

Lecture 4: Sieves

*Week 1 of 1**Mathcamp 2010*

In previous lectures, we would often illustrate a generating-function method by opening with an example, and then discussing how it can generalize. This is often a productive way to build intuition; however, sometimes it's clearer to begin in full generality and then illustrate what we're doing by actually tackling a problem or two. Today is such a day!

Specifically, the motivating question for today's lecture on the sieve method is the following:

Question 1 *Consider the following objects:*

- Ω , some finite set of objects,
- P , some collection of properties that the elements of Ω may or may not have, and
- $f : \Omega \rightarrow \mathcal{P}(P)$, a function that sends any $x \in \Omega$ to the subset of P corresponding to the properties it has.

For a given r , how many objects in Ω have precisely r properties? What is the average number of properties possessed by a given element?

If the above notation is confusing, consider the following very basic example:

Example. Let

- $\Omega = \{1, 2, 3, 4\}$,
- $P = \{\text{odd, prime}\}$, and
- $f(1) = \{\text{odd}\}$, $f(2) = \{\text{prime}\}$, $f(3) = \{\text{odd, prime}\}$, and $f(4) = \emptyset$.

. In this situation, our above question is trivial to answer: there is one element with no properties, two with one property, one with two properties, and the average number of properties possessed is 1.

So: for many quantities, it can be much easier to count how many objects have at **least** r properties rather than counting how many objects have precisely r properties. To illustrate this point, consider the following example:

Example. (Stirling numbers of the second kind) For fixed n, k , let

- $\Omega =$ the collection of all k^n ways of putting n labeled balls into k labeled boxes, and
- $P = \{P_1, \dots, P_k\}$, where P_i is the property that the i -th box is empty.

From this definition, we have that the number of elements that don't satisfy any properties is just

$$k! \binom{n}{k},$$

as failing to satisfy any of the P_i means that we've put a ball into every box (i.e. created a nontrivial partition of $\{1, \dots, n\}$, and the $k!$ comes from us now caring about how the boxes are labeled.

This, as we saw on class Tuesday, is nontrivial to find! However, for a fixed $S \subset P$, the number of elements of Ω that satisfy at least S is just $(k - |S|)^n$, which is completely trivial!

How can we use this to our advantage? In other words, how can we turn knowledge about the amount of objects possessing at least r properties into knowledge about objects possessing exactly r properties? Generating functions!

Specifically, for some fixed Ω, P, f , we do the following: Let $N(S)$ be the number of elements in Ω that satisfy all of the properties in S , and let

$$N_r = \sum_{S \subset P: |S|=r} N(S).$$

Then, we have that

$$\begin{aligned} N_r &= \sum_{S \subset P: |S|=r} N(S) \\ &= \sum_{S \subset P: |S|=r} \left(\sum_{x \in \Omega: S \subset f(x)} 1 \right) \\ &= \sum_{x \in \Omega} \left(\sum_{S \subset P: |S|=r, S \subset f(x)} 1 \right) \\ &= \sum_{x \in \Omega} \binom{|f(x)|}{r} \end{aligned}$$

This implies that every object with exactly t properties contributes $\binom{t}{r}$ to N_r . So, if we let e_t denote the coll. of objects with exactly t properties, we have that

$$N_r = \sum_{t=0}^{\infty} \binom{t}{r} e_t$$

So: let $N(x)$ be the generating function for the N_r 's, and $E(x)$ be the generating function

for the e_t 's. Then, we have the following (stunning!) identity:

$$\begin{aligned}
 N(x) &= \sum_{r=0}^{\infty} N_r x^r \\
 &= \sum_{r=0}^{\infty} \left(\sum_{t=0}^{\infty} \binom{t}{r} e_t x^r \right) \\
 &= \sum_{t=0}^{\infty} e_t \cdot \left(\sum_{r=0}^{\infty} \binom{t}{r} x^r \right) \\
 &= \sum_{t=0}^{\infty} e_t (1+x)^t \\
 &= E(x+1).
 \end{aligned}$$

So: via the toolset given to us by generating functions, we can convert back and forth between “exact” counting and “at-least” counting with absolutely no effort!

Specifically, this method – the method of “sieves” – gives us the following pair of remarkably useful answers to our earlier questions:

1. Because $E(x) = N(x-1)$, we have that e_t is just the coefficient of x^t in $N(x-1)$; i.e

$$\begin{aligned}
 e_t &= [x^t] \sum_{r=0}^{\infty} N_r (x-1)^r \\
 &= \sum_{r=0}^{\infty} N_r \cdot [x^t] (x-1)^r \\
 &= \sum_{r=0}^{\infty} (-1)^{r-t} \binom{r}{t} N_r.
 \end{aligned}$$

So we can switch from the e_t 's and N_r 's with no difficulty whatsoever.

2. By our earlier work,

$$\begin{aligned}
 N_r &= \sum_{t=0}^{\infty} \binom{t}{r} e_t \\
 \Rightarrow N_1 &= \sum_{t=0}^{\infty} t \cdot e_t \\
 \Rightarrow \frac{N_1}{\Omega} &= \text{the average number of properties possessed by an elt. of } \Omega.
 \end{aligned}$$

So: to illustrate the power of what we've just done, we do an example below:

Example. Of the $n!$ permutations of $\{1, \dots, n\}$, how many have no fixed points¹?
 What is the expected number of fixed points for a random permutation?

¹We say that k is a fixed point of a permutation π iff $\pi(k) = k$

Solution. So: in our language of sets and properties, let

- Ω = the collection of all $n!$ permutations, and
- $P = \{P_1, \dots, P_n\}$, where P_i is the property that i is a fixed point.

Then, for any $S \subset P$, the number of permutations satisfying S , $N(S)$, is just the number of permutations on points not fixed by S : i.e. $(n - |S|)!$.

Consequently, we have that

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

if $r \leq n$, and 0 otherwise. Thus, we have

$$\begin{aligned} N(x) &= \sum_{r=0}^n \frac{n!}{r!} x^r = n! \cdot \sum_{r=0}^n \frac{x^r}{r!} \\ \Rightarrow E(x) &= N(x - 1) = n! \cdot \sum_{r=0}^n \frac{(x - 1)^r}{r!} \\ \Rightarrow e_0 &= E(0) = N(-1) = n! \cdot \sum_{r=0}^n \frac{(-1)^r}{r!} \\ \Rightarrow e_0 &\approx \frac{n!}{e}. \end{aligned}$$

So, the expected number of fixed points is just $N_1/n! = n!/n! = 1$, and the number of permutations with no fixed points is approximately $\frac{n!}{e}$.