Math 116 Professor: Padraic Bartlett

# Lecture 2: Generating Functions

*Weeks 2-3* *UCSB 2015*

This week's notes are on **generating functions**, a new way to count objects! We start with the basics here:

## 1 Generating Functions

If you've taken Calculus BC or an equivalent class in high school, you've probably ran into **power series** before. In case you haven't, here's a quick definition:

**Definition.** Suppose we have a sequence $\{a_n\}_{n=0}^{\infty} = (a_0, a_1, a_2, \ldots)$ of numbers. We can form the **formal power series** associated to this sequence as follows:

$$A(x) = \sum_{n=0}^{\infty} a_n x^n.$$

By a formal power series, we simply mean that we are considering this object above not as something that is a function of $x$, but rather as a collection of convenient placeholders to index our values $a_1, a_2, a_3, \ldots$ with. In other words, we're usually not going to worry about "plugging in values for $x$;" instead, we're going to take this object and just pretend that all of the $x^i$'s are placeholders that allow us to tell $a_1$ and $a_2$ and $a_3$ and so on apart.

Given a formal power series, we can manipulate it in various ways! For example, we can scale it by a number:

$$c \cdot A(x) = \sum_{n=0}^{\infty} c \cdot a_n x^n.$$

We can add two formal power series:

$$A(x) = \sum_{n=0}^{\infty} a_n x^n, B(x) = \sum_{n=0}^{\infty} b_n x^n$$
$$\Rightarrow \quad A(x) + B(x) = \sum_{n=0}^{\infty} (a_n + b_n) x^n.$$

We can define a formal notion of "derivative," where we replace each $x^n$ with $nx^{n-1}$:

$$\frac{d}{dx} A(x) = \sum_{n=1}^{\infty} a_n \cdot n x^{n-1} = \sum_{n=0}^{\infty} (n+1) a_{n+1} x^n.$$

We can also take the product of two formal power series! This is a little more involved: to calculate the power series that is equal to

$$\left(\sum_{n=0}^{\infty} a_n x^n\right) \cdot \left(\sum_{n=0}^{\infty} b_n x^n\right),$$

we basically need to do the same process that we used to FOIL polynomials when we were younger! In other words, we need to take every term on the left, and multiply each one of those by every term on the right. Because there are infinitely many, this might seem awful to write down; so, to help, let's try to restrict ourselves to a somewhat easier problem. Suppose we want to calculate our product, but we are just trying to figure out how many $x^m$'s we get on the right-hand side, for some fixed value $m$. How does this work?

Well: let's go through the product $(\sum_{n=0}^{\infty} a_n x^n) \cdot (\sum_{n=0}^{\infty} b_n x^n)$ term-by-term. If we just look at the $a_0 x^0$ term from the left part, we can see that we'll have to multiply this by the $b_m x^m$ term from the right part to get a $x^m$. Similarly, if we look at $a_1 x^1$, we'll need to multiply this by $b_{m-1} x^{m-1}$ from the right to get to $x^m$; in general, if we're looking at the $a_k x^k$ term on the left, we need to multiply it by $b_{m-k} x^{m-k}$ to have the result be a multiple of $x^m$.

Therefore, if we're trying to find **all** of the $x^m$'s, we're actually just calculating the sum

$$\left(\sum_{k=0}^{m} a_k b_{m-k}\right) x^m.$$

But if we know the coefficients of each $x^m$ for every $m$, that gives us all of the terms in our product! In other words, we've shown the following:

$$\left(\sum_{n=0}^{\infty} a_n x^n\right) \cdot \left(\sum_{n=0}^{\infty} b_n x^n\right) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k}\right) x^n$$

So we can multiply power series as well!

In general, we say that two formal power series are equal if and only if each term is equal: i.e. $(\sum_{n=0}^{\infty} a_n x^n) = (\sum_{n=0}^{\infty} b_n x^n)$ if and only if $a_n = b_n$ for all $n$.

So: if you've seen power series before, you may remember that most of the times where they come up, they've been objects where you've used your knowledge about how **sequences** work to study them! In other words, your proofs have probably looked like the following:

$$\left(\text{knowledge of } \{a_n\}_{n=1}^{\infty}\right) \Rightarrow \left(\text{knowledge of } \sum_{n=1}^{\infty} a_n x^n\right).$$

We typically do this in calculus classes because, usually, we understand sequences *better* than we understood power series. However, this is not necessarily true! Given enough time in calculus/analysis classes, you will develop a lot of intuition for power series and Taylor series. Given this, it is perhaps natural to ask if we can **reverse** the method described above. In other words: suppose that we have a sequence that we want to study. What if we turned it into a power series, and used our knowledge of how that power series works to answer questions about the original series? I.e. can we make proofs that look like

$$\left(\text{knowledge of } \sum_{n=1}^{\infty} a_n x^n\right) \Rightarrow \left(\text{knowledge of } \{a_n\}_{n=1}^{\infty}\right)?$$

The answer to this question is a resounding **yes**! In mathematics, this process is called the method of **generating functions**. This works as follows:

- Take some sequence $\{a_n\}_{n=1}^{\infty}$ that you want to study.
- Look at the associated power series $\sum_{n=1}^{\infty} a_n x^n$.
- Find a nice closed form (i.e. like $\sum_{n=0}^{\infty} x^n = \frac{1}{1-x}$) for this power series, using algebra/our operations on power series / clever identities from calculus /etc.
- Use this closed form somehow to regain information about your original sequence. I.e. your closed form may have a different expansion that you can figure out, via Taylor series: therefore, because power series are unique, you know that the terms in this different expansion have to be equal to the terms $\sum_{n=1}^{\infty} a_n x^n$ in your original expansion! In other words, you've found new information about your sequence $\{a_n\}_{n=1}^{\infty}$!

We illustrate this with an object we studied last week:

### 1.1 Fibonacci numbers.

**Definition.** The **Fibonacci sequence** is the following sequence of numbers, defined as follows:

- Base cases: $f_0 = 0$ and $f_1 = 1$.
- Recursive definition: for any $n \geq 2$, we define $f_n = f_{n-1} + f_{n-2}$.

So, for example, the first nine entries of the Fibonacci sequence are the following:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$$

We let $f_n$, the $n$-th Fibonacci number, be the $n$-th element of this sequence.

As defined, it is reasonably difficult to calculate these numbers. I.e. to find $f_{1000}$, we need to find the Fibonacci numbers $f_{999}, f_{998}$, for which we also need the Fibonacci number $f_{997}$, for which we need the next Fibonacci number $f_{996}$... all the way down to $f_1, f_0$. In other words, we have to find **all** of the Fibonacci numbers from 1 to 999 to find $f_{1000}$.

This seems... wasteful! I.e. if all we care about is $f_{1000}$, it seems somewhat silly to have to calculate every number along the way to get to $f_{1000}$. This is certainly not how we work with other arithmetical operations; that is, to calculate $1000 \cdot x$, we don't need to calculate $n \cdot x$ for every value of $n$ between 1 and 999 first!

Therefore, a natural question to ask here is the following: can we find a **closed form** for these numbers $f_n$? In other words, can we a way of calculating $f_n$ without having to find $f_{n-1}$ and $f_{n-2}$?

**Answer:** Yes! Specifically, we can do this with **generating functions**!

To start, let's look at the power series

$$\sum_{n=0}^{\infty} f_n x^n.$$

The only thing we know about the constants $f_n$, at first, is their recurrence relation $f_n = f_{n-1} + f_{n-2}$. So: let's plug that in to our power series! Specifically, let's plug that into all of the terms $f_n$ with $n \geq 2$, as those are the terms where this recurrence relation holds:

$$\begin{aligned}
\sum_{n=0}^{\infty} f_n x^n &= f_0 \cdot x^0 + f_1 \cdot x^1 + \sum_{n=2}^{\infty} f_n x^n \\
&= 0 + x + \sum_{n=2}^{\infty} (f_{n-1} + f_{n-2}) x^n \\
&= x + \sum_{n=2}^{\infty} f_{n-1} x^n + \sum_{n=2}^{\infty} f_{n-2} x^n \\
&= x + x \sum_{n=2}^{\infty} f_{n-1} x^{n-1} + x^2 \sum_{n=2}^{\infty} f_{n-2} x^{n-2} \\
&= x + x \sum_{n=1}^{\infty} f_n x^n + x^2 \sum_{n=0}^{\infty} f_n x^n
\end{aligned}$$

where we justfied this last step by just shifting our indices (i.e. the sum starting at 2 of $f_{n-1}x^{n-1}$ is just the sum starting at 1 of $f_n x^n$.) Finally, if we notice that because $f_0 = 0$, we have $x \sum_{n=1}^{\infty} f_n x^n = x \sum_{n=0}^{\infty} f_n x^n$, we finally have

$$\begin{aligned}
\sum_{n=0}^{\infty} f_n x^n &= x + x \sum_{n=0}^{\infty} f_n x^n + x^2 \sum_{n=0}^{\infty} f_n x^n \\
\Rightarrow \sum_{n=0}^{\infty} f_n x^n - x \sum_{n=0}^{\infty} f_n x^n - x^2 \sum_{n=0}^{\infty} f_n x^n &= x \\
\Rightarrow (1 - x - x^2) \sum_{n=0}^{\infty} f_n x^n &= x \\
\Rightarrow \sum_{n=0}^{\infty} f_n x^n &= \frac{x}{1 - x - x^2}.
\end{aligned}$$

Sweet! A closed form. So: according to our blueprint, we want to use this closed form to find information about our original series, possibly by finding another way to expand it.

To start this, we first notice that with the quadratic formula, we can see that $1-x-x^2$ has roots $-\frac{1\pm\sqrt{5}}{2}$, and therefore that we can factor $1-x-x^2$ as follows:

$$1-x-x^2 = -\left(x+\frac{1+\sqrt{5}}{2}\right)\left(x+\frac{1-\sqrt{5}}{2}\right).$$

You may recognize the fraction $\frac{1+\sqrt{5}}{2}$ as the **golden ratio** $\varphi$, a famous mathematical constant that shows up in all sorts of odd places! This has a few useful properties, especially in relation to the other root $\frac{1-\sqrt{5}}{2}$, which we list here for convenience's sake:

$$\begin{aligned}
-\frac{1}{\varphi} &= -\frac{2}{1+\sqrt{5}} = -\frac{2(1-\sqrt{5})}{(1+\sqrt{5})(1-\sqrt{5})} = -\frac{2(1-\sqrt{5})}{-4} = \frac{1-\sqrt{5}}{2},\\
1-\varphi &= 1-\frac{1+\sqrt{5}}{2} = \frac{1-\sqrt{5}}{2} = -\frac{1}{\varphi},\\
1-\varphi-\varphi^2 = 0 &\Rightarrow \varphi^2 = 1-\varphi = -\frac{1}{\varphi}
\end{aligned}$$

We use these observations to further modify our polynomial:

$$\begin{aligned}
1-x-x^2 &= -\left(x-\frac{1+\sqrt{5}}{2}\right)\left(x-\frac{1-\sqrt{5}}{2}\right)\\
&= -(x+\varphi)(x+(-1/\varphi))\\
&= -(x+\varphi)\cdot\frac{1}{\varphi}\cdot\varphi\cdot(x+(-1/\varphi))\\
&= -((1/\varphi)x+1)(\varphi x-1)
\end{aligned}$$

We can use this observation to cleverly split our expression for the Fibonacci series' power series, using the technique of **partial fractions**[1]:

$$\begin{aligned}
\frac{x}{1-x-x^2} &= \frac{x}{(1-x\varphi)\cdot(1-x(-1/\varphi))}\\
&= \frac{1}{\varphi-(-1/\varphi)}\cdot\left(\frac{1}{1-x\varphi}-\frac{1}{1-x(-1/\varphi)}\right)\\
&= \frac{1}{\sqrt{5}}\cdot\left(\frac{1}{1-x\varphi}-\frac{1}{1-x(-1/\varphi)}\right)
\end{aligned}$$

[1] If you haven't seen this before: this is just the mathematical technique where we replace a fraction of the form $\frac{1}{A(x)B(x)}$ with some clever expression $\frac{C(x)}{A(x)}+\frac{D(x)}{B(x)}$, by "undoing" the common-denominator step that occurs when we add two fractions.

To deal with these two fractions, we now notice the following power series identity: for any $y$, we have as a formal power series the equation

$$\sum_{n=0}^{\infty} y^n = \frac{1}{1-y}.$$

This is not hard to check; if we multiply the LHS by $(1-y)$, we can see that we get

$$\begin{aligned}
(1-y)\sum_{n=0}^{\infty} y^n &= \sum_{n=0}^{\infty} y^n - \sum_{n=0}^{\infty} y^{n+1} \\
&= \sum_{n=0}^{\infty} y^n - \sum_{n=1}^{\infty} y^n \\
&= 1 + \sum_{n=1}^{\infty} y^n - \sum_{n=1}^{\infty} y^n \\
&= 1. \\
\Rightarrow \qquad \sum_{n=0}^{\infty} y^n &= \frac{1}{1-y}.
\end{aligned}$$

In particular, if we let $y = \varphi x$ or $y = (-1/\varphi)x$, we get

$$\frac{1}{1-x\varphi} = \sum_{n=0}^{\infty} (x\varphi)^n, \quad \frac{1}{1-x(-1/\varphi)} = \sum_{n=0}^{\infty} (x(-1/\varphi))^n.$$

Plugging this into our work earlier gives us

$$\begin{aligned}
\frac{x}{1-x-x^2} &= \frac{1}{\sqrt{5}} \cdot \left( \sum_{n=0}^{\infty} (x\varphi)^n - \sum_{n=0}^{\infty} (x(-1/\varphi))^n \right) \\
&= \frac{1}{\sqrt{5}} \cdot \left( \sum_{n=0}^{\infty} (\varphi^n - (-1/\varphi)^n) x^n \right)
\end{aligned}$$

So: we found a new way to expand our series! In particular, because power series are unique, we know that the coefficients of this different way to expand our series must be the same as the coefficients of our original power series $\sum f_n x^n$:

$$\begin{aligned}
\sum_{n=0}^{\infty} f_n x^n &= \frac{1}{\sqrt{5}} \cdot \left( \sum_{n=0}^{\infty} (\varphi^n - (-1/\varphi)^n) x^n \right) \\
\Rightarrow f_n &= \frac{\varphi^n - (-1/\varphi)^n}{\sqrt{5}}.
\end{aligned}$$

So we have a closed form for the $f_n$'s. In other words, it worked!

We now turn to study a second, particularly beautiful example of the method of generating functions: **nonstandard dice**!

## 1.2 Nonstandard dice.

**Definition.** Define a $k$-sided die as a $k$-sided shape on which symbols $s_1, \dots s_k \in \mathbb{N}^+$ are drawn. Analogously, we can define a $k$-die to be a bucket with $k$ balls in it, each stamped with a symbol $s_i \in \mathbb{N}^+$. In this sense, "rolling" our die corresponds to picking a ball out of our bucket; for intuitive purposes, pick whichever model makes more sense and feel free to use it throughout this lecture.

For our lecture, we restrict all of our symbols to be positive integers: i.e. elements from the set $\{1, 2, 3, 4, \dots\}$.

A **standard** k-sided die $D$ is just a $k$-sided die with faces $\{1, 2, 3 \dots k\}$. For example, a standard 6-die is just the normal 6-sided dice that you play most board games with.

The motivating question of this lecture is the following:

**Question 1.** *Can you find two 6-sided dice $B, C$ with the following property: for any $n$, the probability that rolling $B$ and $C$ together and summing them yields $n$ is the same as the probability that rolling two standard 6-sided dice together and summing them yields $n$?*

*For example, the probability that $(B + C = 7)$ would have to be $\frac{6}{36}$, because there are 36 different ways for a pair of two 6-sided dice to be rolled, and there are precisely 6 different ways for a pair of standard 6-sided dice to sum to 7. Similarly, the probablity for $(B+C = 2)$ would have to be $\frac{1}{36}$, because there's only one way for a pair of standard 6-sided dice to sum to 2.*

To answer this, surprisingly, we can use language of generating functions[2]! To do this, let's use the following method of turning dice into sequences:

**Definition.** Given a $k$-sided die $D$, let $d_n$ denote the number of ways in which rolling $D$ yields a $n$. In this sense, the die $D$ and the sequence $\{d_n\}_{n=1}^{\infty}$ are equivalent.

For a standard $k$-die $D$, the associated sequence $\{d_n\}_{n=1}^{\infty}$ is just

$$\underbrace{1, 1, 1 \dots 1}_{\text{k 1's}}, 0, 0, \dots$$

**Question 2.** *Take two dice $B = \{b_n\}_{n=1}^{\infty}, C = \{c_n\}_{n=1}^{\infty}$, and let*

$$d_n = \textit{the number of ways that rolling } B, C \textit{ and summing yields } n.$$

*What is $\{d_n\}_{n=1}^{\infty}$ in terms of the coefficients $b_n, c_n$?*

**Answer:** How many ways can rolling $B, C$ and summing give you $n$? Well: suppose you've already rolled $B$ and gotten a $k$. Then you need to roll a $n - k$ on $C$ to get a sum of $n$! In other words,

$$\begin{aligned} d_n &= \text{the number of ways that rolling } B, C \text{ and summing yields } n \\ &= \sum_{k=1}^{n} (\text{ways to roll } B \text{ and get } k) \cdot (\text{ways to roll } C \text{ and get } n - k) \\ &= \sum_{k=1}^{n} b_k c_{n-k}. \end{aligned}$$

[2]Well, you could try brute force and checking all $10^{12}$ possible pairs of dice with faces from $\{1, \dots 11\}$, but that would make for a very long and boring lecture.

So: let $A = \{a_n\}_{n=1}^{\infty} = \{1, 1, 1, 1, 1, 1, 0, 0 \ldots\}$ be a standard 6-sided die. In the language of sequences, then, we're trying to find a pair of dice-sequences $\{b_n\}_{n=1}^{\infty}, \{c_n\}_{n=1}^{\infty}$ such that for every $n$, we have

$$\sum_{k=1}^{n} b_k c_{n-k} = \sum_{k=1}^{n} a_k a_{n-k}.$$

This looks…awful, right? In other words, we have a problem, and in the language of sequences, it's terrible. So: let's use the method of generating functions to study these sequences! After all, they can't get much worse …

**Question 3.** *If $A = \{a_n\}_{n=1}^{\infty}$ is a standard $k$-die, what is the power series $\sum_{n=1}^{\infty} a_n x^n$ associated to $A$?*

**Answer:** As mentioned earlier, we have

$$\{a_n\}_{n=1}^{\infty} = \{\underbrace{1, 1, 1 \ldots 1}_{\text{k 1's}}, 0, 0, \ldots\}.$$

Therefore, the associated power series to this sequence is just the polynomial

$$x + x^2 + x^3 + \ldots + x^k.$$

Notice that any power series associated to a $k$-sided dice $D$ is just a polynomial, as any $k$-sided dice has only finitely many faces, and therefore finitely many nonzero elements in its associated sequence $\{d_n\}_{n=1}^{\infty}$.

**Question 4.** *Let $B = \{b_n\}_{n=1}^{\infty}, C = \{c_n\}_{n=1}^{\infty}$, be a pair of dice, and let $B(x) = \sum b_n x^n, C(x) = \sum c_n x^n$ be their associated power series.*

*Let $\{d_n\}$ be the sequence associated to rolling both $B, C$ and summing the result, as discussed before. What is the power series associated to $\{d_n\}$?*

**Answer:** If we use our earlier observation about how we can formulate the $d_n$'s in terms of the $b_n, c_n$'s, we have

$$\sum_{n=1}^{\infty} d_n x^n = \sum_{n=0}^{\infty} \left( \sum_{k=0}^{n} b_k c_{n-k} \right) x^n.$$

But this is just the product of the two polynomials $B(x), C(x)$! Specifically, you can check by multiplying terms out via FOIL that

$$\left( \sum_{n=1}^{\infty} b_n x^n \right) \cdot \left( \sum_{n=1}^{\infty} c_n x^n \right) = \sum_{n=1}^{\infty} \left( \sum_{k=0}^{n} b_k c_{n-k} \right) x^n,$$

and therefore that

$$\sum_{n=1}^{\infty} d_n x^n = \left(\sum_{n=1}^{\infty} b_n x^n\right) \cdot \left(\sum_{n=1}^{\infty} c_n x^n\right)$$
$$= B(x) \cdot C(x).$$

In other words, to get the generating function for the sum of two dice, we can simply take the product of their individual generating functions!

So, in the language of generating functions, our question is now the following:

**Question.** Find a pair of polynomials with integer coefficients $B(x), C(x)$ such that

- $B(x), C(x)$ both correspond to 6-sided dice: i.e. $B(0) = C(0) = 0$ [no 0-faces], $B(1) = \sum b_i = 6, C(1) = \sum c_i = 6$ [they're 6-sided], and all of the coefficients of $B(x), C(x)$ are positive [you can't have a negative number of ways to roll a certain result.]

- Rolling $B, C$ and summing is equivalent to rolling two standard 6-sided dice and summing: i.e. via our earlier work

$$\begin{aligned} B(x) \cdot C(x) &= (\text{rolling } B, C \text{ and summing, interpreted as a polynomial}) \\ &= (\text{rolling 2 standard 6-dice and summing, interpreted as a polynomial}) \\ &= (x + x^2 + x^3 + x^4 + x^5 + x^6)^2. \end{aligned}$$

- Neither $B$ or $C$ are standard dice: i.e. neither $B(x)$ or $C(x)$ are equal to $x + x^2 + x^3 + x^4 + x^5 + x^6$.

Now our question is just one about algebra! I.e. we're just looking for a pair of polynomials whose product is some specific polynomial, whose coefficients are all positive, and that when you plug in 0 yield 0 and when you plug in 1 yield 6. This is **doable**!

Specifically: after playing around with the above polynomial, or talking to an algebraicist, you'll realize that

$$(x + x^2 + x^3 + x^4 + x^5 + x^6)^2 = (x)^2(x + 1)^2(x^2 + x + 1)^2(x^2 - x + 1)^2.$$

More specifically, none of the terms $(x), (x + 1), (x^2 + x + 1), (x^2 - x + 1)$ can be broken up into smaller polynomials, and there is no way to break up this polynomial into different integer polynomials. (In this sense, these polynomials $(x), (x+1), (x^2+x+1), (x^2-x+1)$ are thought of as **irreducible** polynomials: you cannot break them into smaller parts, and you cannot break anything made of these polynomials into different parts that does not use them. A good analogy here is to the role of **prime numbers** in the integers: just like any number can be broken up into a bunch of prime factors, any integer polynomial can be broken up into a bunch of irreducible factors.)

So: the only thing for us to do now is find out if we can split these factors $(x), (x+1), (x^2+x+1), (x^2-x+1)$ into two polynomials, so that they both correspond to 6-sided nonstandard dice.

Because $x+1$ is 2 at $x=1$, $x^2+x+1$ is 3 at $x=1$, and $x^2-x+1$ is 1 at $x=1$, we know that each $A_i(x)$ has to have exactly one copy of both $x+1$ and $x^2+x+1$ in it in order for $A_i(1)$ to be 6. As well, because they both need to be 0 at $x=0$, we need to give each polynomial a copy of $x$. Consequently, the only way we can have both of these dice not be standard is if

$$\begin{aligned} B(x) &= x(x+1)(x^2+x+1)(x^2-x+1)^2 = x^8+x^6+x^5+x^4+x^3+x, \\ C(x) &= x(x+1)(x^2+x+1) = x^4+2x^3+2x^2+x; \end{aligned}$$

i.e. we have one die with faces $\{8,6,5,4,3,1\}$ and one die with faces $\{4,3,3,2,2,1\}$.

Check this: they actually work! For example, there are precisely 6 ways in which rolling these two dice yields 7, just like for a pair of standard 6-sided dice.

Generating functions can also give us a new way to understand an object we've already studied: the binomial coefficients!

## 1.3 Binomial coefficients.

**Question 5.** *Let $f(n,k)$ denote the number of ways of picking $k$ elements out of the set $\{1,2,\ldots n\}$, where we don't care about order. What is an explicit form for $f(n,k)$?*

**Answer**: So: temporarily, for the purposes of this question, forget that we know that $f(n,k)=\binom{n}{k}$. Instead: how can we create a generating function for these objects?

Well: first, notice that we have the recurrence relation

$$f(n,k) = f(n-1,k) + f(n-1,k-1).$$

Why is this? Well, pick some way of choosing $k$ elements out of $\{1,2,\ldots n\}$. There are two possibilities: either we picked $n$, or we didn't! If we did, then ignoring the $n$ gives us a way of picking $k-1$ elements out of a set of $n-1$ objects; if we didn't, then we simply picked $k$ objects out of a set of $n-1$ elements. Summing over all of the ways of choosing $k$ elements out of $\{1,2,\ldots n\}$ then gives us our desired result.

Also: notice that $f(n,0)=1$, for all positive $n$, (as there's always exactly one way to not pick anything from a set), that $f(n,k)=0$ for all negative $n,k$ (as there's no way to pick a negative number of things, or have a set with a negative number of elements,) and that $f(n,k)=0$ if $k>n$ (as there's no way to pick more than $n$ things out of a set of $n$ elements.)

So: look at the generating function acquired by fixing $n$,

$$B_n(x) = \sum_{k=0}^{\infty} f(n,k)x^k.$$

Applying our recurrence relation to the above, then, yields

$$\begin{aligned}
B_n(x) &= \sum_{k=0}^{\infty} f(n,k)x^k \\
&= \sum_{k=0}^{\infty} (f(n-1,k) + f(n-1,k-1))x^k \\
&= \sum_{k=0}^{\infty} f(n-1,k)x^k + x\sum_{k=0}^{\infty} f(n-1,k-1)x^{k-1} \\
&= \sum_{k=0}^{\infty} f(n-1,k)x^k + \sum_{k=-1}^{\infty} f(n-1,k)x^k && \text{(b/c } f(-1,k)=0) \\
&= B_{n-1}(x) + xB_{n-1}(x) \\
&= (1+x)B_{n-1}(x).
\end{aligned}$$

Then, because $B_0(x) = 1$ (shown via our boundary conditions,) we have via induction that

$$B_n(x) = (1+x)^n.$$

Using this, then, we can find $f(n,k)$ by extracting the coefficient of $x^k$ in this power series, as follows:

- Simply take $k$ derivatives of $B_n(x)$ to kill off all of the terms with degree $< k$.
- Then, evaluate the resulting power series at 0 to eliminate all of the terms with degree $> k$.
- Finally, divide by $k!$ to cancel out the constant factor acquired by taking $k$ derivatives of $x^k$.

(It bears noting that this process will work on any power series! As such, it's a useful trick to have up your sleeve.)

So: doing this to $B_n(x)$ yields the following:

$$\begin{aligned}
\frac{d^k}{dx^k}\left(B_n(x)\right)\bigg|_0 \cdot \frac{1}{k!} &= \frac{d^k}{dx^k}\left((1+x)^n\right)\bigg|_0 \cdot \frac{1}{k!} \\
&= (n)(n-1)\cdots(n-k+1)\cdot(1+x)^{n-k}\bigg|_0 \cdot \frac{1}{k!} \\
&= (n)(n-1)\cdots(n-k+1)\cdot(1)\cdot\frac{1}{k!} \\
&= \frac{(n)(n-1)\cdots(n-k+1)}{k!} \\
&= \frac{n!}{k!\cdot(n-k)!}
\end{aligned}$$

We've rederived the binomial coefficient! Awesome.

We close with one last example problem on generating functions:

### 1.4 Coins

We close with one last example problem on generating functions. On its surface, this may look like something you could have done (with some tedium) back in elementary school:

**Question 6.** *In how many ways can you get to* 50¢ *with some combination of pennies, nickels, dimes, quarters and half-dollars?*

**Answer.** On one hand, we could simply brute-force the answer to this problem. This wouldn't be too satisfying, however; it wouldn't really tell us anything about the general problem we're studying (how to decompose some natural number $n$ into a sum of 1's, 5's, 10's, 25's and 50's), nor does it seem very "efficient" in terms of the number of calculations we'd have to make.

Instead, let's try applying the one tool we have in this lecture: **generating functions**! To make things easier, let's think about all of the ways to make **any** amount of change, not just 50¢, and suppose that we are using only pennies.

While at first glance you might think that the answer here is trivial — there are infinitely many ways, of course! — the insight is in how we can represent all of those ways. Specifically, let's represent $P$, the total number of ways to use pennies to create some amount of change, as follows:

$$\begin{aligned} P &= ⓪ + ① + ①① + ①①① + ①①①① + \dots \\ &= \emptyset + 1 + 1^2 + 1^3 + 1^4 + \dots, \end{aligned}$$

where $1^n$ denotes $n$ pennies[3].

If we now let $N$ denote the number of ways of making some amount of change with either nickels or pennies, we can write

$$\begin{aligned} N &= P + 5P + 55P + 555P + 5555P + \dots \\ &= P + 5P + 5^2P + 5^3P + 5^4P + \dots. \end{aligned}$$

This is relatively easy to see: if we're using nickels and pennies, we can group any way we have of making change into the number of pennies we use ($\emptyset + 1 + 1^2 + \dots = P$) and the number of nickels we use ($\emptyset + 5 + 5^2 + \dots$)

[3]The reason we use use exponents like $1^n$ to denote this, instead of $n1$, is because we want to keep our various ways of creating amounts of change separate for different amounts of change. In other words, if we have one way to make 5¢, it does not necessarily follow that we would have 5 ways to make 1¢! Therefore, we would not want to use notation like $5 1$ to represent the number of ways to make 5¢, as this notation would suggest that we can split up this way to make 5¢ into other ways of making change — when in fact, we often cannot do this! (I.e. it depends on whether that way was by using 5 pennies or one nickel!)

If we let $D$ equal the number of ways of using dimes, nickels, and pennies, $Q$ be the number of ways of using quarters through pennies, and $H$ be the number of ways of using half-dollars through pennies, we can get similar expressions:

$$D = N + (10)N + (10)^2 N + (10)^3 N + (10)^4 N + \dots,$$
$$Q = D + (25)D + (25)^2 D + (25)^3 D + (25)^4 D + \dots,$$
$$H = Q + (50)Q + (50)^2 Q + (50)^3 Q + (50)^4 Q + \dots.$$

Now, consider the following clever trick: take each of our expressions $P, N, D, Q, H$ and turn them into power series in the variable $z$ by replacing each coin $(k)$ with $z^k$. In other words, set

$$\begin{aligned}
P(z) &= 1 + z + z^2 + z^3 + z^4 + \dots \\
N(z) &= P(z) \cdot \left(1 + z^5 + z^{10} + z^{15} + z^{20} + \dots\right) \\
D(z) &= N(z) \cdot \left(1 + z^{10} + z^{20} + z^{30} + z^{40} + \dots\right) \\
Q(z) &= D(z) \cdot \left(1 + z^{25} + z^{50} + z^{75} + z^{100} + \dots\right) \\
H(z) &= Q(z) \cdot \left(1 + z^{50} + z^{100} + z^{150} + z^{200} + \dots\right)
\end{aligned}$$

Once this is done: think about the coefficient of $z^n$ in $H(z)$ above, for any $n$. With some time, you should be able to persuade yourself of the following fact: The coefficient of $z^n$ is precisely the number of ways to make $n$¢ using pennies, nickels, dimes, quarters, and half-dollars! This is because we've just replaced each of our coins $(k)$ with $z^k$; therefore any collection of coins that sum to $n$¢ has been transformed into a $z^n$.

Therefore, if we can just find the coefficient of $z^{50}$ in $H(z)$ above, we've answered our original problem! If we wanted, we could simply do this out right now by just multiplying our series together; however, this seems difficult (as noted earlier in our notes, the product of two series is hard to calculate!) and not like the most elegant solution.

Instead, let's try to get a cleaner and more general solution. First, recall the following identity from calculus:

$$\sum_{n=0}^{\infty} a^n x^n = \frac{1}{1 - ax}.$$

If you haven't seen this before, well, you weren't paying attention earlier in these notes! We've used this in our earlier generating functions problems. However, we never formally justified it as something we can do with formal power series: we fix this here, using only generating function techniques:

$$\begin{aligned}
\sum_{n=0}^{\infty} a^n x^n &= a^0 x^0 + \sum_{n=1}^{\infty} a^n x^n = 1 + \sum_{n=0}^{\infty} a^{n+1} x^{n+1} = 1 + ax \sum_{n=0}^{\infty} a^n x^n \\
\Rightarrow \quad (1-ax) \sum_{n=0}^{\infty} a^n x^n &= 1 \\
\Rightarrow \quad \sum_{n=0}^{\infty} a^n x^n &= \frac{1}{1-ax}.
\end{aligned}$$

With this established, plugging in $x = z, z^5, z^{10}, z^{25}, z^{50}$ yields the identities

$$\sum_{n=0}^{\infty} z^n = \frac{1}{1-z}, \quad \sum_{n=0}^{\infty} (z^5)^n = \frac{1}{1-z^5}, \quad \sum_{n=0}^{\infty} (z^{10})^n = \frac{1}{1-z^{10}},$$
$$\sum_{n=0}^{\infty} (z^{25})^n = \frac{1}{1-z^{25}}, \quad \sum_{n=0}^{\infty} (z^{50})^n = \frac{1}{1-z^{50}},$$

which when applied to our $P(z), N(z), D(z), Q(z)$ and $H(z)$ yields the identities

$$\begin{aligned}
P(z) &= \frac{1}{1-z}, \\
N(z) &= P(z)\frac{1}{1-z^5} = \frac{1}{(1-z)(1-z^5)}, \\
D(z) &= N(z)\frac{1}{1-z^{10}} = \frac{1}{(1-z)(1-z^5)(1-z^{10})}, \\
Q(z) &= D(z)\frac{1}{1-z^{25}} = \frac{1}{(1-z)(1-z^5)(1-z^{10})(1-z^{25})}, \\
H(z) &= Q(z)\frac{1}{1-z^{50}} = \frac{1}{(1-z)(1-z^5)(1-z^{10})(1-z^{25})(1-z^{50})}.
\end{aligned}$$

Again, from here we could simply expand the denominator of $H(z)$ into the degree-91 polynomial that it is, decompose this into its 91 roots, and use partial fractions to break this up into a ton of fractions, each one of which we could use the $\sum_{n=0}^{\infty} a^n x^n = \frac{1}{1-ax}$ identity to turn into tractable power series. Summing all of those up would give us our answer, and if you think that's a good idea go and give it a shot!

In the meantime, the sane people will continue with these notes, and try to find a solution that doesn't involve factoring a degree-91 polynomial to make change. In particular, there is one clever idea that we can use here that bears special attention! First, recall that throughout all of these notes, we've repeatedly used proof structures that model the following:

Given a recurrence relation, we can find a closed form for a generating function!

The situation we're in now, however, is the opposite; we have generating functions, but we don't have a recurrence relation for our change problem! Accordingly, we're motivated to flip the above method:

Given a generating function, can we find a recurrence relation for its coefficients?

The answer to this question is yes! In particular, notice that if we take our earlier expressions for $P(z), N(z), D(z), Q(z)$ and $H(z)$ and multiply through, we get

$$\begin{aligned}
(1-z)P(z) &= 1, \\
(1-z^5)N(z) &= P(z), \\
(1-z^{10})D(z) &= N(z), \\
(1-z^{25})Q(z) &= D(z), \\
(1-z^{50})H(z) &= Q(z).
\end{aligned}$$

For notation's sake, let $P_n, N_n, D_n, Q_n, H_n$ denote the coefficients of $P(z), N(z), D(z), Q(z)$ and $H(z)$ above. Then, for $P(z)$, we specifically have

$$\begin{aligned}
(1-z)P(z) = (1-z)\sum_{n=0}^{\infty} P_n z^n &= 1 \\
\Rightarrow \sum_{n=0}^{\infty} P_n z^n - z\sum_{n=0}^{\infty} P_n z^n &= 1 \\
\Rightarrow P_0 + \sum_{n=1}^{\infty} P_n z^n - \sum_{n=0}^{\infty} P_n z^{n+1} &= 1 \\
\Rightarrow \sum_{n=1}^{\infty} (P_n - P_{n-1}) z^n &= 1 - P_0 = 0,
\end{aligned}$$

because $P_0 = 0 =$ the number of ways to use zero pennies. However: we know that two formal power series are equal if and only if their coefficients are equal! Therefore, the coefficients of the left-hand-side — the expression $(P_n - P_{n-1})$ — is equal to the coefficients of the right hand side, which are all zero! In other words, we have

$$P_0 = 1, P_n = P_{n-1}.$$

A recurrence relation! A really boring one; it in fact just says that $P_n = 1$ for every $n$. But this is what we would expect, because $P(z) = 1 + z + z^2 + z^3 + \ldots$ is indeed the power series where all of its coefficients are 1!

More usefully, we can use the exact same logic above to deduce recurrence relations for

$N(z), D(z), Q(z)$ and $H(z)$:

$$\begin{aligned}
(1-z^5)N(z) &= P(z) \\
\Rightarrow \sum_{n=0}^{\infty} N_n z^n - z^5 \sum_{n=0}^{\infty} N_n z^n &= \sum_{n=0}^{\infty} P_n z^n \\
\Rightarrow N_0 + N_1 z + N_2 z^2 + N_3 z^3 + N_4 z^4 + \sum_{n=5}^{\infty} N_n z^n - \sum_{n=0}^{\infty} N_n z^{n+5} &= \sum_{n=0}^{\infty} P_n z^n \\
\Rightarrow N_0 + N_1 z + N_2 z^2 + N_3 z^3 + N_4 z^4 + \sum_{n=5}^{\infty} (N_n - N_{n-5}) z^n &= \sum_{n=0}^{\infty} P_n z^n.
\end{aligned}$$

By equating the left and right-hand sides, we have the recurrence relation

$$\begin{aligned}
N_0 = P_0, N_1 = P_1, N_2 = P_2, N_3 = P_3, N_4 = P_4; \\
N_n = N_{n-5} + P_n, \forall n \geq 5.
\end{aligned}$$

Using similar methods to the above two derivations gives us

$$\begin{aligned}
D_0 = N_0, \ldots D_9 = N_9, &\quad D_n = D_{n-10} + N_n, \forall n \geq 10, \\
Q_0 = D_0, \ldots Q_{24} = D_{24}, &\quad Q_n = Q_{n-25} + D_n, \forall n \geq 25, \\
H_0 = Q_0, \ldots H_{49} = Q_{49}, &\quad H_n = H_{n-50} + Q_n, \forall n \geq 50.
\end{aligned}$$

Recurrence relations! We can use these to populate a table of values for our coefficients, by simply applying the relations above to the "base-case" values $P_n = 1, \forall n$:

| $n$ | 0 | 5 | 10 | 15 | 20 | 25 | 30 | 35 | 40 | 45 | 50 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $P_n$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $N_n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| $D_n$ | 1 | 2 | 4 | 6 | 9 | 12 | 16 | 20 | 25 | 30 | 36 |
| $Q_n$ | 1 | 2 | 4 | 6 | 9 | 13 | 18 | 24 | 31 | 39 | 49 |
| $H_n$ | 1 | 2 | 4 | 6 | 9 | 13 | 18 | 24 | 31 | 39 | $\boxed{50}$ |

So there are exactly fifty ways to make 50¢ using our change! That's remarkably nice, actually.

The methods above generalize fairly beautiful to answer the following problem about **partitions**:

**Definition.** Take any natural number $n$. A **partition** of $n$ is any way to write $n$ as a sum of smaller natural numbers, where we do not care about the order in which we write our sum. For example, 5 can be partitioned in six different ways:

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

We let $p_n$ denote the number of partitions of $n$.

**Theorem.** The generating function for the sequence $\{p_n\}_{n=0}^{\infty}$ is

$$P(x) = \prod_{n=1}^{\infty} \frac{1}{1-x^n}.$$

*Proof.* We use the exact same ideas as above. Let $p_n^{(i)}$ denote the number of partitions of $n$ that use only natural numbers that are at most $i$. For example, $p_n^{(1)}$ is 1 for every $n$, as there is exactly one partition of any $n$ if we only can use 1's.

Then, if we let $P^{(m)}(x)$ denote the generating function for the sequence $\{p_n^{(m)}\}_{i=0}^{\infty}$, we have that

$$P^{(1)}(x) = \sum_{n=0}^{\infty} p_n^{(1)} x^n = \sum_{n=0}^{\infty} 1 \cdot x^n = \frac{1}{1-x}.$$

I claim that in general,

$$P^{(m)}(x) = \prod_{n=1}^{m} \frac{1}{1-x^n},$$

and prove it by induction. We have already established our base case above; so let's move to the inductive step. Assume that

$$P^{(m)}(x) = \prod_{n=1}^{m} \frac{1}{1-x^n};$$

we seek to prove that this relation holds for $m+1$ as well. To do this, we do the same trick we did for coins: think of all of the ways to make natural numbers using unordered sums of natural numbers no greater than $m+1$. If we let $M$ denote the collection of all of these ways that use only numbers up to $m$, we can group these ways by the number of "m+1" elements we use as follows:

$$M + \text{m+1}\, M + \text{m+1}\,\text{m+1}\, M + \text{m+1}\,\text{m+1}\,\text{M+1}\, M + \dots$$

As before, if we replace each k with $x^k$, we replace each way to make $n$ with $x^n$; therefore, the coefficients of the resulting power series are precisely the coefficients of $P^{(m+1)}(x)$, the series we want to study!

In particular, if we do this here, we would replace $M$ with $P^{(m)}(x)$ by definition, and get

$$\begin{aligned}
P^{(m+1)}(x) &= P^{(m)}(x) + x^{m+1}P^{(m)}(x) + x^{2m+2}P^{(m)}(x) + \dots \\
&= P^{(m)}(x)(1 + x^{m+1} + x^{2m+2} + \dots) \\
&= P^{(m)}(x) \cdot \frac{1}{1-x^{m+1}} \\
&= \prod_{n=1}^{m+1} \frac{1}{1-x^n}.
\end{aligned}$$

Our claim was about $\{p_n\}_{n=0}^{\infty}$, however; i.e. the sequence of partitions where we do not restrict the sizes of our terms. But this is simply the limit of the $P^{(m+1)}(x)$'s as $m$ goes to infinity, as letting $m$ go to infinity is just letting our terms be arbitrarily large! Therefore, we have

$$P(x) = \prod_{n=1}^{\infty} \frac{1}{1-x^n}.$$

□

# 2 Sieves and Generating Functions

In the above four subsections, we studied many individual examples of generating functions and how they work; along the way, we saw several useful techniques (partial fractions, using recurrence relations to get generating functions, using generating functions to recurrence relations, when plugging in values to a generating function is a useful idea, how derivatives work with generating functions.)

In this section, we reverse things a bit to a more top-down approach: rather than introduce an idea with an example, we start with some abstraction first (and then make it concrete with an example!)

**Concept.** Consider the following set of general "things:"

- $\Omega$, a finite set of objects.
- $P$, a collection of properties.

To give a concrete example, you could have

- $\Omega = \{1, 2, 3, 4\}$, and
- $P = \{\text{odd, prime}\}$,

In general, this is a sort of situation we will often find ourself in: we will have a set of objects and they will have properties. In this setting, a very common combinatorial question to ask is the following:

**Question.** For a given subset of our properties $P$, how many of our elements satisfy precisely those properties and no others?

In our example earlier, we can simply answer this question via brute-force; for instance, there are two odd elements, two prime elements, one odd prime element, and one element that is neither odd nor prime. In general, however, this can be a difficult question to answer directly; it is often hard to say **exactly** how many elements have $r$ properties. Instead, it's often easier to count how many objects have at **least** $r$ properties! To give an example, consider the following problem:

**Example.** A **permutation** of $\{1, 2, \ldots n\}$ is any bijection $\pi : \{1, 2, \ldots n\} \to \{1, 2, \ldots n\}$ from the set $\{1, \ldots, n\}$ to itself. A **fixed point** of a permutation $\pi$ is any element $k \in \{1, \ldots n\}$ such that$\pi(k) = k$.

Take any subset $S$ of $\{1, 2 \ldots n\}$. How many permutations fix every element of $S$ but no others? In particular, what happens when $S = \emptyset$?

Trying to answer this directly seems... hard (if you don't believe me, try it!) Conversely, suppose that we had the following different question:

**Example.** Take any subset $S$ of $\{1, 2 \ldots n\}$. How many permutations fix at least all of the elements of $S$?

**Answer.** This is pretty straightforward! By definition, any such permutation $\pi$ must have $\pi(s) = s$ for every $s \in S$. This leaves us with the remaining $n - |S|$ elements to make decisions on, and we can do whatever we want to these remaining elements as long as we stay a bijection. Therefore, we have a total of $(n - |S|)!$ many such permutations (as we have $n - |S|$ many choices for where to send the first non-$S$ element, $n - |S| - 1$ choices for where to send the second, and so on.)

Can we use this to our advantage? In other words, can we turn knowledge about the amount of objects possessing at least $r$ properties into knowledge about objects possessing exactly $r$ properties?

The answer is yes, and the method should be unsurprising: we use generating functions!

**Concept.** Take any pair $\Omega, P$, where $\Omega$ denotes some set of objects and $P$ a set of properties. For any subset $S$ of $\Omega$, let $A(S)$ be the number of elements in $\Omega$ that satisfy all of the properties in $S$ (and possibly others too, but at least these properties.) Let $n_r$ denote the following sum:

$$n_r = \sum_{S \subseteq P : |S| = r} A(S).$$

Given any $x \in \Omega$, let $f(x)$ denote the subset of $P$ corresponding to the collection of properties that $x$ satisfies. Then, we have that

$$\begin{aligned}
n_r &= \sum_{S \subseteq P : |S| = r} A(S) \\
&= \sum_{S \subseteq P : |S| = r} \left( \sum_{x \in \Omega : S \subseteq f(x)} 1 \right) \\
&= \sum_{x \in \Omega} \left( \sum_{S \subseteq P : |S| = r, S \subseteq f(x)} 1 \right) \\
&= \sum_{x \in \Omega} \binom{|f(x)|}{r}.
\end{aligned}$$

The clever trick we did above here is "switching the order of summation:" that is, instead of first summing over all of the subsets $S$ of $P$ and then summing over the elements of $\Omega$, we are instead grouping things by elements in $\Omega$ and then summing over subsets $S$ of $P$. This sort of trick is very useful/will come up lots!

If we look at what we've proven above, we can see that every element of $\Omega$ with exactly $t$ properties contributes $\binom{t}{r}$ to the quantity $n_r$. Let $e_t$ denote the number of elements in $\Omega$ with exactly $t$ properties. Then, I claim that

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

To see why this is true, consider any element $x$ of $\Omega$ with $t$ properties $\{p_1, \ldots p_r\}$. There are precisely $\binom{t}{r}$ subsets of these properties that $x$ satisfies, and for each such subset we counted $x$ once in the earlier sum for $n_r$! This justifies the claim above.

Given this claim, 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, if we stick our results from earlier together and again switch the order of summation, we get the following surprising identity:

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

In other words: with the tools 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 remarkably useful trick:

**Observation.** Because $E(x) = N(x-1)$, we have that $e_t$ is just the coefficient of $x^t$ in $N(x-1)$. To be specific: for any power series $G(x)$, let $[x^t]G(x)$ denote the coefficient of

$[x^t]$ in $G(x)$. Then, we have

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

So: if you know the $n_r$'s, you can use them to determine the $e_t$'s! That's nice.

To illustrate the power of what we've just done, we return to our earlier example:

**Question.** Of the $n!$ permutations of $\{1, \ldots, n\}$, how many have no fixed points?

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

- $\Omega =$ the collection of all permutations on $\{1, 2, \ldots n\}$, and
- $P = \{P_1, \ldots P_n\}$, where $P_i$ is the property that $i$ is a fixed point of our permutation.

As discussed earlier, for any $S \subset P$, the number of permutations $A(S)$ satisfying $S$ is just $(n - |S|)!$.

Consequently, we have that if $r \leq n$, that

$$n_r = \sum_{|S|=r} A(S) = \sum_{|S|=r} (n-|S|)! = \binom{n}{r}(n-r)! = \frac{n!}{r!}.$$

Trivially, we have that $r_n = 0$ for $r > n$, as it is impossible for a permutation on $n$ points to have more than $n$ fixed points.

If we look at the power series $N(x)$ for the $n_r$'s, we get

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

where that last step is justified by remembering that $e^x$'s Taylor series is $\displaystyle\sum_{r=0}^{\infty} \frac{x^r}{r!}$, and therefore that for any decently-sized value of $n$ the sum $\displaystyle\sum_{r=0}^{n} \frac{(-1)^r}{r!}$ is approximately $e^{-1}$.

Consequently, we have proven that the number of permutations with no fixed points is approximately $\frac{n!}{e}$. Cool!