\ & & & & & & \\ \dots & & & & \dots & & \dots \end{array}$$

The total number of partitions $p(n)$ of each number n is obtained by summing the entries in each row of this triangle.

A recurrence

We can express the values of $p_k(n)$ in terms of smaller such numbers by splitting up the partitions of n according to the number of parts that are equal to 1. So if P is the set of all partitions of n with k parts, then define P_0, P_1, \dots, P_k by

$$P_i = \{\pi \in P \mid \pi \text{ has exactly } i \text{ 1s}\}$$

Then clearly

$$|P| = \sum_{i=0}^k |P_i|.$$

Therefore we need to count the number of partitions in each set P_i .

Partitions with i 1s

Given a partition $\pi \in P_i$, consider the partition obtained by subtracting one from each part of π . This is a partition of $n - k$ with $k - i$ parts, and conversely any partition of $n - k$ with $k - i$ parts yields a partition in P_i if we add 1 to each part, and adjoin i parts equal to 1.

Therefore

$$|P_i| = p_{k-i}(n - k).$$

Example

The partitions of 10 into 4 parts with two 1s are

$$4411 \quad 5311 \quad 6211$$

and the partitions of 6 into 2 parts are

$$33 \quad 42 \quad 51.$$

Putting it all together

Therefore

$$p_k(n) = \sum_{i=0}^k p_{k-i}(n-k)$$

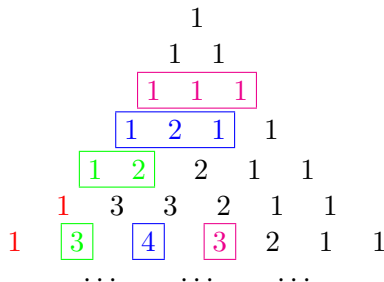
and replacing i by $k-i$ we get

$$p_k(n) = \sum_{i=0}^k p_i(n-k).$$

This sum involves terms of the form $p_0(x)$; this value must be taken to be 0 unless $x = 0$ in which case $p_0(0)$ is defined to be 1.

Extending the triangle

We will use this to extend the triangle to $n = 7$



The blue value $p_3(7)$ is obtained by adding the first 3 values on the line for $n = 7 - 3 = 4$, thus

$$4 = 1 + 2 + 1.$$

Size of conjugacy classes

Given a partition of n , how many permutations have that cycle structure?

For example, how big is the conjugacy class of $\text{Sym}(7)$ with cycle structure 322? A permutation with this cycle structure has the form

$$(a, b, c)(d, e)(f, g).$$

There are $7!$ ways of assigning the numbers $1, 2, \dots, 7$ to the 7 positions, but many of them yield the same permutation.

For example

$$(1, 2, 3)(4, 5)(6, 7) \text{ and } (2, 3, 1)(6, 7)(4, 5)$$

are the same.

Overcounting

For the conjugacy class of $\text{Sym}(7)$ with cycle structure 322, there are

- ▶ 3 ways to write the cycle (a, b, c)
- ▶ 2 ways to write the cycle (d, e)
- ▶ 2 ways to write the cycle (f, g)
- ▶ 2 ways to order the two 2-cycles

Therefore every permutation arises in

$$3 \times 2 \times 2 \times 2 = 24$$

ways, and so the total number of distinct permutations in this conjugacy class is

$$7!/24 = 210.$$

In general

In general, suppose that a partition has c_i parts equal to i , so that

$$c_1 + 2c_2 + 3c_3 + \cdots + nc_n = n.$$

Then the number of permutations in the conjugacy class with this cycle structure is

$$\frac{n!}{(\prod_i c_i! i^{c_i})}.$$

Proof.

Each cycle of length i can be written in i different ways, and the c_i cycles of length i can be written in $c_i!$ different orders. Hence the denominator of this expression counts the number of different ways of writing the permutation.

Example

Check that this all works for $n = 5$ where there are 7 partitions:

Partition	c_1	c_2	c_3	c_4	c_5	Overcount	Number
11111	5	0	0	0	0	120	1
2111	3	1	0	0	0	12	10
221	1	2	0	0	0	8	15
311	2	0	1	0	0	6	20
32	0	1	1	0	0	6	20
41	1	0	0	1	0	4	30
5	0	0	0	0	1	5	24
							120

Stirling Numbers

The *Stirling numbers* are the two series of numbers $s(n, k)$ and $S(n, k)$ defined as follows:

- ▶ Stirling numbers of the 1st kind:
 $(-1)^{n-k}s(n, k)$ is the number of permutations of degree n with k cycles.
- ▶ Stirling numbers of the 2nd kind:
 $S(n, k)$ is the number of partitions of an n -set into k non-empty parts.

First, the second kind

It is easy to list all the set partitions for small n and k :

- ▶ $n = 1$
 - ▶ $k = 1$: 1
- ▶ $n = 2$
 - ▶ $k = 1$: 12
 - ▶ $k = 2$: 1|2
- ▶ $n = 3$
 - ▶ $k = 1$: 123
 - ▶ $k = 2$: 12|3, 13|2, 1|23
 - ▶ $k = 3$: 1|2|3
- ▶ $n = 4$
 - ▶ $k = 1$: 1234
 - ▶ $k = 2$: 1|234, 134|2, 124|3, 123|4, 12|34, 13|24, 14|23
 - ▶ $k = 3$: 12|3|4, 13|2|4, 14|2|3, 1|23|4, 1|24|3, 1|2|34
 - ▶ $k = 4$: 1|2|3|4

The triangle

We can write the numbers out in a triangle (similar to Pascal's triangle) as follows:

$$\begin{array}{ccccccc} & & & S(1,1) & & & \\ & & S(2,1) & & S(2,2) & & \\ & S(3,1) & & S(3,2) & & S(3,3) & \\ S(4,1) & & S(4,2) & & S(4,3) & & S(4,4) \\ \dots & & \dots & & \dots & & \end{array}$$

From the previous slide we get

$$\begin{array}{ccccccc} & & & 1 & & & \\ & & 1 & & 1 & & \\ & 1 & & 3 & & 1 & \\ 1 & & 7 & & 6 & & 1 \\ \dots & & \dots & & \dots & & \end{array}$$

A recurrence

We can express the Stirling number $S(n, k)$ in terms of smaller Stirling numbers by noting that a set partition of $\{1, \dots, n\}$ with k parts is obtained either by

- ▶ Adding n as a singleton to a partition of $\{1, \dots, n-1\}$ with $k-1$ parts, or
- ▶ Putting n into one of the cells of a partition of $\{1, \dots, n-1\}$ with k parts

Counting the number of set partitions of each type yields

$$S(n, k) = S(n-1, k-1) + kS(n-1, k).$$

Illustration

For $(n, k) = (4, 3)$, this formula is

$$S(4, 3) = S(3, 2) + 3 \times S(3, 3)$$

$$\begin{array}{ccccccc} & & & & 1 & & \\ & & & & 1 & & 1 \\ & & & 1 & 3 & 3 \times 1 & \\ & 1 & 7 & 6 & 1 & & \\ \dots & & \dots & & \dots & & \end{array}$$

and the corresponding set partitions in the two groups are

- ▶ $12|3|4, 13|2|4, 1|23|4$
- ▶ $14|2|3, 1|24|3, 1|2|34$

An explicit formula

We can find an explicit formula for $S(n, k)$ by using the principle of inclusion and exclusion:

Let A denote the set of all functions

$$f : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, k\}$$

Now, let A_i be the set

$$A_i = \{f \in A \mid f^{-1}(i) = \emptyset\}.$$

In other words, A_i is the set of functions whose *range* does not include i .

Principle of Inclusion/Exclusion

If A_1, A_2, \dots, A_k are all subsets of a set A then for any index set $\mathcal{I} \subseteq \{1, 2, \dots, k\}$, define

$$A_{\mathcal{I}} = \bigcap_{i \in \mathcal{I}} A_i$$

(where we take $A_{\emptyset} = X$).

Principle of Inclusion/Exclusion

The number of elements of X that do not belong to any of the sets A_1, A_2, \dots, A_k is given by

$$\sum_{\mathcal{I} \subseteq \{1, 2, \dots, k\}} (-1)^{|\mathcal{I}|} |A_{\mathcal{I}}|.$$

Set partitions with k parts

By PIE, the number of functions that map $\{1, 2, \dots, n\}$ *onto* $\{1, 2, \dots, k\}$ is given by:

$$\sum_{\mathcal{I} \subseteq \{1, 2, \dots, k\}} (-1)^{|\mathcal{I}|} |A_{\mathcal{I}}|.$$

For each possible size $0 \leq j \leq k$ there are $\binom{k}{j}$ possible subsets \mathcal{I} of size j , and each of them makes the same contribution to this sum. More precisely, if $|\mathcal{I}| = j$ then

$$|A_{\mathcal{I}}| = (k - j)^n$$

because this just counts the number of functions that avoid a particular set of j elements.

The formula

Putting this together, we see that the number of functions from $\{1, \dots, n\}$ onto $\{1, \dots, k\}$ is given by

$$\sum_{j=0}^{j=k} (-1)^j \binom{k}{j} (k-j)^n$$

which (on replacing j by $k-j$) is equal to

$$\sum_{j=1}^{j=k} (-1)^{k-j} \binom{k}{j} j^n.$$

Now each such function determines a partition of $\{1, 2, \dots, n\}$ into k parts, but we have counted each partition $k!$ times and so

$$S(n, k) = \frac{1}{k!} \sum_{j=1}^{j=k} (-1)^{k-j} \binom{k}{j} j^n.$$

Bell numbers

The *total number* of partitions of a set of size n into any number of non-empty parts is called the Bell number $B(n)$.

Thus

$$B(n) = \sum_{k=1}^{k=n} S(n, k).$$

The first few Bell numbers are

1, 2, 5, 15, 52, 203, 877, 4140, 21147, 115975

GAP has built-in functions `Stirling1(n,k)`, `Stirling2(n,k)` and `Bell(n)` giving these numbers.

Now, the first kind

The triangle of Stirling numbers of the first kind

$$\begin{array}{ccccccc} & & & & s(1,1) & & \\ & & & & & & \\ & & & s(2,1) & & s(2,2) & \\ & & s(3,1) & & s(3,2) & & s(3,3) \\ s(4,1) & & s(4,2) & & s(4,3) & & s(4,4) \\ \dots & & \dots & & \dots & & \end{array}$$

starts as follows:

$$\begin{array}{ccccccc} & & & & 1 & & \\ & & & & & & \\ & & & -1 & & 1 & \\ & & 2 & & -3 & & 1 \\ -6 & & 11 & & -6 & & 1 \\ \dots & & \dots & & \dots & & \end{array}$$

A recurrence

We can find a recurrence expressing $s(n, k)$ in terms of smaller Stirling numbers, by noting that a permutation of degree n with k cycles can be obtained either by

- ▶ Adjoining element n as a fixed point to a permutation of degree $n - 1$ with $k - 1$ cycles, or
- ▶ Inserting n into one of the cycles of a permutation of degree $n - 1$ with k cycles.

and then counting the number of permutations in each category.

Finding $s(4, 2)$

The permutations of degree 4 with 2 cycles consist of

- ▶ The permutations of degree 3 with 1 cycle, with 4 adjoined as a fixed point

$$(1, 2, 3)(4) \quad (1, 3, 2)(4)$$

- ▶ The permutations of degree 3 with 2 cycles, with 4 inserted into one of the cycles

$(1, 2)(3)$	$(1, 3)(2)$	$(1)(2, 3)$
<hr/>		
$(1, 4, 2)(3)$	$(1, 4, 3)(2)$	$(1, 4)(2, 3)$
$(1, 2, 4)(3)$	$(1, 3, 4)(2)$	$(1)(2, 4, 3)$
$(1, 2)(3, 4)$	$(1, 3)(2, 4)$	$(1)(2, 3, 4)$

There are 2 in the first group and $9 = 3 \times 3$ in the second group, thus giving us 11 altogether.

The formula

This arguments shows us that

$$|s(n, k)| = |s(n-1, k-1)| + (n-1)|s(n-1, k)|$$

but it does not take into account the sign of $s(n, k)$ (that is, whether it is positive or negative).

Now $(-1)^{n-k}$ is equal to $(-1)^{(n-1)-(k-1)}$ and so taking the signs into consideration we get

$$s(n, k) = s(n-1, k-1) - (n-1)s(n-1, k).$$

An astonishing connection

The reason for associating signs with the Stirling numbers is related to the following astonishing connection between these two sets of numbers, illustrated here for $n = 4$.

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 3 & 1 & 0 \\ 1 & 7 & 6 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 2 & -3 & 1 & 0 \\ -6 & 11 & -6 & 1 \end{pmatrix} = I_4$$

Pólya Counting II

Gordon Royle

Semester 1, 2004

Group Action on B^A

Suppose that G is a permutation group acting on a set A , and consider the set B^A of all functions

$$f : A \rightarrow B.$$

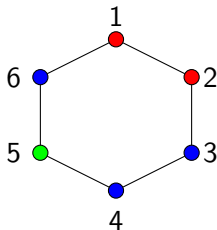
Then G acts naturally on B^A as follows: if $g \in G$ and $f \in B^A$ then define the function fg by

$$fg(a) = f(ag^{-1}).$$

This is simply formalizing our previous usage.

Example

Let A be the set $\{1, 2, \dots, 6\}$, and $B = \{\text{red}, \text{green}, \text{blue}\}$. Then a function $f \in B^A$ is just a 6-tuple of colours, which can be viewed as a necklace representative.



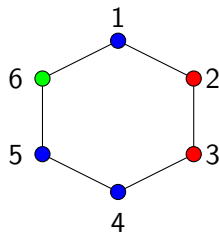
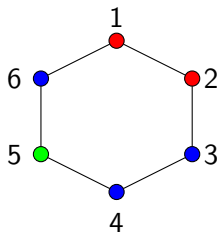
If G is the cyclic group C_6 generated by $g = (1, 2, 3, 4, 5, 6)$ then what is the result of applying g to this function?

Example cont.

According to the definition the function fg maps an element $a \in A$ to $f(ag^{-1})$. So if f is the function on the previous slide, then

$$fg(1) = f(1g^{-1}) = f(6) = \text{blue.}$$

Continuing in this fashion we see that fg is exactly the function that we “intuitively” expect.



Weighted configurations

We will now extend PET to count *weighted configurations*.

Suppose that each element of B has a different *weight* given by a weight function

$$w : B \rightarrow R$$

where R is unspecified at the moment.

Then we define the weight of a function $f \in B^A$ by

$$w(f) = \prod_{a \in A} w(f(a)),$$

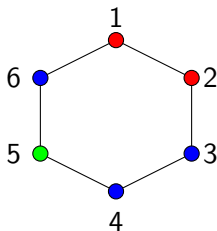
and extend this by defining the weight of a G -orbit of functions to be the weight of any function in that orbit. (This is well-defined because every function in a G -orbit has the same weight.)

Example

Returning to our necklace example, suppose that we assign different weights to the beads. For example, we might have

$$w(\text{red}) = 1 \quad w(\text{blue}) = 10 \quad w(\text{green}) = 100$$

Then the weight of our favourite necklace is:



$$w(f) = 1 \times 1 \times 10 \times 10 \times 10 \times 100 = 10^5.$$

The new question

In this context, we now have a “weighted” version of our original question about the number of orbits of G on B^A :

Question

What is the sum of the weights of the orbits of G on B^A ?

If the weights are all equal to 1, then each orbit has weight 1 and hence this just counts the number of orbits, and therefore this is a direct generalization of the situation where the simple version of PET applies.

As PET was proved directly from Burnside's orbit-counting lemma, we need to start by considering a weighted version of this lemma.

Weighted Burnside

Let G be a weight-preserving permutation group acting on a weighted set X with weight function w , and define the weight of a G -orbit to be the weight of any of its points.

For $g \in G$, let $\text{wfix}(g)$ denote the sum of the weights of the fixed points of g in X , that is

$$\text{wfix}(g) = \sum_{\{i \in X \mid ig=i\}} w(i).$$

Then the sum of the weights of the G -orbits in X is equal to

$$\frac{1}{|G|} \sum_{g \in G} \text{wfix}(g).$$

Proof

We will calculate in two ways the value of the sum

$$\sum_{\{(i,g) \in X \times G \mid ig=i\}} w(i).$$

On one hand, for each $i \in X$ we see that there are G_i group elements $g \in G$ that fix i , and hence the sum is equal to

$$\sum_{i \in X} |G_i| w(i).$$

On the other hand, for each element $g \in G$ we get a contribution of $w(i)$ for each fixed point i , and so the sum is equal to

$$\sum_{g \in G} \sum_{\{i \in X \mid ig=i\}} w(i) = \sum_{g \in G} \text{wfix}(g).$$

Proof cont.

Therefore

$$\sum_{i \in X} |G_i| w(i) = \sum_{g \in G} \text{wfix}(g).$$

Now any G -orbit, say j^G , contributes $|j^G|$ terms to the left-hand side, each of them of value $|G_j| w(j)$, and so in total it contributes

$$|j^G| \cdot |G_j| \cdot w(j) = |G| w(j).$$

Therefore the left-hand side is equal to $|G|$ times the sum of the weights of the orbits, and the result follows.

Recall $(6, 3)$ -necklaces

When we counted the *unweighted* $(6, 3)$ -necklaces, we had to calculate just the *number* of fixed points for each element of C_6 .

Element g	$ \text{fix}(g) $
e	3^6
$(1, 2, 3, 4, 5, 6)$	3
$(1, 3, 5)(2, 4, 6)$	3^2
$(1, 4)(2, 5)(3, 6)$	3^3
$(1, 5, 3)(2, 6, 4)$	3^2
$(1, 6, 5, 4, 3, 2)$	3

Now we have to consider counting the *sum of the weights* of the fixed points of each element of C_6 .

Weighted $(6, 3)$ -necklaces

Consider calculating $w_{\text{fix}}(g)$ for the element $g = (1, 3, 5)(2, 4, 6)$.
In order for a function f to be fixed by g we must have

$$f(1) = f(3) = f(5) \quad f(2) = f(4) = f(6)$$

and hence

$$w(f) = w(f(1))^3 w(f(2))^3.$$

Now $f(1)$ and $f(2)$ can be any of **red**, **green**, **blue** and so $w_{\text{fix}}(g)$ is equal to

$$(w(\text{red})^3 + w(\text{blue})^3 + w(\text{green})^3)^2.$$

Counting the others

If we repeat this process for the other elements of C_6 then we get

Element g	$\text{wfix}(g)$
e	$(w(\text{red}) + w(\text{blue}) + w(\text{green}))^6$
$(1, 2, 3, 4, 5, 6)$	$w(\text{red})^6 + w(\text{blue})^6 + w(\text{green})^6$
$(1, 3, 5)(2, 4, 6)$	$(w(\text{red})^3 + w(\text{blue})^3 + w(\text{green})^3)^2$
$(1, 4)(2, 5)(3, 6)$	$(w(\text{red})^2 + w(\text{blue})^2 + w(\text{green})^2)^3$
$(1, 5, 3)(2, 6, 4)$	$(w(\text{red})^3 + w(\text{blue})^3 + w(\text{green})^3)^2$
$(1, 6, 5, 4, 3, 2)$	$w(\text{red})^6 + w(\text{blue})^6 + w(\text{green})^6$

For any given values of $w(\text{red})$, $w(\text{blue})$ and $w(\text{green})$ we can calculate this sum and find the sum of the weights of the weighted $(6, 3)$ -necklaces.

In general

In general, the value of $\text{wfix}(g)$ depends on its cycle structure. In particular, if g has c_i cycles of length i in its cycle decomposition, then the sum of the weights of the fixed points of g (in its action on B^A) is

$$\text{wfix}(g) = \prod_{i=1}^n \left(\sum_{b \in B} w(b)^i \right)^{c_i}.$$

Notice that if $w(b) = 1$ for all $b \in B$, then this simply reverts to the expression for $|\text{fix}(g)|$.

Pólya's Enumeration Theorem

We have now essentially proved the main theorem of this part of the unit:

Pólya's Enumeration Theorem

Let G be a group acting on a set A , and consider the set B^A of all functions from a set A to a weighted set B with weight function w . Then the sum of the weights of the orbits of G on B^A is given by

$$Z_G \left(\sum_{b \in B} w(b), \sum_{b \in B} w(b)^2, \dots, \sum_{b \in B} w(b)^n \right).$$

Choosing weights

We left unspecified the codomain of the weight function

$$w : B \rightarrow R$$

because we have considerable freedom in choosing R . In particular, R does not *have* to be numerical (like the real or rational numbers) and we usually get more information out of PET when it is not numerical.

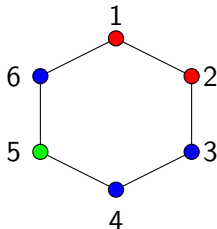
Technically R can be any commutative ring that contains the rationals, but for our purposes it is enough to observe that all the above proofs work when R is the collection of polynomials (over a fixed set of variables) with rational coefficients.

Back to (6, 3) necklaces

Rather than assigning *integers* as the weights of the three colours, we will assign *indeterminates* (or variables) as follows:

$$w(\text{red}) = r \quad w(\text{blue}) = b \quad w(\text{green}) = g.$$

Then the *weight* of a necklace representative is not a number, but a *multivariate polynomial* in the variables r , b and g .



$$w(f) = b \times b \times r \times r \times g \times b = b^3 r^2 g.$$

Using PET

We saw earlier that

$$Z_{C_6}(X_1, X_2, \dots, X_6) = \frac{1}{6}(X_1^6 + X_2^3 + 2X_3^2 + 2X_6).$$

Now substitute

$$\begin{aligned} X_1 &\leftarrow r + b + g \\ X_2 &\leftarrow r^2 + b^2 + g^2 \\ X_3 &\leftarrow r^3 + b^3 + g^3 \\ X_4 &\leftarrow r^4 + b^4 + g^4 \\ X_5 &\leftarrow r^5 + b^5 + g^5 \\ X_6 &\leftarrow r^6 + b^6 + g^6. \end{aligned}$$

The $(6, 3)$ –necklaces

The resulting expression is the multivariate polynomial

$$\begin{aligned} Z_{C_6} = & r^6 + g^6 + b^6 + 5r^4gb + 10r^3g^2b + 10r^3gb^2 + 10r^2g^3b + \\ & 16r^2g^2b^2 + 10r^2gb^3 + 5rg^4b + 10rg^3b^2 + rg^5 + rb^5 + r^5g + r^5b + \\ & 3r^4g^2 + 3r^4b^2 + 4r^3g^3 + 4r^3b^3 + 3r^2g^4 + 3r^2b^4 + gb^5 + g^5b + \\ & 3g^4b^2 + 4g^3b^3 + 3g^2b^4 + 10rg^2b^3 + 5rgb^4. \end{aligned}$$

Each term of this expression corresponds to necklaces with a fixed number of red, green and blue beads. For example, the term $10r^2g^3b$ says that there are 10 orbits with weight r^2g^3b or in other words 10 necklaces with 2 red beads, 3 green beads and 1 blue bead.

In GAP

Unlike languages like Mathematica or Maple, symbolic polynomials are a little bit awkward to handle in GAP. The main reason is that in Mathematica/Maple every undefined term is treated as an indeterminate whereas undefined variables cause GAP to complain.

```
> x^2-3;
```

$$x^2 - 3$$

```
>
```

```
gap> x^2-3;
```

```
Variable: 'x' must have a value
```

```
gap>
```

Indeterminates

Therefore we need to explicitly create any indeterminates that are used; we can give them names for our own convenience, but internally they are all called x_1 , x_2 and so on.

```
gap> x1 := Indeterminate(Rationals,"x1");  
x1  
gap> x2 := Indeterminate(Rationals,"x2");  
x2  
gap> x3 := Indeterminate(Rationals,"x3");  
x3  
gap> x6 := Indeterminate(Rationals,"x6");  
x6  
gap> cyc6 := (x1^6 + x2^3 + 2*x3^2 + 2*x6)/6;  
1/3*x6+1/3*x3^2+1/6*x2^3+1/6*x1^6
```

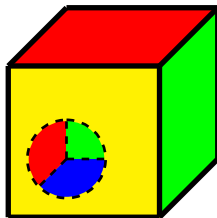
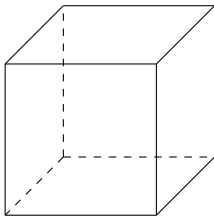
Evaluating the cycle index

The GAP command `Value` is used to evaluate the cycle index.
(The commands defining `r`, `g` and `b` as indeterminates have been omitted.)

```
gap> vars := [x1,x2,x3,x6];  
[ x1, x2, x3, x6 ]  
gap> vals := [r+g+b,r^2+g^2+b^2,r^3+g^3+b^3,r^6+g^6+b^6];  
[ r+b+g, r^2+b^2+g^2, r^3+b^3+g^3, r^6+b^6+g^6 ]  
gap> result := Value(cyc6,vars,vals);  
r^6+r^5*b+r^5*g+3*r^4*b^2+5*r^4*b*g+3*r^4*g^2+4*r^3*b^3+  
10*r^3*b^2*g+10*r^3*b*g^2+4*r^3*g^3+3*r^2*b^4+  
10*r^2*b^3*g+16*r^2*b^2*g^2+10*r^2*b*g^3+3*r^2*g^4+  
r*b^5+5*r*b^4*g+10*r*b^3*g^2+10*r*b^2*g^3+5*r*b*g^4+  
r*g^5+b^6+b^5*g+3*b^4*g^2+4*b^3*g^3+3*b^2*g^4+  
b*g^5+g^6  
gap>
```

The cube

Suppose we have a cube with faces that can be coloured, and have to determine how many inequivalent ways there are to colour it with 2 red, 2 green, 1 blue and 1 yellow face.



First we need to decide what is meant by *equivalent* (and hence inequivalent).

Equivalence for the cube

There are two natural ways of defining when two colourings are equivalent.

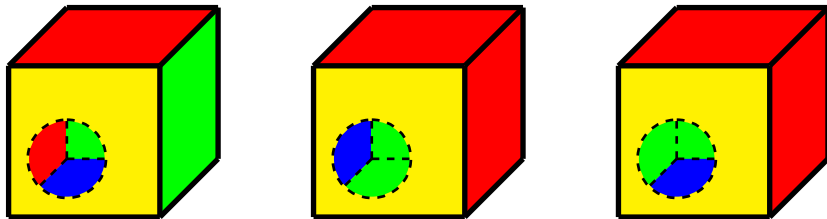
- ▶ Rotations only

The cube can be rotated about a line parallel to the x -, y - or z -axes through the centre of a pair of opposite faces. This corresponds to the motions that can be performed with a physical cube.

- ▶ Rotations and Reflections

In addition to the rotations, we can also *reflect* the cube in a plane passing through the centre points of four parallel edges of the cube.

Two types of equivalence



The second cube is obtained from the first by rotation and the third is obtained from the first by a reflection. The third cube *cannot* be obtained from the first by rotations alone.

Set up for PET

The question reduces to finding the number of orbits on face-colourings of either

- ▶ The group G_1 of rotational symmetries of the cube, or
- ▶ The group G_2 of all symmetries of the cube.

We will work through the case for the group G_1 , leaving G_2 for the exercises.

Identify the group

The first step is to identify the group G_1 as a permutation group acting on *the set of faces* of the cube.

If we name the faces Up, Down, Left, Right, Front and Back then we see that G_1 includes the following three elements

- ▶ Rotation around a line parallel to the x -axis (coming out of the page)

$$a = (U, L, D, R)$$

- ▶ Rotation around a line parallel to the y -axis (going left to right)

$$b = (U, F, D, B)$$

- ▶ Rotation around a line parallel to the z -axis (going up the page)

$$c = (F, R, B, L)$$

In GAP

To put these into GAP we need to encode the faces as numbers, so using Up = 1, Down = 2, Left = 3, Right = 4, Front = 5 and Back = 6 we get

$$a = (1, 3, 2, 4) \quad b = (1, 5, 2, 6) \quad c = (5, 4, 6, 3)$$

```
gap> a := (1,3,2,4);  
(1,3,2,4)  
gap> b := (1,5,2,6);  
(1,5,2,6)  
gap> c := (5,4,6,3);  
(3,5,4,6)  
gap> g1 := Group(a,b,c);  
Group([ (1,3,2,4), (1,5,2,6), (3,5,4,6) ])  
gap> Order(g1);  
24
```

Conjugacy Classes

With a group of order only 24, we can find its cycle index easily by checking each element and adding up the contribution to the cycle index, but we will use a technique that scales better. We need to refine a definition that we have used before.

Definition

Two permutations f and g in a permutation group G are *conjugate in G* if there is an element $h \in G$ such that

$$f = h^{-1}gh.$$

This is an equivalence relation on the permutations in G and the equivalence classes are called the *conjugacy classes* of G .

Permutations in the same conjugacy class have the same cycle structure, but the converse is not true in general.

In GAP

Usually there are far more elements in the group than conjugacy classes, and so working with an entire conjugacy class at a time significantly reduces the problem size.

```
gap> cl := ConjugacyClasses(g1);  
[ ()^G, (3,4)(5,6)^G, (3,5,4,6)^G,  
(1,2)(3,5)(4,6)^G, (1,3,5)(2,4,6)^G ]  
gap>
```

GAP's `ConjugacyClasses` command returns a list identifying the conjugacy classes and giving a representative of each class.

In GAP cont.

We can get the representatives and the size of each conjugacy class easily by using the appropriate GAP commands.

```
gap> for c in cl do  
> Print(Size(c), " ", Representative(c), "\n");  
> od;  
1 ()  
3 (3,4)(5,6)  
6 (3,5,4,6)  
6 (1,2)(3,5)(4,6)  
8 (1,3,5)(2,4,6)  
gap>
```

Cycle Index

We can write down the cycle index for G_1 immediately from the list of conjugacy classes:

$$Z_{G_1} = \frac{1}{24} (X_1^6 + 3X_1^2X_2^2 + 6X_1^2X_4 + 6X_2^3 + 8X_3^2).$$

Now, using the cycle index and PET, we can answer a whole range of questions about face-colourings of the cube.

PET

In particular, we can answer our original question by using PET and making the following substitutions into the cycle index for G_1 .

$$X_1 \leftarrow r + b + g + y$$

$$X_2 \leftarrow r^2 + b^2 + g^2 + y^2$$

$$X_3 \leftarrow r^3 + b^3 + g^3 + y^3$$

$$X_4 \leftarrow r^4 + b^4 + g^4 + y^4$$

The resulting expression is fairly large and nasty, but the number of colourings with 2 red, 2 green, 1 blue and 1 yellow face can easily be found by extracting the coefficient of the term r^2b^2gy which is

$$\dots 8r^2bg^2y \dots$$

For the curious only

In fact

$$\begin{aligned} Z_{G_1} = & r^6 + b^6 + g^6 + y^6 + 2g^3y^3 + g^5y + 2g^4y^2 + rb^5 + rg^5 + ry^5 + \\ & 2r^2b^4 + 2r^2g^4 + 2r^2y^4 + r^5b + r^5g + r^5y + 2r^4b^2 + 2r^4g^2 + 2r^4y^2 + \\ & 2r^3b^3 + 2r^3g^3 + 2r^3y^3 + bg^5 + by^5 + 2b^2g^4 + 2b^2y^4 + b^5g + b^5y + \\ & 2b^4g^2 + 2b^4y^2 + 2b^3g^3 + 2b^3y^3 + gy^5 + 2g^2y^4 + 5r^3bg y + 8r^2b^2gy + \\ & \mathbf{8r^2bg^2y} + 8r^2bg y^2 + 5rb^3gy + 8rb^2g^2y + 8rb^2gy^2 + 5rbgy^3 + \\ & 5rbg^3y + 8rbg^2y^2 + 2r^4bg + 2r^4by + 2r^4gy + 3r^3b^2g + 3r^3b^2y + \\ & 3r^3bg^2 + 3r^3by^2 + 3r^3g^2y + 3r^3gy^2 + 3r^2b^3g + 3r^2b^3y + 6r^2b^2g^2 + \\ & 6r^2b^2y^2 + 3r^2bg^3 + 3r^2by^3 + 3r^2gy^3 + 3r^2g^3y + 6r^2g^2y^2 + 2b^4gy + \\ & 3b^3g^2y + 3b^3gy^2 + 3b^2gy^3 + 3b^2g^3y + 6b^2g^2y^2 + 2rbg^4 + 2rby^4 + \\ & 2rb^4g + 2rb^4y + 3rb^3g^2 + 3rb^3y^2 + 3rb^2g^3 + 3rb^2y^3 + 2rgy^4 + \\ & 3rg^2y^3 + 2rg^4y + 3rg^3y^2 + 2bg y^4 + 3bg^2y^3 + 2bg^4y + 3bg^3y^2. \end{aligned}$$

Counting boolean functions

A *boolean function* on n variables is a function

$$f : \{0, 1\}^n \rightarrow \{0, 1\}.$$

A boolean function can be specified in a number of different ways, with *disjunctive normal form* being a familiar one, where the function is expressed as a disjunction of conjunctions — that is, an OR statement where each term is an AND.

For example we could take

$$f(x_1, x_2, x_3) = x_1 x_2 \overline{x_3} \vee \overline{x_1} x_2 \overline{x_3} \vee x_1 \overline{x_2} \overline{x_3}.$$

Disjunctive normal form is just a way of explicitly listing the n -tuples where the function f takes the value 1, so we could equally well express f by listing them in normal set notation.

In this representation we have

$$f = \{(1, 1, 0), (0, 1, 0), (1, 0, 0)\}.$$

Alternatively we can just view f as a subset of the vertices of the cube, and — conversely — any subset of the vertices of the cube determines a boolean function.

Equivalence

Two boolean functions f and g are said to be *equivalent* if f is obtained from g by any combination of

- ▶ Permuting the variables x_i , and/or
- ▶ Exchanging any variable x_i with its complement $\overline{x_i}$.

The automorphism group of the n -cube Q_n is generated by the operations of

- ▶ Permuting the co-ordinates, and
- ▶ Swapping 0s and 1s in any co-ordinate position.

Number of boolean functions

This implies that two boolean functions are equivalent if and only if there is an automorphism of the cube that maps the two corresponding vertex subsets to each other.

Therefore, the number of equivalence classes of boolean functions on n variables is equal to the number of orbits of $\text{Aut}(Q_n)$ on subsets of $V(Q_n)$.

Computing these numbers is a direct application of Pólya's Enumeration Theorem.

Generating Functions

Cheryl E Praeger

Semester 1, 2004

Generating functions

Another means of organising enumeration. Two examples we have seen already.

Example 1. Binomial coefficients.

Let $X = \{1, 2, \dots, n\}$

$c_k = \#$ k -element subsets of $X = \binom{n}{k}$.

Consider

$$F(x) = \sum_{k=0}^n c_k x^k.$$

This is the generating function for k -element subsets of X . We can find it explicitly:

$$F(x) = \sum_{k=0}^n \binom{n}{k} x^k = (1+x)^n.$$

Example 2. Cycle types of permutations.

Type $\underline{a} = 1^{a_1} 2^{a_2} \dots n^{a_n}$

i.e. a_i cycles of length i , where $\sum_{i=1}^n a_i i = n$.

The cycle index is the generating function for cycle types. For a permutation group G

$$Z(G; x_1, \dots, x_n) = \sum_{\underline{a}} c_{\underline{a}} x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}$$

where $c_{\underline{a}} = \#$ elements in G with cycle type \underline{a} .

- ▶ Generating functions are defined for any sequence $\underline{a} = (a_1, a_2, \dots)$.
We usually assume \underline{a} is an infinite sequence.
- ▶ When \underline{a} is of finite length $\underline{a} = (a_1, a_2, \dots, a_n)$ we can define $a_i = 0$ for $i > n$.
- ▶ There can be many variables (as for the cycle index) but we will consider mainly one variable generating functions.
- ▶ Sometimes we can find the functions explicitly (as for the k -subsets) and in other cases we may only find information about their asymptotic or analytic properties.

Suppose f_n is the number of objects (of a certain kind) of “size” n .
The **ordinary generating function** (ogf) for these objects is

$$\sum_{n \geq 0} f_n x^n$$

and the **exponential generating function** (egf) for these objects is

$$\sum_{n \geq 0} \frac{f_n x^n}{n!}.$$

These are called “formal power series” because we are not concerned (at least not right now) in letting x take on any particular value and we ignore (for now) questions of convergence and divergence.

Example 3. Partition function. (An ordinary generating function).

$p(n) = \#$ partitions of n

$$P(x) = 1 + \sum_{n \geq 1} p(n)x^n. \quad (\text{Convention: } p(0) = 1.)$$

Let $p_k(n) = \#$ partitions of n with exactly k (non-zero) parts.

So $p_k(n) = 0$ for $k > n$, and for $k = 0, n \geq 1$, while $p_0(0) = 1$

$$P_k(n) = \sum_{n \geq 0} p_k(n)x^n \quad \text{the } k\text{-part partition function.}$$

Recurrences on coefficients lead to equations on the generating functions.

Exercise. Use the recursion you proved for Assignment 2

$$p_k(n) = p_k(n - k) + p_{k-1}(n - k)$$

to prove that

$$P_k(x) = \frac{x}{1 + x^k} P_{k-1}(x).$$

You can use this to find an explicit formula for $P_k(t)$.

Examples 4. Consider the all-1 sequence $(1, 1, 1, \dots)$.

$$(\text{ogf}) \quad F(x) = \sum_{n=0}^{\infty} 1 \cdot x^n.$$

Note $(1 + x + x^2 + \dots + x^n)(1 - x) = 1 - x^{n+1}$ so for $|x|$ small and $n \rightarrow \infty$

$$(1 + x + x^2 + \dots + x^n) = \frac{1 - x^{n+1}}{1 - x} \longrightarrow \frac{1}{1 - x}$$

$$F(x) = \frac{1}{1 - x}.$$

$$(\text{egf}) \quad G(x) = \sum_{n=0}^{\infty} \frac{1}{n!} x^n = e^x.$$

We can use simple generating functions like these to determine more interesting/complicated ones.

For sequences $(a_n)_{n \geq 0}$ and $(b_n)_{n \geq 0}$.

ogfs: $A(x) = \sum_{n \geq 0} a_n x^n$

$$B(x) = \sum_{n \geq 0} b_n x^n$$

Addition:

$$A(x) + B(x) = \sum_{n \geq 0} (a_n + b_n) x^n, \text{ the ogf for } (a_n + b_n)_{n \geq 0}.$$

Multiplication:

$$A(x).B(x) = \sum_{n \geq 0} \left(\sum_{k=0}^n a_k b_{n-k} \right) x^n,$$

the ogf for $(\sum_{k=0}^n a_k b_{n-k})_{n \geq 0}$.

$$\text{egfs: } A(x) = \sum_{n \geq 0} \frac{a_n}{n!} x^n, \quad B(x) = \sum_{n \geq 0} \frac{b_n}{n!} x^n$$

Addition:

$$A(x) + B(x) = \sum_{n \geq 0} \frac{a_n + b_n}{n!} x^n, \text{ the egf for } (a_n + b_n)_{n \geq 0}.$$

Multiplication:

$$\begin{aligned} A(x).B(x) &= \sum_{n \geq 0} \left(\sum_{k=0}^n \frac{a_k}{k!} \frac{b_{n-k}}{(n-k)!} \right) x^n \\ &= \sum_{n \geq 0} \frac{1}{n!} \left(\sum_{k=0}^n \binom{n}{k} a_k b_{n-k} \right) x^n \\ &\quad \text{the egf for } \left(\sum_{k=0}^n \binom{n}{k} a_k b_{n-k} \right)_{n \geq 0}. \end{aligned}$$

We can also do calculus: differentiate, take logs etc.

Example 5. Derangements: $d(n) = \#$ derangements on $\{1, 2, \dots, n\}$.

Permutations with k fixed points are derangements on the remaining $n - k$ points.

For a given k there are $\binom{n}{k}$ subsets of size k and hence $\binom{n}{k}d(n - k)$ permutations with exactly k fixed points. Hence

$$n! = \sum_{k=0}^n \binom{n}{k} d(n - k).$$

Form the egf for the sequence $(n!)_{n \geq 0}$.

$$F(x) = \sum_{n \geq 0} \frac{n!}{n!} x^n = \sum_{n \geq 0} x^n = \frac{1}{1 - x}.$$

But we also have

$$\begin{aligned} F(x) &= \sum_{n \geq 0} \frac{1}{n!} \left(\sum_{k=0}^n \binom{n}{k} d(n-k) \right) x^n \\ &= A(x) \cdot D(x) \end{aligned}$$

where $A(x)$ is the egf for $(1)_{n \geq 0}$, i.e. $A(x) = e^x$
and $D(x)$ is the egf for $(d(n))_{n \geq 0}$.

$$\text{Hence } D(x) = \frac{F(x)}{A(x)} = \frac{1}{1-x} \cdot \frac{1}{e^x} = \frac{e^{-x}}{1-x}.$$

We can use this to find $d(n)$ by expanding both sides and equating coefficients.

$$\begin{aligned}\sum_{n \geq 0} \frac{d(n)}{n!} x^n &= \frac{1}{1-x} \cdot e^{-x} = \left(\sum_{n \geq 0} x^n \right) \left(\sum_{n \geq 0} \frac{(-x)^n}{n!} \right) \\ &= \sum_{n \geq 0} \left(\sum_{k=0}^n \frac{(-1)^k}{k!} \right) x^n.\end{aligned}$$

So, equating coefficients:

$$d(n) = n! \sum_{k=0}^n \frac{(-1)^k}{k!}.$$

This alternative derivation is sometimes simpler than combinatorial or “Pólya-theoretic” methods.

The Partition Function

Infinite products occur and are useful — the partition function

$$P(t) = \sum_{n \geq 0} p(n)t^n$$

where $p(0) = 1$ (convention) and $p(n) = \#$ partitions of n .

Each partition of n consists of a_i parts of size i ($i = 1, \dots, n$) where each $a_i \geq 0$ and $a_1 \cdot 1 + a_2 \cdot 2 + \dots + a_n \cdot n = n$.

So: $p(n)$ = the coefficient of t^n in

$$\prod_{i \geq 1} (1 + t^i + t^{2i} + t^{3i} + \dots).$$

The Partition Function continued

To simplify this product recall

$$\frac{1}{1-x} = 1 + x + x^2 + \dots$$

So taking $x = t^i$, $1 + t^i + t^{2i} + \dots = \frac{1}{1-t^i}$.

Hence $p(n) = \text{coeff. of } t^n \text{ in } \prod_{i \geq 1} \frac{1}{1-t^i}$.

So

$$P(t) = \prod_{i \geq 1} \frac{1}{1-t^i}$$

This is a famous result going back to Euler.

The Partition Function continued

The i^{th} factor is $1 + t^i + t^{2i} + \dots$

Note: coefficient of t^{ij} is 1 and this is the number of partitions of ij with **all parts of size i** .

The partition function $P(t)$ is the product over all i of the (rather trivial) generating functions $P_i(t) = 1 + t^i + t^{2i} + \dots$ for the partitions with all parts of size i .

We can use this observation in several ways.

First way: To get at $p_{\text{odd}}(n) = \#$ partitions of n with all odd parts. We just take the $P_i(t)$ with i odd so

$$P_{\text{odd}}(t) = \sum_{n \geq 0} p_{\text{odd}}(n) t^n = \prod_{i \text{ odd}} \frac{1}{1 - t^i}$$

Second way: Restricting multiplicities.

Suppose we only want partitions in which all parts have distinct sizes; i.e. a_i parts of size i where each $a_i = 0$ or 1 and $\sum a_i i = n$.

Let $p_{\text{unequal}}(n) = \#$ partitions of n with distinct parts.

Then $p_{\text{unequal}}(n)$ is the coefficient of t^n in $\prod_{i \geq 1} \frac{1}{1+t^i}$.

So

$$\begin{aligned} P_{\text{unequal}}(t) &= \sum_{n \geq 0} p_{\text{unequal}}(n) t^n \\ &= \prod_{i \geq 1} (1 + t^i). \end{aligned}$$

You can experiment with many other restrictions e.g. all parts even, no part occurs more than k times, etc.

A Bizarre Coincidence

In the expression for $P_{\text{unequal}}(t)$ write each $1 + t^i$ as $\frac{1-t^{2i}}{1-t^i}$ so

$$P_{\text{unequal}}(t) = \prod_{i \geq 1} \frac{1 - t^{2i}}{1 - t^i}.$$

Every $1 - t^{2i}$ in the numerator (i^{th} term) cancels with $1 - t^{2i}$ in the denominator ($2i^{\text{th}}$ term) and leaves

$$P_{\text{unequal}}(t) = \prod_{i \text{ odd}} \frac{1}{1 - t^i} = P_{\text{odd}}(t).$$

This slightly hand-waving proof is hard to believe, so here is a “bijective” “combinatorial proof”.

Take a partition λ of n into odd parts

$$\lambda : a_{2i-1} \text{ parts of size } 2i - 1.$$

Define a new partition $\mu = \mu(\lambda)$ depending on and determined by λ as follows.

Write each positive integer (uniquely) as $2^k j$ where $k \geq 0$ and j is odd.

μ has either zero or 1 part of size $2^k j$ (for each $k \geq 0$ and odd j), namely μ has a part of size $2^k j \Leftrightarrow a_j$ contains the term 2^k in its binary expansion.

Examples

$$\begin{aligned}n = 7 \quad \lambda : 1 + 3 + 3 \\ a_1 = 1, a_3 = 2\end{aligned}$$

So μ has 1 part of size $2^0.1 = 1$
and 1 part of size $2^1.3 = 6$

$$\begin{aligned}n = 19 \quad \lambda : 1 + 3 + 3 + 3 + 3 + 3 + 3 \\ a_1 = 1, a_3 = 6 = 2 + 4\end{aligned}$$

Here μ has 1 part of size $2^0.1 = 1$
and 1 part of size $2^1.3 = 6$
and 1 part of size $2^2.3 = 12$

Always $\mu = \mu(\lambda)$ is a partition of n with distinct parts, and the correspondence $\lambda \mapsto \mu(\lambda)$ is 1 – 1 and onto.

Why is μ a partition of n ?

$$n = \sum_{i \text{ odd}} a_i i \text{ by definition of } \lambda.$$

Let $a_i = 2^{k_{i1}} + 2^{k_{i2}} + \dots$ (binary expansion).

Then $n = \sum_{i,j} 2^{k_{ij}} \cdot i = \text{sum of sizes of parts of } \mu.$

Why is $\lambda \mapsto \mu(\lambda) 1 - 1$?

Suppose $\mu(\lambda) = \mu(\lambda')$ and λ' has a'_i parts of size i , \forall odd i .

By definition of μ : μ has a part of size $2^k j \Leftrightarrow 2^k$ occurs in binary expansion of a_j (and a'_j).

This means a_j and a'_j have exactly the same binary expansion, so $a_j = a'_j$ for all j . So $\lambda = \lambda'$.

Why is $\lambda \mapsto \mu(\lambda)$ onto?

Take any partition of n into distinct parts μ .

For each part $2^k j$ (j odd)

“put 2^k into a_j .”

i.e. for each odd j , define $a_j =$ sum of all 2^k such that μ has a part of size $2^k j$.

There are also generating function *proofs* for results where no natural combinatorial proofs are known.

- ▶ the number of self-complementary digraphs on $2n$ vertices is equal to the number of self-complementary graphs on $4n$ vertices.
- ▶ the number of self-complementary graphs on n vertices is equal to the difference between the numbers of graphs with an even number of edges and an odd number of edges on n vertices.

Unlabelled graphs and their connected components

$g_n = \#$ unlabelled graphs on n vertices

$c_n = \#$ connected graphs on n vertices.

Consider ogf for these

$$C(t) = \sum_{n \geq 1} c_n t^n, \quad G(t) = \sum_{n \geq 0} g_n t^n \quad (g_0 = 1).$$

Each unlabelled graph on n vertices arises as a union of its connected components, say c_Γ copies of each connected unlabelled graph Γ where each $c_\Gamma \geq 0$ and $\sum_\Gamma c_\Gamma n(\Gamma) = n$.

Here $n(\Gamma) = \#$ vertices of Γ .

So g_n = the coefficient of t^n in

$$\prod_{\Gamma} (1 + t^{n(\Gamma)} + t^{2n(\Gamma)} + \dots)$$

where the product is over all finite unlabelled graphs Γ . This product is equal to

$$\prod_{n \geq 1} (1 + t^n + t^{2n} + \dots)^{c_n}$$

since for each n there are c_n factors $(1 + t^n + \dots)$, one for each of the c_n unlabelled connected graphs on n vertices.

This function is equal to $\prod_{n \geq 1} \frac{1}{(1 - t^n)^{c_n}}$. Thus

$$G(t) = \prod_{n \geq 1} \frac{1}{(1 - t^n)^{c_n}}.$$

Remark: We can find g_n (Pólya theory) and solve for the c_n , one by one.

Question: How might we find $C(t) = \sum_{n \geq 1} c_n t^n$ from this? Or at least see an equation relating $C(t)$ and $G(t)$.

$$\log G(t) = - \sum_{n \geq 1} c_n \log(1 - t^n)$$

by an extension of the properties of “log”. (This can be proved.)

Then using the Taylor expansion of \log :

$$\begin{aligned}\log G(t) &= -\sum_{n \geq 1} c_n \log(1 - t^n) \\&= \sum_{n \geq 1} c_n \left(\sum_{j \geq 1} \frac{t^{jn}}{j} \right) \\&= \sum_{j \geq 1} \frac{1}{j} \left(\sum_{n \geq 1} c_n (t^j)^n \right) \\&= \sum_{j \geq 1} \frac{C(t^j)}{j}\end{aligned}$$

Hence

$$G(t) = \exp\left(\sum_{j \geq 1} \frac{C(t^j)}{j}\right).$$

Exercises I

Exercise 1: Use the recursion you proved for Assignment 2

$$p_k(n) = p_k(n - k) + p_{k-1}(n - k)$$

to prove that

$$P_k(x) = \frac{x}{1 + x^k} P_{k-1}(x).$$

Hence find an explicit formula for $P_k(t)$.

Exercise 2: The Fibonacci Numbers are defined by $F_0 = 1$, $F_1 = 1$, $F_2 = 2$ and, for all $n \geq 2$, $F_n = F_{n-1} + F_{n-2}$.

- (a) Find an equation satisfied by the ogf for $(F_n)_{n \geq 1}$.
- (b) Solve it to find the ogf.

- (c) (Link with partitions.) Show that F_n is the number of *ordered* partitions of n with all parts equal to 1 or 2. [e.g. the ordered partitions $1 + 2$ and $2 + 1$ of 3 are regarded as different.]

Exercises II

Exercise 3: (Exercise 11 on p70 of Cameron's book)

- (a) Let $s(n)$ be the number of sequences (x_1, \dots, x_k) of integers satisfying $1 \leq x_i \leq n$ for all i and $x_{i+1} \geq 2x_i$ for $i = 1, \dots, k-1$. (The length of the sequence is not specified; in particular, the empty sequence is included.) Prove the recurrence

$$s(n) = s(n-1) + s(\lfloor \frac{n}{2} \rfloor)$$

for $n \geq 1$, with $s(0) = 1$. Calculate a few values of s . Show that the generating function $S(t)$ satisfies $(1-t)S(t) = (1+t)S(t^2)$.

Exercises III

Exercise 3 continued:

- (b) Let $u(n)$ be the number of sequences (x_1, \dots, x_k) of integers satisfying $1 \leq x_i \leq n$ for all i and $x_{i+1} > \sum_{j=1}^i x_j$ for $i = 1, \dots, k-1$. Calculate a few values of u . Can you discover a relationship between s and u ? Can you prove it?

Exercises IV

Exercise 4: Let $g_n(m) = \#$ labelled graphs on n vertices with m edges.

Define the ogf for $g_n(m)$ by

$$G_n(x) = \sum_{m \geq 0} g_n(m) x^m.$$

Recursion: Let $\mathcal{S}_{n,m}$ be the set of labelled graphs on n vertices with m edges.

Define a map ϕ from X to Y , where

$$\begin{aligned} X &= \{(e, \Gamma) \mid \Gamma \in \mathcal{S}_{n,m+1}, e \in E(\Gamma)\} \\ Y &= \{(e', \Gamma') \mid \Gamma' \in \mathcal{S}_{n,m}, e' \notin E(\Gamma')\}, \end{aligned}$$

by $\phi : (e, \Gamma) \mapsto (e, \Gamma \setminus e)$ where $\Gamma \setminus e$ denotes the graph Γ with the edge e removed.

Exercises V

Exercise 4 continued:

For example, if Γ is the triangle on vertex set $\{1, 2, 3\}$, then $\phi : (\{1, 2\}, \Gamma) \rightarrow (\{1, 2\}, P)$ where P is the path with edges $\{1, 3\}$, and $\{2, 3\}$.

- (a) Prove that ϕ is a well-defined bijection.
- (b) Hence prove that

$$(m+1)g_n(m+1) = \left(\binom{n}{2} - m \right) g_n(m).$$

Exercises VI

Exercise 4 continued:

(c) Multiply by x^m and add over all $m \geq 0$ to obtain

$$\sum_{m \geq 1} (m+1) g_n(m+1) x^m = \binom{n}{2} G_n(x) - \sum_{m \geq 0} m g_n(m) x^m.$$

What is this? Differentiate $G_n(x)$ with respect to x :

$$G'_n(x) = \sum_{m \geq 1} m g_n(m) x^{m-1}.$$

(d) Prove that $G'_n(x) = \binom{n}{2} \frac{G_n(x)}{1+x}$ and deduce that $G_n(x) = (1+x) \binom{n}{2}$. Can you also give a more direct proof of this result?