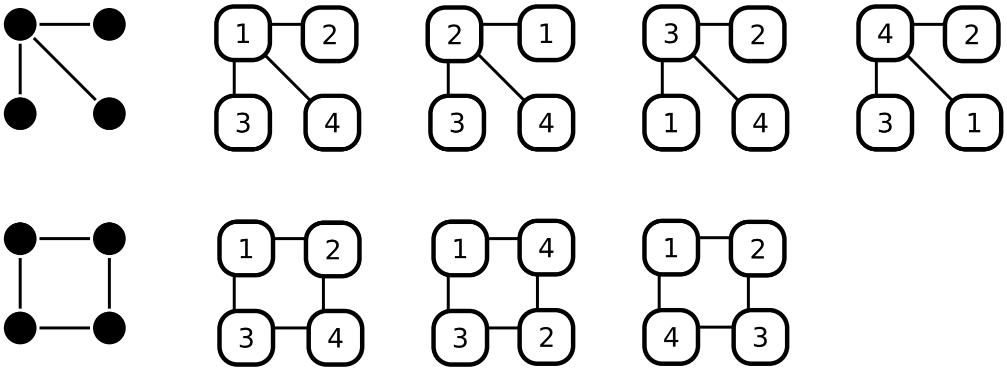
Labelled combinatorial classes

Contents

1 Labelling Atoms

A great many objects in combinatorics like to be labelled — indeed in many cases counting labelled objects is significantly easier than counting their unlabelled siblings — graphs and trees particularly. So what do we mean by labelled? Since the objects we consider are constructed from atomic pieces, simply attatch a label (wlog a natural number) to each atomic piece.



The first unlabelled graph corresponds to 4 different labelled graphs, while the second corresponds to 3.

1.1 Well-labelling

Labelling is a very intuitive notion, but we have a formal defintion anyhow:

Definition. A labelled class of combinatorial objects is a combinatorial class such that every atomic component (atom) is labelled by a distinct integer, and the set of labels associated to an object of size n is the set $\{1, 2, \ldots, n\}$. In this case we say that the objects are well-labelled. If the set of labels is not $\{1, 2, \ldots, n\}$, but still distinct, then we say theobject is weakly labelled.

Going back to the above graph example — there are $2^{\binom{4}{2}} = 64$ labelled graphs of 4 vertices (every edge is there or not), but only 11 unlabelled graphs.

1.2 The Exponential Generating Function (egf)

We do not use ogfs to enumerate labelled classes (though one can), instead we use exponential generating functions.

Definition. The exponential generating function (egf) of a sequence (A_n) is the formal power series

$$A(z) = \sum_{n \geq 0} A_n \frac{z^n}{n!} \qquad\qquad = \sum_{\alpha \in \mathcal{A}} \frac{z^{|\alpha|}}{|\alpha|!}$$

Again we need the neutral class that contains ϵ which has size zero and no label. Similarly the atomic class contains a single well-labelled object of size 1. So we have $\mathcal{Z} = \{①\}$. The egfs are

$$E(z) = 1 \qquad\qquad Z(z) = z,$$

which coincides with their ogf, incidentally.

1.3 Examples

We have already seen permutations. We now think of them as a labelled line of n vertices. Since $P_n = n!$ the egf is

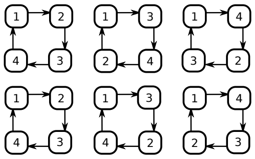
$$P(z) = \sum_{n \geq 0} n! \frac{z^n}{n!} = \frac{1}{1 - z}$$

which is nice and simple.

Example. The class $\mathcal{U}$ of urns consists of completely disconnected labelled graph. Since there are no edges, there can only be a single labelling and thus $U_n = 1$. Hence

$$U(z) = \sum_{n\geq 0} \frac{z^n}{n!} = e^z.$$

Example. Circular graphs, $\mathcal{C}$, are oriented cycles (so $1 \to 2 \to 3 \to 1 \not\equiv 1 \to 3 \to 2 \to 1$).



One can simply decompose such cycles by cutting them on either side of the ① and unrolling them. This gives a permutation of $2, \ldots, n$ and there are $(n-1)!$ such objects. This is a bijective construction and thus $C_n = (n-1)!$.

$$C(z) = \sum_{n\geq 1} \frac{(n-1)!}{n!} z^n = \sum_{n\geq 1} \frac{z^n}{n} = \log \frac{1}{1-z}.$$

Remark that labelled cycles are much easier than unlabelled ones.

1.4 Aside: comparing to unlabelled families

More generally one can find examples of enumerations of labelled objects $\mathcal{A}$ and their unlabelled counterparts $\hat{\mathcal{A}}$ such that

$$1 \leq \frac{A_n}{\hat{A}_n} \leq n!$$

To show both sides of this — consider the class of Urns. Here $U_n = \hat{U_n} = 1$. And similarly, consider permutations: $P_n = n!$, but one can consider them as labellings of a linear graph on n-vertices, so $\hat{P}_n = 1$. Note that one can also consider permutations to be sets of cycles, then the unlabelled version of the object is a partition.

2 Admissible constructions

So the combinatorial sum still works just fine, but clearly we are going to have difficulties with cartesian product — the labels don't work quite right. In particular, if we take $\beta \in \mathcal{B}$ and $\gamma \in \mathcal{C}$ and glue them together to get (β, γ) the label ① appears twice, so the object is not well-labelled. Clearly we need to relabel things carefully to make this work.

Proposition (Binomial convolution formula)**.** *Let $A(z), B(z), C(z)$ be egfs of sequences A_n, B_n, C_n such that $A(z) = B(z) \cdot C(z)$ then*

$$A_n = \sum_{k=0}^{n} \binom{n}{k} B_k C_{n-k}$$

Proof. Expand:

$$\begin{aligned} A(z) = B(z) \cdot C(z) &= \sum_n B_n \frac{z^n}{n!} \cdot \sum_n C_n \frac{z^n}{n!} \\ &= \sum_n \left(\sum_{k=0}^{n} \frac{B_k}{k!} \frac{C_{n-k}}{(n-k)!} \right) z^n \\ &= \sum_n n! \left(\sum_{k=0}^{n} \frac{B_k}{k!} \frac{C_{n-k}}{(n-k)!} \right) \frac{z^n}{n!} \\ &= \sum_n \sum_{k=0}^{n} \underbrace{\frac{n!}{k!(n-k)!}}_{\binom{n}{k}} B_k C_{n-k} \frac{z^n}{n!} \\ &= \sum_n \sum_{k=0}^{n} \binom{n}{k} B_k C_{n-k} \frac{z^n}{n!}. \end{aligned}$$

□

2.1 Labelled products

Next we describe how to generate labelled products. In the unlabelled case, a pair (β, γ) with $\beta \in \mathcal{B}$ and $\gamma \in \mathcal{C}$ gave rise to a single object of size $|\beta| + |\gamma|$. In the labelled case we will generate a *set* of objects. We describe how we get this set. Essentially, we keep the structure of the pair (β, γ) and we generate new labels that preserve the order relation among labels. We can do this formally using the following two operations:

- reduction: For a weakly labelled structure size n, this reduces its labels to the standard interval $[1, \dots, n]$ while keeping the relative order fixed. Eg $\langle 4, 6, 2, 9 \rangle$ becomes $\langle 2, 3, 1, 4 \rangle$. Denote this operation by $\rho(\alpha)$.
- expansion: roughly — the inverse of reduction. Let $e : \mathbb{N} \to \mathbb{Z}$ be any strictly increasing function. Then the expansion of a well-labelled object α by e is denoted $e(\alpha)$ and results in a weakly-labelled object in which the label j is replaced by $e(j)$. So $\langle 2, 3, 1, 4 \rangle$ may expand to $\langle 7, 10, 2, 88 \rangle$ or $\langle 3, 9, 1, 15 \rangle$ etc etc.

Now, given any two objects $\beta \in \mathcal{B}$ and $\gamma \in \mathcal{C}$ their labelled product (or product) is $\beta \star \gamma$. This is a set of well-labelled pairs (β', γ') that reduce back to β, γ.

$$\beta \star \gamma = \{(\beta', \gamma') \text{ s.t. it is well-labelled and } \rho(\beta') = \beta, \rho(\gamma') = \gamma\}$$

So how big is this set? If $|\beta| = n_1$ and $|\gamma| = n_2$ then

$$\text{card}(\beta \star \gamma) = \binom{n_1 + n_2}{n_1, n_2} = \binom{n}{n_1}$$

where $n = n_1 + n_2$. You can see this by considering all the "new" labels and allocating n_1 of them to the part of the object coming from β and the rest go to the part coming from γ. Then assign each block of labels so as to preserve the original orderings.

Definition (Labelled product). The labelled product $\mathcal{B} \star \mathcal{C}$ is obtained by forming all ordered pairs from $\mathcal{B} \times \mathcal{C}$ and computing all possible order-consistent relabellings. That is

$$\mathcal{B} \star \mathcal{C} = \cup_{\beta \in \mathcal{B}, \gamma \in \mathcal{C}} (\beta \star \gamma)$$

Now we can look at the admissible constructions.

2.2 Labelled product

When $\mathcal{A} = \mathcal{B} \star \mathcal{C}$ the corresponding counting sequences satisfy

$$A_n = \sum_{n_1+n_2=n} \binom{n}{n_1, n_2} B_{n_1} C_{n_2}$$

The product $B_{n_1}C_{n_2}$ takes care of all possible pairings of objects and the binomial takes care of the possible relabellings. This is just the binomial convolution of the two sequences and thus

$$\mathcal{A} = \mathcal{B} \star \mathcal{C} \qquad \Rightarrow \qquad A(z) = B(z) \cdot C(z)$$

2.3 Sequences

The kth (labelled) power of $\mathcal{B}$ is just the k-fold labelled product of $\mathcal{B}$ with itself. It is denoted $\textsc{Seq}_k(\mathcal{B})$. The sequence class is

$$\textsc{Seq}(\mathcal{B}) = \mathcal{E} + \mathcal{B} + \mathcal{B} \star \mathcal{B} + \cdots = \cup_{k \geq 0} \textsc{Seq}_k(\mathcal{B})$$

These translate to the following operations on the egf

$$\begin{aligned} \mathcal{A} &= \textsc{Seq}_k(\mathcal{B}) \qquad \Rightarrow \qquad & A(z) &= B(z)^k \\ \mathcal{A} &= \textsc{Seq}(\mathcal{B}) \qquad \Rightarrow \qquad & A(z) &= \frac{1}{1 - B(z)} \qquad\qquad \mathcal{B}_0 = \varnothing \end{aligned}$$

2.4 Sets

The class of sets of k-components of $\mathcal{B}$ is denoted $\textsc{Set}_k(B)$. Formally it is defined as a k-sequence counted modulo permutation of the components. That is $\textsc{Set}_k(\mathcal{B}) = \textsc{Seq}_k(\mathcal{B})/\mathbf{R}$ where $\mathbf{R}$ is an equivalence relation that identifies two sequences if one is simply a permutation of the components of the other. The labelled set construction is then defined by

$$\textsc{Set}(\mathcal{B}) = \cup_{k \geq 0} \textsc{Set}_k(\mathcal{B})$$

If we take a labelled k-set, we can order its components in $k!$ different ways to get $k!$ labelled k-sequences. Each component must be distinct since the k-set must be well-ordered. In reverse we can consider the smallest label in each component of a k-sequnce (they must all be different) and then reduce these labels to get a permutation of k. Hence we must have

$$\begin{aligned} \mathcal{A} &= \textsc{Set}_k(\mathcal{B}) \qquad \Rightarrow \qquad & A(z) &= \frac{1}{k!} B(z)^k \\ \mathcal{A} &= \textsc{Set}(\mathcal{B}) \qquad \Rightarrow \qquad & A(z) &= \exp(B(z)) \end{aligned}$$

Note that this is so much easier than the multiset construction for the unlabelled case since components must be distinct thanks to their labels.

2.5 Cycles

The class of k-cycles of $\mathcal{B}$ is denoted $\textsc{Cyc}_k(\mathcal{B})$. It is defined as a k-sequence counted modulo cyclic shifts of it components: $\textsc{Cyc}_k(B) = \textsc{Seq}_k(\mathcal{B})/\mathrm{S}$ where S is an equivalence relation that identifies two sequences if the components of one is a cyclic shift of the components of the other. Since any k-sequence is well-labelled, its components are necesarrily distinct and thus there is a k-to-one mapping between k-sequences and k-cycles. Thus

$$\begin{aligned} \mathcal{A} &= \textsc{Cyc}_k(\mathcal{B}) \qquad \Rightarrow \qquad & A(z) &= \frac{1}{k} B(z)^k \\ \mathcal{A} &= \textsc{Cyc}(\mathcal{B}) \qquad \Rightarrow \qquad & A(z) &= \log \frac{1}{1 - B(z)} \end{aligned}$$

Again — this is much easier because the components are distinct thanks to their labelling.

2.6 Admissibility Theorem

Thus we have now proved

Theorem. *The constructions of combinatorial sum, labelled product, sequence, set and cycle all admissible. The operators are*

$$\begin{array}{rll}
\textit{sum} & \mathcal{A}=\mathcal{B}+\mathcal{C} & A(z)=B(z)+C(z) \\[2em]
\textit{labelled product} & \mathcal{A}=\mathcal{B}\star\mathcal{C} & A(z)=B(z)C(z) \\[2em]
\textit{sequence} & \mathcal{A}=\textsc{Seq}(\mathcal{B}) & A(z)=\dfrac{1}{1-B(z)} \\
 & \mathcal{A}=\textsc{Seq}_k(\mathcal{B}) & A(z)=B(z)^k \\[2em]
\textit{set} & \mathcal{A}=\textsc{Set}(\mathcal{B}) & A(z)=\exp(B(z)) \\
 & \mathcal{A}=\textsc{Set}_k(\mathcal{B}) & A(z)=\dfrac{1}{k!}B(z)^k \\[2em]
\textit{cycle} & \mathcal{A}=\textsc{Cyc}(\mathcal{B}) & A(z)=\log\dfrac{1}{1-B(z)} \\
 & \mathcal{A}=\textsc{Cyc}_k(\mathcal{B}) & A(z)=\dfrac{1}{k}B(z)^k
\end{array}$$

where for sequence, set and cycle it is assumed that $\mathcal{B}_0=\varnothing$.

Note how the cycle and set operations are nearly inverses of each other.

3 Surjections

Consider the class of surjections:

$$\mathcal{R}=\textsc{Seq}(\textsc{Set}_{\geq 1}(\mathcal{Z})).$$

http://www.nourishingdays.com/2009/02/make-yogurt-in-your-crock-pot/ A mapping from A to B is a surjection if every element of B is mapped to be at least one element of A. Now let $\mathcal{R}_n^{(r)}$ denote the set of surjections from $[1,n]$ onto $[1,r]$. Further let $\mathcal{R}^{(r)}=\cup_n\mathcal{R}_n^{(r)}$.

Consider the following surjection, ϕ from $[1,9]$ to $[1,4]$

$$\begin{array}{ccccc}
1\to 3 & 2\to 2 & 3\to 4 & 4\to 2 & 5\to 1 \\
 & 6\to 1 & 7\to 2 & 8\to 3 & 9\to 4
\end{array}$$

Now consider the preimage of each point

$$\begin{aligned}
\phi^{-1}(1)&=\{5,6\}\\
\phi^{-1}(2)&=\{2,4,7\}\\
\phi^{-1}(3)&=\{1,8\}\\
\phi^{-1}(4)&=\{3,9\}
\end{aligned}$$

This is clearly an ordered sequence of non-empty sets. More generally one can decompose a surjection to $[1,r]$ as an r-sequence of sets. Thus

$$\begin{array}{cc}
\mathcal{R}^{(r)}=\textsc{Seq}_r(\mathcal{V}) & \mathcal{V}=\textsc{Set}_{\geq 1}(\mathcal{Z}) \\
V(z)=\exp(z)-1 & R^{(r)}(z)=(e^z-1)^r
\end{array}$$

Note that here $\mathcal{V} \cong \mathcal{U} - \{\epsilon\}$ — non-empty urns

We can expand this to get at $R_n^{(r)}$

$$\begin{aligned} R_n^{(r)} &= n![z^n]\sum_{j=0}^{r}(-1)^j\binom{r}{j}e^{(r-j)z} \\ &= \sum_{j=0}^{r}(-1)^j\binom{r}{j}(r-j)^n \end{aligned}$$

which is related to stirling numbers $\left\{ {n \atop r} \right\}$, which we will learn about next.

4 Set Partitions

4.1 Definition

Let us look at set-partitions. Consider the interval $[1, n]$. We can partition this into r distinct subsets (called blocks). For example $[1, 2, 3, 4]$ can be partitioned into

- 1 set = $[1, 2, 3, 4]$
- 2 sets = $[1, 2, 3|4]$ $[1, 2, 4|3]$ $[1, 3, 4|2]$ $[1|2, 3, 4]$ $[1, 2|3, 4]$ $[1, 3|2, 4]$ $[1, 4|2, 3]$
- 3 sets = $[1, 2|3|4]$ $[1, 3|2|4]$ $[1, 4|2|3]$ $[1|2, 3|4]$ $[1|2, 4|3]$ $[1|2|3, 4]$
- 4 sets = $[1|2|3|4]$

So let $S_n^{(r)}$ be the number of ways of partitioning an n-set into r-blocks, then we have

$$S_4^{(1)} = 1 \qquad S_4^{(2)} = 7 \qquad S_4^{(3)} = 6 \qquad S_4^{(4)} = 1$$

The numbers $S_n^{(r)}$ are called the Stirling partition numbers (or Stirling numbers of the second kind) and are frequently denoted $\left\{ {n \atop r} \right\}$.

4.2 Set partitions as a labelled class

Now let $\mathcal{S}^{(r)}$ denote the class of set partitions in r-blocks. Unlike the surjections we just studied, these blocks are not ordered. Thus we have a set of non-empty sets

$$\mathcal{S}^{(r)} = \textsc{Set}_r(\mathcal{V}) \qquad \mathcal{V} = \textsc{Set}_{\geq 1}(\mathcal{Z})$$

$$S^{(r)}(z) = \frac{1}{r!}(e^z - 1)^r$$

so we clearly have the relation

$$S_n^{(r)} = \frac{1}{r!}R_n^{(r)} \qquad = \frac{1}{r!}\sum_{j=0}^{r}(-1)^j\binom{r}{j}(r-j)^n$$

Which is quite obvious, since we can take an r-partition and order the r-blocks in $r!$ different ways to get surjections into $[1, r]$.

It is the work of a moment to extend these to get the total number of surjections from $[1, n]$ and setpartitions of $[1, n]$

$$\mathcal{R} = \cup_r \mathcal{R}^{(r)} \qquad \mathcal{S} = \cup_r \mathcal{S}^{(r)}$$
$$\mathcal{R} = \textsc{Seq}(\textsc{Set}_{\geq 1}(\mathcal{Z})) \qquad \mathcal{S} = \textsc{Set}(\textsc{Set}_{\geq 1}(\mathcal{Z}))$$
$$R(z) = \frac{1}{2 - e^z} = 1 + z + 3\frac{z^2}{2!} + 13\frac{z^3}{3!} + \dots$$
$$S(z) = e^{e^z - 1} = 1 + z + 2\frac{z^2}{2!} + 5\frac{z^3}{3!} + \dots$$

The numbers R_n are called surjection numbers while the S_n are called Bell numbers.

One can then quite easily compute the egfs of set partitions with any / odd / even number of blocks of any / odd / even sizes, by making suitable restrictions of the set / sequence operators in the constructions. In fact, quite generally we have

Lemma. *The class $\mathcal{R}^{(A,B)}$ of surjections in which the cardinalities of the premiages lie in $A \subseteq \mathbb{N}$ and the cardinality of the range lies in $B \subseteq \mathbb{N}$ is given by*

$$R^{(A,B)}(z) = \beta(\alpha(z))$$
$$\alpha(z) = \sum_{a \in A} \frac{z^a}{a!} \qquad \beta(z) = \sum_{b \in B} z^b$$

The class $\mathcal{S}^{(A,B)}$ of set partitions with block sizes in $A \subseteq \mathbb{N}$ and number of blocks in in $B \subseteq \mathbb{N}$ is given by

$$S^{(A,B)}(z) = \beta(\alpha(z))$$
$$\alpha(z) = \sum_{a \in A} \frac{z^a}{a!} \qquad \beta(z) = \sum_{b \in B} \frac{z^b}{b}!$$

4.3 Set partitions as an unlabelled class

Now, we can also consider set partitions using an unlabelled class. This shows that we need to keep an open mind when deciding these properties. We encode set partitions as a family of words! Let $\mathcal{S}_n^{(r)}$ denote the set partitions of an n-set into r-blocks, so that $\left\{ {n \atop r} \right\} = \text{card}(\mathcal{S}_n^{(r)})$.

We can encode any such set partition as a word on $\mathcal{B} = \{b_1, \dots, b_r\}$. In particular take each block and sort its elements smallest to largest. Then order the blocks according to the smallest element in each block. Label everything in the first block by b_1, the second block by b_2 etc etc. Eg

$$\begin{aligned} \{1, 2, \dots, 9\} &= \{6, 4\} + \{5, 1, 2\} + \{3, 8, 7\} \\ &= \underbrace{\{1, 2, 5\}}_{b_1} + \underbrace{\{3, 7, 8\}}_{b_2} + \underbrace{\{4, 6\}}_{b_3} \end{aligned}$$

Then simply read off the label of each number in order

$$\equiv [b_1, b_1, b_2, b_3, b_1, b_3, b_2, b_2]$$

Now this is not just any word in the letters b_i there are some extra conditions

- all r letters must occur
- the first occurrance of b_1 is before that of b_2 which is before the first occurrance of b_3 etc etc.

So this means that our word looks like

- a sequence of at least 1 b_1, then
- a b_2 then a sequence of $\{b_1, b_2\}$, then
- a b_3 then a sequence of $\{b_1, b_2, b_3\}$, then etc etc

This gives

$$b_1\textsc{Seq}(b_1)b_2\textsc{Seq}(b_1+b_2)b_3\textsc{Seq}(b_1+b_2+b_3)\ldots b_r\textsc{Seq}(b_1+\cdots+b_r)$$

Hence the **o**gf is

$$S^{(r)}(z) = \frac{z^r}{(1-z)(1-2z)\ldots(1-rz)}$$

Which we can re-write using partial fraction decomposition, or other methods as:

$$S(z) = \frac{1}{r!}\sum_{j=1}^{r}\binom{r}{j}\frac{(-1)^{r-j}}{1-jz}$$

and so

$$\left\{ {n \atop r} \right\} = \frac{1}{r!}\sum_{j=1}^{r}(-1)^{r-j}\binom{r}{j}j^n,$$

as before.

4.4 Wrapping up surjections and set partitions

Proposition. *The class $\mathcal{R}^{(A,B)}$ of surjections in which the cardinalities of the premiages lie in $A \subseteq \mathbb{N}$ and the cardinality of the range lies in $B \subseteq \mathbb{N}$ is given by*

$$R^{(A,B)}(z) = \beta(\alpha(z))$$

$$\alpha(z) = \sum_{a\in A}\frac{z^a}{a!} \qquad \beta(z) = \sum_{b\in B} z^b$$

Proposition. *The class $\mathcal{S}^{(A,B)}$ of set partitions with block sizes in $A \subseteq \mathbb{N}$ and number of blocks in in $B \subseteq \mathbb{N}$ is given by*

$$S^{(A,B)}(z) = \beta(\alpha(z))$$

$$\alpha(z) = \sum_{a\in A}\frac{z^a}{a!} \qquad \beta(z) = \sum_{b\in B}\frac{z^b}{b}!$$

5 Permutations

We just looked at sequences and sets of sets. We could do the same for cycles. Sequences of cycles are called alignments, but do not appear that frequently. Let us instead consider sets of cycles, also known as permutations:

$$\mathcal{P} = \textsc{Set}(\textsc{Cyc}(\mathcal{Z}))$$

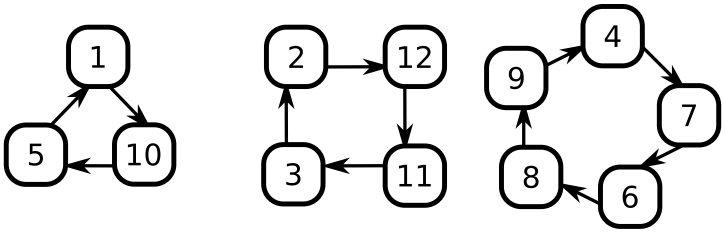
As suggested by this formula, every cycle can be naturally decomposed into a set of cycles. Consider the permutation

$$\sigma = (10, 12, 2, 7, 1, 8, 6, 9, 4, 5, 3, 11)$$

Let us track where 1 moves under the action of this permutation

$$\begin{aligned} 1 \to 10 \to 5 \to 1 \\ 2 \to 12 \to 11 \to 3 \to 2 \\ 4 \to 7 \to 6 \to 8 \to 9 \to 4 \end{aligned}$$

So the above decomposes into 3 cycles of lengths 3,4,5; its cycle number is 3. Schematically this gives



Using this decomposition as a set of cycles we get

$$\mathcal{P} \cong \textsc{Set}(\textsc{Cyc}(\mathcal{Z})) \cong \textsc{Seq}(\mathcal{Z})$$
$$P(z) = \exp\left(\log\frac{1}{1-z}\right) = \frac{1}{1-z}$$

The fact that $\exp$ and $\log$ are inverses is reflected in cycle-decomposition of permutations.

Now we can go further by playing with restrictions (as we did above) to get

Proposition. *The class $\mathcal{P}^{(A,B)}$ of permutations with cycle lengths in $A \subseteq \mathbb{N}$ and cycle number in $B \subseteq \mathbb{N}$ is given by*

$$P^{(A,B)}(z) = \beta(\alpha(z))$$
$$\alpha(z) = \sum_{a\in A}\frac{z^a}{a} \qquad \beta(z) = \sum_{b\in B}\frac{z^b}{b!}$$

5.1 Sub-classes of permutations

5.1.1 Involutions

The permutation σ is an involution if $\sigma\circ\sigma$ = identity. This means that all cycles are length 1 or 2, but the number of cycles is unconstrained. In the language of the above theorem, $A = \{1,2\}$ and $B = \{0,1,2,\dots\}$. Hence

$$\begin{aligned}
\mathcal{I} &= \textsc{Set}(\textsc{Cyc}_{1,2}(\mathcal{Z}))\\
I(z) &= \exp\left(z + z^2/2\right)\\
&= \sum_{k\geq 0}\frac{z^k}{k!}(1+z/2)^k = \sum_{k\geq 0}\sum_{j=0}^{k}\binom{k}{j}\frac{z^{j+k}}{2^j k!}\\
&= \sum_{n\geq 0}\sum_{j=0}^{n/2}\binom{n-j}{j}\frac{1}{2^j(n-j)!}z^n\\
I_n &= \sum_{j=0}^{n/2}\frac{n!}{2^j(n-2j)!j!}
\end{aligned}$$

One can of course extend this to consider permutations in which all cycles are of length $\leq r$.

5.1.2 Derangements

In the opposite direction, a derangement is a permutation in which no number stays put — hence all cycles must be 2 or longer. In the language of the above theorem, $A = \{2,3,4,5,\dots\}$ and $B =$

$\{0, 1, 2, \dots\}$.

$$\begin{aligned}
\mathcal{D} &= \textsc{Set}(\textsc{Cyc}_{>1}(\mathcal{Z})) \\
D(z) &= \exp\left(\log\frac{1}{1-z} - z\right) = \frac{e^{-z}}{1-z} \qquad = \sum_{n\geq 0}(-1)^n\frac{z^n}{n!} \times \sum_{n\geq 0} z^n \\
D_n &= n!\left(1 - \frac{1}{1!} + \frac{2}{2!} - \cdots + \frac{(-1)^n}{n!}\right)
\end{aligned}$$

Hence $D_n/n!$ = probability that a permutation leaves nothing in place, is the truncation of the expansion of e^{-1}. Since this converges very quickly, the probability of a permutation being a derangment is asymptotically $1/e \approx 0.37$.

So — if you require all cycles to be length $> r$ or longer one gets

$$\begin{aligned}
\mathcal{D}^{(r)} &= \textsc{Set}(\textsc{Cyc}_{>r}(\mathcal{Z})) \\
D^{(r)}(z) &= \exp\left(\log\frac{1}{1-z} - \sum_{k\leq r}\frac{z^k}{k}\right) = \frac{e^{-\frac{z}{1}-\frac{z^2}{2!}-\cdots-\frac{z^r}{r!}}}{1-z}
\end{aligned}$$

5.1.3 Other variants

This approach will work well to consider other classes of permutations such as permutations with all even cycles, all odd cycles, cycles of even length, all of odd length etc. It is also not hard to get all permutations so that σ^d = identity for a given d. Give these a shot.

5.2 The number of cycles in a permutation

Let $P^{(r)}$ be the class of permutations that decompose into r cycles. The number $P_n^{(r)} \equiv \left[{n \atop r}\right]$ are the Stirling cycle numbers (or Stirling numbers of the first kind), and their egf is

$$\begin{aligned}
P^{(r)} &= \textsc{Set}_r(\textsc{Cyc}(\mathcal{Z})) \\
P^{(r)}(z) &= \frac{1}{r!}\left(\log\frac{1}{1-z}\right)^r
\end{aligned}$$

So — the probability that a permutation has exactly r cycles is $\left[{n \atop r}\right]\frac{1}{n!}$.

What do these numbers look like? Let $p_{n,k}$ be this probability, and consider $n = 100$.

k	1	2	3	4	5	6	7	8	9	10
$p_{n,k}$	.01	.05	.12	.19	.21	.17	.11	.06	.03	.01

How do we interpret this? A random permutation of 100 has on average a few more than 5 cycles. It rarely has more than 10. What does this imply about the average *length* of a cycle?

5.3 Application: 100 Prisoners

This example is a reformulation of an applied problem on probing and hashing. The wording is modified from the wikipedia page on Random permutation statistics.

5.3.1 The game

A prison warden wants to make room in his prison and is considering liberating one hundred prisoners, thereby freeing one hundred cells. He assembles one hundred prisoners and asks them to play the following game:

1. he lines up one hundred urns in a row, each containing the name of one prisoner, where every prisoner's name occurs exactly once;
2. every prisoner is allowed to look inside *fifty* urns. If he or she **does not** find his or her name in one of the fifty urns, all prisoners will immediately be executed, otherwise the game continues.

The prisoners have a few moments to decide on a strategy, knowing that once the game has begun, they will not be able to communicate with each other, mark the urns in any way or move the urns or the names inside them. Choosing urns at random, their chances of survival are almost zero, but there is a strategy giving them a 30% chance of survival, assuming that the names are assigned to urns randomly what is it?

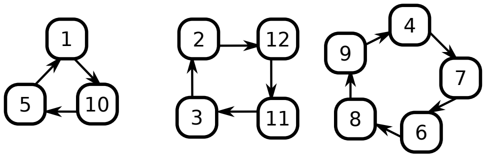
First of all, the survival probability using random choices is $\left(\frac{\binom{99}{49}}{\binom{100}{50}}\right)^{100} = \frac{1}{2^{100}}$ so this is definitely not a practical strategy.

5.3.2 The strategy

The 30% survival strategy is to consider the contents of the urns to be a permutation of the prisoners, and traverse cycles. To keep the notation simple, assign a number to each prisoner, for example by sorting their names alphabetically. The urns may thereafter be considered to contain numbers rather than names. Now clearly the contents of the urns define a permutation. The first prisoner opens the first urn. If he finds his name, he has finished and survives. Otherwise he opens the urn with the number he found in the first urn. The process repeats: the prisoner opens an urn and survives if he finds his name, otherwise he opens the urn with the number just retrieved, up to a limit of fifty urns. The second prisoner starts with urn number two, the third with urn number three, and so on. This strategy is precisely equivalent to a traversal of the cycles of the permutation represented by the urns. Every prisoner starts with the urn bearing his number and keeps on traversing his cycle up to a limit of fifty urns. The number of the urn that contains his number is the pre-image of that number under the permutation. Hence the prisoners survive if all cycles of the permutation contain at most fifty elements. We have to show that this probability is at least 30%.

Let us see how this works on a smaller example. Consider the permutation from the beginning of these notes:

BOX 1	BOX 2	BOX 3	BOX 4	BOX 5	BOX 6	BOX 7	BOX 8	BOX 9	BOX 10	BOX 11	BOX 12
10	12	2	7	1	8	6	9	4	5	3	11



This simulates the situation where the warden has put a 10 in box 1, a 12 in box 2, a 2 in box 3 and in general $\sigma(i)$ in box i. If the prisoners are following the strategy, they will each have 6 boxes to look in to, and since the maximum cycle size is 5, they will win.

How will it go down? Prisoner one will open box 1. It will say 10. He then opens box 10, and it will say 5. He opens box 5, it says 1, and he breathes a sigh of relief. Prisoner two's turn. He opens box 2: it says 12. He continues along the cycle and the fourth box he opens will have a 2 inside. Later, prisoner 4 is up. He follows this and he starts to sweat because it takes him 5 turns, but this is still less than 6, so he is okay. We know what this permutation looks like, and that every cycle is of length less than 6, so, as we already noted, if this were the scheme, the prisoners would win.

Note that this assumes that the warden chooses the permutation randomly; if the warden anticipates this strategy, he can simply choose a permutation with a cycle of length 51. To overcome this, the prisoners may agree in advance on a random permutation of their names.

5.3.3 The analysis

First, let us consider the general problem with $2n$ prisoners choosing n urns. Let us calculate the egf that a random permutation (of any size) has a cycle of length $n+1$, and then deduce the probability for the case of permutations of length n, and these are the cases in which case this strategy will fail. Fix n and consider the class of all permutations which have a cycle of length at least $n+1$. We take a sum over all permutations σ of the term $z^{|\sigma|}$ if it has no such cycle and $z^{|\sigma|}u$ if it does

$$g^{(n)}(z,u) = \sum_{\sigma\in\mathcal{P}} \frac{z^{|\sigma|}u^{1\,(\text{if } \sigma \text{ has a cycle of length } n);0 \text{ otherwise}}}{|\sigma|!} = 1 + z + \frac{2z^2}{2!} + \cdots + n!\frac{z^n}{n!} + (n!u + nn!)\frac{z^{n+1}}{(n+1)!} + \ldots$$

We first expand the decomposition $\mathcal{P} = \textsc{Set}(\textsc{Cyc}(\mathcal{Z})) = \textsc{Set}(\textsc{Cyc}_{\leq n}(\mathcal{Z}) + \textsc{Cyc}_{>n}(\mathcal{Z}))$ which we then expand as follows:

$$\begin{aligned} g^{(n)}(z,u) &= \exp\left(\underbrace{z + \frac{z^2}{2} + \frac{z^3}{3} + \cdots + \frac{z^n}{n}}_{\textsc{Cyc}_{\leq n}(\mathcal{Z})} + \underbrace{u\frac{z^{n+1}}{n+1} + u\frac{z^{n+2}}{n+2} + \ldots}_{\textsc{Cyc}_{>n}(\mathcal{Z})}\right) \\ &= \frac{1}{1-z}\exp\left((u-1)\left(\frac{z^{n+1}}{n+1} + \frac{z^{n+2}}{n+2} + \ldots\right)\right). \end{aligned}$$

The desired probability is

$$[z^{2n}]\left([u]g^{(n)}(z,u)\right) = [z^{2n}][u]\frac{1}{1-z}\left(1 + (u-1)\left(\frac{z^{n+1}}{n+1} + \frac{z^{n+2}}{n+2} + \ldots\right)\right),$$

since $\exp(\bullet) = 1 + \bullet + \bullet^2 + \ldots$, and so once you square the argument to the $\exp$, you will only create terms which are a power of z greater than $2n$. This is equal to

$$\begin{aligned} [z^{2n}]\left([u]g^{(n)}(z,u)\right) &= [z^{2n}]\frac{1}{1-z}\left(\frac{z^{n+1}}{n+1} + \frac{z^{n+2}}{n+2} + \ldots\right) \\ &= [z^{2n}]\sum_{\ell}\left(\sum_{k=n+1}^{\ell}\frac{1}{k}\right)z^{\ell} = \sum_{k=n+1}^{2n}\frac{1}{k}. \end{aligned}$$

These are related to *Harmonic numbers* and have good estimates. Using one of these good estimates we compute that

$$[z^{2n}]\left([u]g^{(n)}(z,u)\right) < \log 2 \implies \quad 1 - [z^{2n}]\left([u]g^{(n)}(z,u)\right) > 1 - \log 2 = 0.3068528\ldots$$

That is, at least 30 %.

5.4 Computing Stirling cycle numbers

We can follow a similar analysis to get formulas for Stirling cycle numbers $\left[{n \atop r}\right]$ which we recall are the number of permutations of n that decompose into r cycles. Start with the bivariate g.f.

$$\begin{aligned} P(z,u) &= \sum_{r=0}^{\infty} P^{(r)}(z)u^r \\ &= \sum_{r=0}^{\infty}\left(u\log\frac{1}{1-z}\right)^r\frac{1}{r!} \\ &= \exp\left(u\log\frac{1}{1-z}\right) = (1-z)^{-u} \\ &= \sum_{n\geq 0}(-1)^n\binom{-u}{n}z^n \end{aligned}$$

so the coeff of z^n is an expansion in u

$$\sum_{r=0}^{n} \begin{bmatrix} n \\ r \end{bmatrix} u^r = u(u+1)(u+2)\dots(u+n-1)$$

Differentiating this and setting $u = 1$ gives

$$\frac{1}{n!}\sum r \begin{bmatrix} n \\ r \end{bmatrix} = 1 + 1/2 + 1/3 + \dots 1/n$$

This is the expected number of cycles in a permutation of length n and is approximately $\log n$.

6 Trees maps and graphs

For trees, the labelled case is not so different to the unlabelled case. We can consider planar and non-planar rooted trees.

Example. Let $\mathcal{A}$ be the class of rooted labelled planar trees whose vertex outdegrees must lie in the set Ω. Then we have

$$\mathcal{A} = \mathcal{Z}\textsc{Seq}_{\Omega}(\mathcal{A})$$

and so using similar reasoning as the unlabelled case

$$A(z) = z\phi(A(z)) \qquad\qquad \phi(u) = \sum_{\omega\in\Omega} u^{\omega}$$

and indeed this is identical to the ogf for the unlabelled version. Hence $A_n = n!\hat{A}_n$ — this is easy to prove by reading the vertices of a labelled tree in a canonical order (eg breadth first) to obtain a permutation and an unlabelled tree of the same shape. Using this idea or lagrange inversion we get that all labelled rooted planar trees are

$$A_n = n!\frac{1}{n}\binom{2n-2}{n-1} = 2^{n-1}\cdot 1\cdot 3\cdots(2n-3)$$

So — to the non-planar case

Example. Let $\mathcal{T}$ be the class of all non-planar rooted labelled trees. By deleting the root vertex one obtains a set of labelled trees. Thus

$$\mathcal{T} = \mathcal{Z}\star\textsc{Set}(\mathcal{T})$$
$$T(z) = ze^{T(z)}$$

Now $\phi(u) = e^u$ and Lagrange inversion gives

$$\begin{aligned} T_n &= n![z^n]T(z) \\ &= n!\left(\frac{1}{n}[u^{n-1}]\left(e^u\right)^n\right) \\ &= (n-1)!\frac{n^n}{n!} = n^{n-1} \end{aligned}$$

Which is a famous result due to Cayley. These are usually called Cayley trees. A k-forest of Cayley trees gives a very similar result

$$F_n^{(k)} = n![z^n]\frac{T(z)^k}{k!} = \binom{n-1}{k-1}n^{n-k}$$

Similar games with restricted vertex degree lead to

$$\mathcal{T}^{(\Omega)} = \mathcal{Z} \star \textsc{Set}_{\Omega}(\mathcal{T}^{(\Omega)})$$

$$T^{(\Omega)}(z) = z\bar{\phi}(T^{(\Omega)}(z)) \qquad \bar{\phi}(u) = \sum_{\omega\in\Omega} \frac{u^{\omega}}{|\omega|!}$$