by (3.5.2). After taking logarithms and differentiating, following (4.1.3), we find $F(1) = n!$, $(\log F)'(1) = H_n$, and

$$(\log F)''(1) = -1 - 1/4 - 1/9 - 1/16 - \cdots - 1/n^2.$$

If we substitute this into (4.1.3), we find that the variance of the distribution of cycles over permutations of n letters is

$$\begin{aligned}\sigma^2 &= H_n - 1 - 1/4 - 1/9 - \cdots - 1/n^2 \\ &= \log n + \gamma - \pi^2/6 + o(1).\end{aligned}$$

where γ is Euler's constant.

Hence the average number of cycles is $\sim \log n$ with a standard deviation $\sigma \sim \sqrt{\log n}$. ■

4.2 A generatingfunctionological view of the sieve method

The sieve method* is one of the most powerful general tools in combinatorics. It is explained in most texts in discrete mathematics, however it most often appears as a sequence of manipulations of alternating sums of binomial coefficients. Here we will emphasize the fact that generating functions can greatly simplify the lives of users of the method.

We are given a finite set Ω of objects and a set P of properties that the objects may or may not possess.** In this context, we want to answer questions of the following kind: how many objects have no properties at all? how many have exactly r properties? what is the average number of properties that objects have? etc., etc.

The characteristic flavor of problems that the sieve method can handle is that, although it is hard to see how many objects have *exactly* r properties, for instance, it is relatively easy to see how many objects have *at least* a certain set of properties and maybe more.

What the method does is to convert the 'at least' information into the 'exactly' information.

To see how this works, if $S \subseteq P$ is a set of properties, let $N(\supseteq S)$ be the number of objects that have *at least* the properties in S. That is, $N(\supseteq S)$ is the number of objects whose set of properties contains S.

For fixed $r \geq 0$, consider the sum

$$N_r = \sum_{|S|=r} N(\supseteq S). \tag{4.2.1}$$

* A.k.a. 'the principle of inclusion-exclusion,' and often abbreviated as 'p.i.e.'

** Strictly speaking, a property is just a subset of the objects, but in practice we will usually have simple verbal descriptions of the properties.

Introduce the symbol $P(\omega)$ for the set of properties that ω has. Then we can write N_r as follows:

$$\begin{aligned} N_r &= \sum_{|S|=r} N(\supseteq S) \\ &= \sum_{|S|=r} \sum_{\substack{\omega\in\Omega \\ S\subseteq P(\omega)}} 1 \\ &= \sum_{\omega\in\Omega} \left\{ \sum_{\substack{|S|=r \\ S\subseteq P(\omega)}} 1 \right\} \\ &= \sum_{\omega\in\Omega} \binom{|P(\omega)|}{r}. \end{aligned} \tag{4.2.2}$$

Therefore *every object that has exactly t properties contributes $\binom{t}{r}$ to N_r.* If there are e_t objects that have exactly t properties, then (4.2.2) simplifies to

$$N_r = \sum_{t\ge 0} \binom{t}{r} e_t \qquad (r = 0, 1, 2, \ldots). \tag{4.2.3}$$

Recall the philosophy of the method: the N_r's are easier to calculate than the e_r's because they can be found from (4.2.1). However, the e_r's are what we want. Therefore it is desirable to be able to solve the equations (4.2.3) for the e's in terms of the N's. But how can we do that? After all, (4.2.3) is a set of simultaneous equations.

At first glance that might seem to be a tall order, but with a friendly generating function at your side, it's easy. Let $N(x)$ and $E(x)$ denote* the opsgf's of the sequences $\{N_r\}$, $\{e_r\}$, respectively. What relation between the two generating functions is implied by the equations (4.2.3)?

Multiply (4.2.3) by x^r and sum on r. We then get

$$\begin{aligned} N(x) &= \sum_r \sum_t \binom{t}{r} e_t x^r \\ &= \sum_t e_t \left\{ \sum_r \binom{t}{r} x^r \right\} \\ &= \sum_t e_t (x+1)^t \\ &= E(x+1). \end{aligned} \tag{4.2.4}$$

* The letters 'N' and 'E' are intended to suggest the N_r's and the word 'Exactly.'

In the language of generating functions, the set of equations (4.2.3) boils down to the fact that $N(x) = E(x + 1)$. Now the problem of solving for the e's in terms of the N's is a triviality, and the solution is obviously

$$\boxed{E(x) = N(x - 1)} \tag{4.2.5}$$

This is the sieve method. *The act of replacing the variable x by $x - 1$ in the generating function $N(x)$ replaces the unfiltered data $\{N_r\}$ by the sieved quantities $\{e_r\}$.*

If the N's are known, then in principle we can read off the e's as the coefficients of $N(x - 1)$.

For example, e_0 is the number of objects that have no properties at all. By (4.2.5),

$$e_0 = E(0) = N(-1) = \sum_t (-1)^t N_t. \tag{4.2.6}$$

It's easy to find explicit formulas for all of the e_j's by looking at the coefficient of x^j on both sides of (4.2.5). The result is

$$e_j = \sum_t (-1)^{t-j} \binom{t}{j} N_t. \tag{4.2.7}$$

But (4.2.5) says it all, in a much cleaner fashion.

We will now summarize the sieve method, and then give a number of examples of its use.

The Sieve Method

(A) (*Find Ω and P*) Given an enumeration problem, find a set of objects and properties such that the problem would be solved if we knew the number of objects with each number of properties.

(B) (*Find the unfiltered counts $N(\supseteq S)$*) For each set S of properties, find $N(\supseteq S)$, the number of objects whose set of properties contains S.

(C) (*Find the coefficients N_r*) For each $r \geq 0$, calculate the N_r by summing the $N(\supseteq S)$ over all sets S of r properties, as in (4.2.1).

(D) (*The answer is here.*) The numbers e_r are the coefficients of the powers of x in the polynomial $N(x - 1)$. ∎

Before we get to some examples, we would like to point out that the number N_1 has a special role to play. According to (4.2.3), $N_1 = \sum_t te_t$. That, however, is what you would want to know if you were trying to calculate the average number of properties that objects have. Hence it is good to remember that *when using the sieve method on a set of N objects, the average number of properties that an object has is N_1/N.*

Example 1. The fixed points of permutations.

Of the $n!$ permutations of n letters, how many have exactly r fixed points?

Step (A) of the sieve method asks us to say what the set of objects is and what the set of properties is. It is almost always worthwhile to be quite explicit about these. In the case at hand, the set Ω of objects is the set of all permutations of n letters. There are n properties: for each $i = 1, \ldots, n$, a permutation τ has property i if i is a fixed point of τ, i.e., if $\tau(i) = i$.

With those definitions of Ω and P, it is indeed true that we would like to know the numbers of objects that have exactly r properties, for each r.

In step (B) we must find the $N(\supseteq S)$. Hence let S be a set of properties. Then $S \subseteq [n]$ is a set of letters, and we want to know the number of permutations of n letters that leave *at least* the letters in S fixed.

If a permutation leaves the letters in S fixed, then it can act freely on only the remaining $n - |S|$ letters, and so there are $(n - |S|)!$ such permutations. Hence

$$N(\supseteq S) = (n - |S|)!.$$

For step (C) we calculate the N_r's. But, for each $r = 0, \ldots, n$,

$$N_r = \sum_{|S|=r} N(\supseteq S) = \sum_{|S|=r} (n - |S|)! = \binom{n}{r}(n-r)! = \frac{n!}{r!}.$$

In step (D) we're ready for the answers. It will save some writing if we introduce the abbreviation $\exp_{|\alpha}$ for the truncated exponential series

$$\exp_{|\alpha}(x) = \sum_{0 \le r \le \alpha} \frac{x^r}{r!}. \tag{4.2.8}$$

Now we form the opsgf $N(x)$ from the N_r's that we just found:

$$N(x) = \sum_{r=0}^{n} \frac{n!}{r!} x^r = n! \sum_{r=0}^{n} \frac{x^r}{r!}.$$

Then e_t is the coefficient of x^t in $N(x-1)$, i.e.,

$$E(x) = \sum_t e_t x^t = n! \sum_{r=0}^{n} \frac{(x-1)^r}{r!} = n! \exp_{|n}(x-1). \tag{4.2.9}$$

As an extra dividend, the *average* number of fixed points that permutations of n letters have is

$$\frac{N_1}{N} = \frac{n!}{n!} = 1.$$

On the average, a permutation has 1 fixed point.

The number of permutations that have no fixed points at all is

$$e_0 = E(0) = N(-1) = n! \exp_{|n}(-1) \sim \frac{n!}{e}. \tag{4.2.10}$$

Finally, if we really want a formula for the e_t's, it's quite easy to find from (4.2.9) that

$$\begin{aligned} e_t &= \frac{n!}{t!} \exp_{|(n-t)}(-1) \\ &\sim e^{-1} \frac{n!}{t!} \qquad (n \to \infty). \end{aligned} \tag{4.2.11}$$

■

Example 2. The number of k-cycles in permutations.

Fix positive integers n, k, and $r \geq 0$. How many permutations of n letters have exactly r cycles of length k?

Whatever the answer is, it should at least have the good manners to reduce to the answer of the previous example when $k = 1$, since a fixed point is a cycle of length 1.

What are the objects and the properties? Evidently Ω is the set of all permutations of n letters. Further, the set P of properties is the set of all possible k-cycles chosen from n letters. How many such k-cycles are there? The k letters can be chosen in $\binom{n}{k}$ ways, and they can be arranged around a cycle in $(k-1)!$ ways, so we are facing a list of $\binom{n}{k}(k-1)!$ properties.

Choose a set S of k-cycles from P. How many permutations have at least the set S of properties? None at all, unless the sets of letters in those cycles are pairwise disjoint. If the sets are pairwise disjoint, then there are $N(\supseteq S) = (n - k|S|)!$ permutations that have at least all of those k-cycles.

Next we calculate N_r, the sum of $N(\supseteq S)$ over all sets of r properties. The terms in this sum are either 0 or $(n - kr)!$. So we really need to know only how many of them are not 0, that is, in how many ways we can choose a set of r k-cycles from n letters in such a way that the cycles operate on disjoint sets of letters.

The letters for the first cycle can be chosen in $\binom{n}{k}$ ways, and they can be ordered around the cycle in $(k-1)!$ ways. The letters for the second cycle can then be chosen in $\binom{n-k}{k}$ ways, and ordered in $(k-1)!$ ways, etc. Finally, since the sequence in which the cycles are constructed is of no significance, we divide by $r!$. Hence

$$\begin{aligned} N_r &= \frac{(n-kr)!}{r!} \frac{n!(k-1)!^r}{(k!)^r(n-kr)!} \\ &= \frac{n!}{k^r r!} \qquad (0 \leq r \leq n/k). \end{aligned} \tag{4.2.12}$$

We can get a little piece of the solution right here, with no more work: the *average* number of k-cycles that permutations of n letters have is $N_1/n! = 1/k$.

The opsgf of $\{N_r\}$ is

$$\begin{aligned} N(x) &= n! \sum_{0 \le r \le n/k} \frac{x^r}{k^r r!} \\ &= n! \exp_{|(n/k)}(\frac{x}{k}). \end{aligned} \tag{4.2.13}$$

Finally, in the sieving step, we convert this to exact information by replacing x by $x-1$, to obtain

$$E(x) = n! \exp_{|(n/k)} \left(\frac{x-1}{k} \right). \tag{4.2.14}$$

Example 3. Stirling numbers of the second kind.

The Stirling numbers $\left\{ {n \atop k} \right\}$, which we studied in section 1.6, are the numbers of partitions of a set of n elements into k classes. We can find out about them with the sieve method if we can invent a suitable collection of objects and properties. For the set Ω of objects we take the collection of all k^n ways of arranging n labeled balls in k labeled boxes. Further, such an arrangement will have property P_i if box i is empty ($i = 1, \ldots, k$). Then $k! \left\{ {n \atop k} \right\}$ is the number of objects that have exactly no properties.

Let S be some set of properties. How many arrangements of balls in boxes have at least the set S of properties? If $N(\supseteq S)$ is that number, then $N(\supseteq S)$ counts the arrangements of n labeled balls into just $k - |S|$ labeled boxes, because all of the boxes that are labeled by S must be empty.

There are obviously $(k - |S|)^n$ such arrangements. Hence

$$N(\supseteq S) = \begin{cases} (k-|S|)^n & \text{if } |S| \le k, \\ 0, & \text{else.} \end{cases}$$

If we now sum over all sets S of r properties, we obtain for $r \le k$,

$$N_r = \binom{k}{r} (k-r)^n,$$

whose opsgf is

$$N(x) = \sum_{0 \le r \le k} \binom{k}{r} (k-r)^n x^r.$$

We can now invoke the sieve to find that the number of arrangements that have exactly t empty cells is the coefficient of x^t in $N(x-1)$. On the other hand, the number of arrangements that have exactly t empty cells is clearly

$$\binom{k}{t}(k-t)!\left\{ {n \atop k-t} \right\} = \frac{k!}{t!}\left\{ {n \atop k-t} \right\}.$$

The result is the identity

$$\sum_{0\le r\le k} \binom{k}{r}(k-r)^n(x-1)^r = k!\sum_{0\le t\le k} \left\{ {n \atop k-t} \right\}\frac{x^t}{t!}. \tag{4.2.15}$$

If we put $x = 0$, we find the explicit formula (1.6.7) again.

If, on the other hand, we compare (4.2.15) with the rule (2.3.3) for finding the coefficients of the product of two egf's, we discover the following remarkable identity:

$$\sum_{1\le k\le n} \left\{ {n \atop k} \right\} y^k = e^{-y}\sum_{r\ge 1} \frac{r^n}{r!}y^r. \tag{4.2.16}$$

This shows that e^{-y} times the infinite series is a polynomial! The special case $y = 1$ has been previously noted in (1.6.10).

Example 4. Rooks on chessboards

For n fixed, a *chessboard* C is a subset of $[n] \times [n]$. We are given C, and we define a sequence $\{r_k\}$ as follows: r_k is the number of ways we can place k nonattacking (i.e., no two in the same row or column) rooks on C.

Next, let σ be a permutation of n letters. For each j we let e_j denote the number of permutations that 'meet the chessboard C in exactly j squares,' i.e., if the event $(i, \sigma(i)) \in C$ occurs for exactly j values of i, $1 \le i \le n$.

The question is, how can we find the e_j's in terms of the r_k's?

Let the objects Ω be the $n!$ permutations of $[n]$. There will be a property $P(s)$ corresponding to each square $s \in C$. A permutation σ has property $P(s)$ if σ meets the mini-chessboard that consists of the single cell s.

Let S be a set of properties, i.e., of cells in C, and consider the sum $N_k = \sum_{|S|=k} N(\supseteq S)$. Each arrangement of k nonattacking rooks on C contributes $(n-k)!$ to this sum. Indeed, when the set S corresponds to the cells on which those rooks can be placed, then we are looking at k of the n values of a permutation that hits C in at least k squares. The permutation can be completed, in the remaining $n-k$ rows, in $(n-k)!$ ways.

Hence $N_k = r_k(n-k)!$, for each k, $0 \le k \le n$. Therefore

$$N(x) = \sum_k (n-k)!r_k x^k,$$

and immediately we find that the number of n-permutations that hit C in exactly j cells is

$$[x^j]\sum_k (n-k)!r_k(x-1)^k. \tag{4.2.17}$$

Example 5. A problem on subsets.

This example is more cute than profound, but we will at least finish with a combinatorial proof of an interesting identity, as well as illustrating the generating function aspect of the sieve method.

For a fixed positive n, take as our set Ω of objects the $\binom{2n}{n}$ ways of choosing an n-subset of $[2n]$. For the set P of properties we take the following list of n (not $2n$) properties: an n-subset Q has property i if $i \notin Q$, for each $i = 1, 2, \ldots, n$ (note that we are working with only the first half of the possible elements of S).

If S is a set of properties (i.e., is a set of letters chosen from $[n]$), then the number of ‘objects’ Q that have at least that set of properties (i.e., are missing at least all of the $i \in S$) is clearly

$$N(\supseteq S) = \binom{2n - |S|}{n}.$$

Hence

$$N_r = \sum_{|S|=r} N(\supseteq S) = \binom{n}{r}\binom{2n-r}{n}.$$

If we substitute these N's into the sieve (4.2.5) we find that

$$\sum_j e_j t^j = \sum_r \binom{n}{r}\binom{2n-r}{n}(t-1)^r. \tag{4.2.18}$$

This formula tells us the number e_j of objects that have *exactly* j properties, for each j.

But we didn't need to be told that!

An object that has exactly j of these properties is a subset Q of $[2n]$ that is missing exactly j of the elements $1, 2, \ldots, n$. Obviously there are just $\binom{n}{j}^2$ such subsets Q, because we can choose the j elements that they are missing in $\binom{n}{j}$ ways, and we can then choose the other j elements that are needed to fill the subset from $n+1, \ldots, 2n$ in $\binom{n}{j}$ ways also.

Thus, with no assistance from the sieve method, we already knew that $e_j = \binom{n}{j}^2$, for all j. Hence, according to (4.2.18), it must be true that

$$\sum_j \binom{n}{j}^2 t^j = \sum_r \binom{n}{r}\binom{2n-r}{n}(t-1)^r. \tag{4.2.19}$$

We therefore have an odd kind of a combinatorial proof of the identity (4.2.19). The reader should suspect that something of this sort is going on whenever an identity involves an expansion around the origin on one side, and an expansion around $t = 1$ on the other side.