How to Discover Generating Functions

Yuv Saxena, Jamie Baker

SoME3

Maths should be something that is intuitive - it shouldn't only make sense to the talented mathematician, but it should be something that an uninitiated reader can think about for a while and follow along naturally, without having to make any massive weird steps that don't make any sense (in so far as why you are doing that step) until you somehow, inexplicably, arrive at a solution. Each part of the solution should be motivated by what came before without much surprise. Sometimes, some proofs and mathematical works have multiple key cruxes that all are important to the final solution, and so we have to pause work on one crux and start on another in order to catch up and move forward with our proof. But in any case, one piece of mathematics that seems to consistently break all these rules is generating functions. However they are presented or taught, it seems like there is no way to feel like you could have discovered them yourself - it seems that there is no way to just play around with some maths and stumble upon something that an experienced mathematician could look at and say "looks like you have a generating function on your hands". Hopefully this will change your mind.

Imagine you are studying a sequence; specifically one generated by the recurrence relation $a_{n+1} = 2a_n + 1$, where $a_1 = 0$

We can write out the first few terms in the sequence:

$$0, 1, 3, 7, 15, ...$$

However, this form is not particularly useful, as you may often want to write the sequence as an nth term formula, $U(n) = f(n)$.

Now, our sequence is an infinite string of numbers. Just as we can represent any list of numbers as a vector, we can represent our infinite list of numbers as an infinite vector, which we will call **a**. We arrange the numbers in **a** such that the number found in the nth row corresponds to the nth term in the sequence.

$$\mathbf{a} = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ ... \end{bmatrix}$$

But this is no good if all we have done is rephrase our sequence. We need to be able to use it algebraically. In this case, it would be useful to be able to shift the numbers in a up and down to represent going from a_n to a_{n+1} and vice versa. A shift up would move the term a_{n+1} into the nth row and so we can see that the entry in that row was a_n and is now a_{n+1}. A shift down does the opposite.

To do this we define the infinite matrices S and P.

$$S = \begin{bmatrix} 0 & 1 & 0 & 0 & ... \\ 0 & 0 & 1 & 0 & ... \\ 0 & 0 & 0 & 1 & ... \\ 0 & 0 & 0 & 0 & ... \\ . & . & . & . & ... \end{bmatrix}$$

$$P = \begin{bmatrix} 0 & 0 & 0 & 0 & ... \\ 1 & 0 & 0 & 0 & ... \\ 0 & 1 & 0 & 0 & ... \\ 0 & 0 & 1 & 0 & ... \\ . & . & . & . & ... \end{bmatrix}$$

Because when we multiply a vector by a matrix, we go along the row of the matrix and down the column of the vector, the rows of the resulting vector are entirely determined by the corresponding rows in the matrix.

For example, when doing S**a**, from the first row of S, we get the second row in **a**, so the first number in the resulting vector is the second number in **a**. Likewise, the second number in the resulting vector is the third number in **a**. Thus, by applying S to **a**, we shift all the terms up by one.

Similarly, P shifts all the terms down by one. And so you may intuitively expect that $SP = I$, which is correct. This is because shifting up by one undoes the action of shifting down by one; it is the inverse. However, $PS \neq I$. This is because when we apply S first, we lose the first row of a, so when it is shifted down, we cannot regain that row and instead just get 0 in the first row of the resulting vector.

$$PS = \begin{bmatrix} 0 & 0 & 0 & 0 & ... \\ 0 & 1 & 0 & 0 & ... \\ 0 & 0 & 1 & 0 & ... \\ 0 & 0 & 0 & 1 & ... \\ . & . & . & . & ... \end{bmatrix}$$

This is of course the identity matrix, but with a 0 instead of a 1 in the top left corner, meaning it leaves all terms in the vector unchanged apart from the first (which goes to 0).

We have almost everything we need. But remember in our original recurrence relation, we have the $+1$ term, which we need to be able to represent with vectors and matrices to make it compatible with what we have done so far. As we want to add one to all the terms in our infinite vector (our recurrence relation is valid over the whole infinite sequence), this can be done by an infinite vector of 1s, which we will call $\mathbf{b}$.

$$\mathbf{b} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ ... \end{bmatrix}$$

Now we are in a position to write our recurrence relation in terms of matrices and vectors. As we said that $S\mathbf{a}$ acts to give us $a_n + 1$, we see that:

$$S\mathbf{a} = 2\mathbf{a} + \mathbf{b}$$

But we need to rearrange this equation in terms of $\mathbf{a}$ to get our answer. Perhaps it is as simple as:

$$S\mathbf{a} = 2I\mathbf{a} + \mathbf{b}$$
$$(S - 2I)\mathbf{a} = \mathbf{b}$$
$$\mathbf{a} = (S - 2I)^{-1}\mathbf{b}$$

No, this cannot be correct. The issue is that this gives an answer already, but we haven't yet put in our values for a_1, which the entire sequence must depend on in order for the recurrence relation to be the one that we are interested in and not any other similar recurrence relation. Remember, we want this method to work in general for any choice of a_1. So how do we introduce the a_1

term to the equation? We can use the fact that PS is not exactly equal to I. To see this, let's apply the P matrix to both sides of the original equation:

$$\begin{aligned} PS\mathbf{a} &= P(2\mathbf{a} + \mathbf{b}) \\ PS\mathbf{a} &= 2P\mathbf{a} + P\mathbf{b} \end{aligned}$$

Now, because we have lost the first row of a by applying PS, we notice that the left hand side differs from **a** by

$$\begin{bmatrix} a_1 \\ 0 \\ 0 \\ 0 \\ \dots \end{bmatrix}$$

So let's add it to both sides of the equation:

$$\begin{aligned} PS\mathbf{a} + \begin{bmatrix} a_1 \\ 0 \\ 0 \\ 0 \\ \dots \end{bmatrix} &= 2P\mathbf{a} + P\mathbf{b} + \begin{bmatrix} \mathbf{a}_1 \\ 0 \\ 0 \\ 0 \\ \dots \end{bmatrix} \\ I\mathbf{a} &= 2P\mathbf{a} + P\mathbf{b} + \begin{bmatrix} a_1 \\ 0 \\ 0 \\ 0 \\ \dots \end{bmatrix} \\ (I - 2P)\mathbf{a} &= P\mathbf{b} + \begin{bmatrix} a_1 \\ 0 \\ 0 \\ 0 \\ \dots \end{bmatrix} \\ \mathbf{a} &= (I - 2P)^{-1}(P\mathbf{b} + \begin{bmatrix} a_1 \\ 0 \\ 0 \\ 0 \\ \dots \end{bmatrix}) \end{aligned}$$

Great, but how do we take the inverse of the infinite matrix? Specifically we need a matrix, M, such that $M(I - 2P) = I$.

Let's start by writing down what I-2P is.

$$I - 2P = \begin{bmatrix} 1 & 0 & 0 & 0 & ... \\ 0 & 1 & 0 & 0 & ... \\ 0 & 0 & 1 & 0 & ... \\ 0 & 0 & 0 & 1 & ... \\ . & . & . & . & ... \end{bmatrix} - 2 \begin{bmatrix} 0 & 0 & 0 & 0 & ... \\ 1 & 0 & 0 & 0 & ... \\ 0 & 1 & 0 & 0 & ... \\ 0 & 0 & 1 & 0 & ... \\ . & . & . & . & ... \end{bmatrix}$$

$$I - 2P = \begin{bmatrix} 1 & 0 & 0 & 0 & ... \\ -2 & 1 & 0 & 0 & ... \\ 0 & -2 & 1 & 0 & ... \\ 0 & 0 & -2 & 1 & ... \\ . & . & . & . & ... \end{bmatrix}$$

We can now try algebraic methods for a few of the entries of the matrix, and the pattern we seem to get is:

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 & ... \\ 2 & 1 & 0 & 0 & ... \\ 4 & 2 & 1 & 0 & ... \\ 8 & 4 & 2 & 1 & ... \\ . & . & . & . & ... \end{bmatrix}$$

Can we prove that this works? Well, if we apply the matrix multiplication in the general case, we can indeed see that a matrix with entries that are powers of two will be the inverse of (I-2P).

Hence we have

$$\mathbf{a} = M(P\mathbf{b} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ ... \end{bmatrix})\mathbf{a}_1 = 0$$

So

$$\mathbf{a} = MP\mathbf{b}$$

Hence each row of the resulting vector will have a value that is the sum of the first (n - 1) powers of 2. This is a geometric series that has a value of $2^{n-1} - 1$ for the nth row.

$$a_n = 2^{n-1} - 1$$

And so we're done! We have a closed form formula for the nth term of our sequence that previously we were only given a recurrence formula for.

So our method so far is to rewrite the sequence as an infinite vector, and form an equation in terms of this vector. We can solve this pretty easily (at least so far) for the vector in terms of a simple matrix-vector product, and then this converts fairly easily to an nth term formula, at least in this case. What about in a slightly harder case?

Let's consider the sequence where $a_{n+1} = 2a_n + n$, and $a_1 = 0$. In a similar style to last time, let's define the vector **a** to be

$$\mathbf{a} = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ \cdots \end{bmatrix}$$

Then, the vector **z** to be

$$\mathbf{z} = \begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \\ \cdots \end{bmatrix}$$

Note that just as the infinite vector of 1s represented adding 1 to each term, z represents adding n to each term. We will use the same definitions as before for the matrices P and S.

Thus the equation this time we can form in terms of this vector looks like

$$S\mathbf{a} = 2\mathbf{a} + \mathbf{z}$$

We need to find a way to rewrite this equation now, so let's begin by taking P of both sides:

$$PS\mathbf{a} = 2P\mathbf{a} + P\mathbf{z}$$

PS**a**, again, is very nearly equal to **Ia**, but is missing the a_1 term, so lets add

$$\begin{bmatrix} a_1 \\ 0 \\ 0 \\ 0 \\ \cdots \end{bmatrix}$$

to both sides of our equation, giving:

$$I\mathbf{a} = 2P\mathbf{a} + P\mathbf{z} + \begin{bmatrix} a_1 \\ 0 \\ 0 \\ 0 \\ ... \end{bmatrix}$$

We can rearrange to get

$$(I - 2P)\mathbf{a} = P\mathbf{z} + \begin{bmatrix} a_1 \\ 0 \\ 0 \\ 0 \\ ... \end{bmatrix}$$

Finally, we can say that

$$\mathbf{a} = (I - 2P)^{-1}(P\mathbf{z} + \begin{bmatrix} a_1 \\ 0 \\ 0 \\ 0 \\ ... \end{bmatrix})$$

We already found the inverse of I - 2P last time, so we can use that here as well, and we find after some algebraic manipulation that the nth row of the product will have the equation

$$a_n = 2^n - n - 1$$

Is this technique applicable for more complicated sequences? Let's try it for what is probably the most famous recursively defined sequence.

Let f_n be the nth Fibonacci number - hence the relation we are looking at is $f_{n+2} = f_{n+1} + f_n$, where $f_1 = 0, f_2 = 1$. Let us define

$$\mathbf{f} = \begin{bmatrix} f_1 \\ f_2 \\ f_3 \\ f_4 \\ ... \end{bmatrix}$$

and let's also use a function called g(x) that is defined for all real x, such that

$$g(x) = \begin{bmatrix} x \\ 0 \\ 0 \\ 0 \\ ... \end{bmatrix}$$

We will still use the same definitions for P and S as before.

So, how would we write the relation $f_{n+2} = f_{n+1} + f_n$ in terms of the vector? Well, we would have to use the S matrix once for the f_{n+1} term, and you can probably guess that similarly, for the f_{n+2} term, we would need to use it twice. Hence that gives us the equation:

$$SS\mathbf{f} = S\mathbf{f} + \mathbf{f}$$

Again, we want all of our vectors to get rid of the S matrices, so let us multiply both sides by P:

$$PSS\mathbf{f} = PS\mathbf{f} + P\mathbf{f}$$

The PS**f** term is very nearly I**f**, but requires the addition of $g(f_1)$, while the PSS**f** term is very nearly S**f**, but requires the addition of $g(f_2)$. Hence, let us add $g(f_1)$ and $g(f_2)$ to both sides, which gives us:

$$PSS\mathbf{f} + g(f_1) + g(f_2) = PS\mathbf{f} + P\mathbf{f} + g(f_1) + g(f_2)$$

$$[PSS\mathbf{f} + g(f_2)] + g(f_1) = [PS\mathbf{f} + g(f_1)] + P\mathbf{f} + g(f_2)$$

$$S\mathbf{f} + g(f_1) = I\mathbf{f} + P\mathbf{f} + g(f_2)$$

There is still one more lingering S**f** vector, so let's multiply both sides by P again, giving:

$$PS\mathbf{f} + Pg(f_1) = P\mathbf{f} + PP\mathbf{f} + Pg(f_2)$$

Again, let us add $g(f_1)$ to both sides and note that we can simplify $PS\mathbf{f} + g(f_1)$ as $I\mathbf{f}$:

$$I\mathbf{f} + Pg(f_1) = P\mathbf{f} + PP\mathbf{f} + Pg(f_2) + g(f_1)$$

Rearranging, we get:

$$(I - P - PP)\mathbf{f} = g(f_1) + Pg(f_2) - Pg(f_1)$$

We need to just take the inverse of I-P-PP, and that will give us our answer pretty easily! But so far the only way we have been able to take inverses of infinite matrices is when they are of the form I+kP - this isn't something we've dealt with before. Trying to brute force it seems to just take us in circles. Let's see if there's any way to rewrite I-P-PP into a form that's more approachable.

Well, we already know how to handle matrices of the form I+kP, so let's think about combining these matrices. Let's say we have two matrices, I+aP and I+bP, for some constants a,b. If we choose those constants well, is there a way that we can combine the matrices to get I-P-PP? What does it even mean to "combine" matrices? Well, the most obvious choice is multiplication, so let's see where that takes us:

$$(I + aP)(I + bP) = I^2 + bIP + aIP + abPP = I + (b + a)P + (ab)PP$$

Well, if we set this equal to I - P - PP, then that gives us $b + a = -1$ and $ab = -1$ - we can solve this like a quadratic! The mean of a,b is -0.5, and the product is -1, so we get:

$$a, b = -\frac{1}{2} \pm \sqrt{(-\frac{1}{2})^2 + 1}$$
$$a, b = -\frac{1 + \sqrt{5}}{2}, \frac{2}{1 + \sqrt{5}}$$

So a and b will take values of $-\phi$ and $\frac{1}{\phi}$, where $\phi = \frac{1+\sqrt{5}}{2}$ Hence we can say:

$$(I - \phi P)(I + (\frac{1}{\phi})P)\mathbf{f} = g(f_1) + Pg(f_2) - Pg(f_1) = \begin{bmatrix} f_1 \\ f_2 - f_1 \\ 0 \\ 0 \\ ... \end{bmatrix}$$

Now let's solve for **f**

$$\mathbf{f} = (I - \phi P)^{-1}(I + (\frac{1}{\phi})P)^{-1} \begin{bmatrix} f_1 \\ f_2 - f_1 \\ 0 \\ 0 \\ ... \end{bmatrix}$$

Inverting these matrices is fairly straightforward, but multiplying both inverses together is more involved - let's look for a way to simplify this problem. We could multiply the second inverse by the vector and then multiply by the first inverse, but this also turns out to be involved, so is there a way to write a matrix-matrix-vector product in some form that does not involve a matrix-matrix product at any point?

If we let $(I - \phi P) = A$ and $(I + (\frac{1}{\phi})P) = B$, and let

$$\mathbf{v} = \begin{bmatrix} f_1 \\ f_2 - f_1 \\ 0 \\ 0 \\ ... \end{bmatrix}$$

then clearly the question we are asking is whether there exist vectors **a** and b such that $A^{-1}\mathbf{a} + B^{-1}\mathbf{b} = (BA)^{-1}\mathbf{v}$ - there isn't really any other way to split the product and the equation still be valid.

But wait, this looks just like the way we do partial fractions! In that case, we should instead write the vectors **a**, **b** as g(a) and g(b) (using the same definition of g(x) as before) for some constants a, b, since in the same way that the numerators in partial fractions are constants, the only term in each vector that is non-zero should be the first row. Does this give us any assurance that the method will work? No; the only way to make progress is to see whether our intuition has led us astray by actually trying to compute an answer, and seeing if we run into any errors.

We get:

$$A^{-1}g(a) + B^{-1}g(b) = (BA)^{-1}\mathbf{v}$$

Remembering that AB = BA, let's multiply both sides by this matrix product, so that we get the equation:

$$Bg(a) + Ag(b) = \mathbf{v}$$

Now, if we expand this, we get:

$$\begin{bmatrix} a \\ \frac{1}{\phi}a \\ 0 \\ 0 \\ ... \end{bmatrix} + \begin{bmatrix} b \\ -\phi b \\ 0 \\ 0 \\ ... \end{bmatrix} = \begin{bmatrix} f_1 \\ f_2 - f_1 \\ 0 \\ 0 \\ ... \end{bmatrix}$$

We now have 2 simultaneous equations:

$$a + b = f_1$$

$$\frac{1}{\phi}a - \phi b = f_2 - f_1$$

Solving these, we get:

$$a = \frac{1}{\sqrt{5}}(\frac{1}{\phi}f_1 + f_2)$$

$$b = \frac{1}{\sqrt{5}}(\phi f_1 - f_2)$$

Putting this back into the original equation, we have thus shown that:

$$\mathbf{f} = A^{-1}g(\frac{1}{\sqrt{5}}(\frac{1}{\phi}f_1 + f_2)) + B^{-1}g(\frac{1}{\sqrt{5}}(\phi f_1 - f_2))$$

And this is indeed a valid equation, as we have shown that this is exactly equivalent to $(BA)^{-1}\mathbf{v}$, and so it only remains to find the inverse of A and B, which we can do fairly easily as we already know the inverse of the general matrix of the form I + kP. This then means that we have our final solution:

$$f_n = \frac{1}{\sqrt{5}}((\frac{1}{\phi}f_1 + f_2)(\phi)^{n-1})((\phi f_1 - f_2)(-\frac{1}{\phi})^{n-1})$$

It is true that this method works and is valid - it's also (hopefully) true that the method makes intuitive sense and doesn't feel convoluted. However, it gets a little notationally messy, and so we should probably look for a way to express it more succinctly. For any sort of linear algebra method, including the vectors and matrices we used, the underlying maths is true for any other vector space too. So, is there another vector space that we should use instead of lists of numbers? We could, for example, use literal arrows from the origin in some infinite dimensional space, but this feels like it complicates our method even further, so let's consider the steps we did and whether any particular vector space jumps out at us.

Firstly, the matrices S and P move each of the basis vectors to the "next" or "previous" basis vectors, so we need some space where shifting from one basis vector to another is a natural process and where there is some sense of order (hopefully it's clear why the physical literal arrows, for example, would not have been helpful here). When we split the matrix I-P-PP into $I - \phi P$ and $I + \frac{1}{\phi}P$, we solved it like a quadratic, so something that preserves that notion would be helpful. Also, when simplifying the resultant matrix-matrix-vector product, we solved it like partial fractions, so something is being consistently hinted at from all of these clues towards using the abstract vector of polynomials.

The polynomials do indeed form a vector space with infinite dimensions, and they also satisfy all the axioms of a vector space. Therefore, we can re-visualise all of the work we have done in the language of polynomials.

Firstly, let's be a little more precise in our definitions. Each column in the infinite vector will be represented by a power of x, starting with $x^0 = 1$. x in this case is just a variable, and its value isn't relevant as such to our method (although you will find that sometimes there are ways to exploit its value to find interesting results). The basis vectors are therefore these powers of x, with a coefficient of 1 and with no other additional powers of x added to it.

So, in our first example, we had a vector that we were investigating called **a**, such that the nth row of a was equal to a_n. In our new vector space, this will be some function of x, a polynomial where the coefficient of the nth power of x is a_n. In this case, it makes sense to include a_0 as well for the x_0 term. Let's call this polynomial A(x). The other vector we were using was called **b**, and it was equal to

$$\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ ... \end{bmatrix}$$

so the polynomial it corresponds to is

$$1 + x + x^2 + ...$$

which, if you know a bit of calculus, you might recognise as the series expansion of $\frac{1}{1-x}$. What about the matrices S and P? Well P refers to the moving of each basis vector to the next one, i.e. dividing by x. S refers to moving each basis vector to the previous one, with the exception of the first which goes to zero. This is equivalent, therefore, to subtracting the constant term and then dividing by x.

Hence, the equation we had before in terms of vectors can be written instead with polynomials in the form:

$$\frac{A(x) - a_0}{x} = 2A(x) + \frac{1}{1-x}$$

Rearranging:

$$A(x) - a_0 = 2xA(x) + \frac{x}{1-x}$$
$$(1-2x)A(x) = a_0 + \frac{x}{1-x}$$

As in our definition, $a_0 = 0$:

$$A(x) = \frac{x}{(1-x)(1-2x)}$$

In this form it's quite easy to use partial fractions here and simplify the problem, whereas before we had to find another way to tackle a few infinite sums. Here, we can find that:

$$A(x) = x(\frac{2}{1-2x} - \frac{1}{1-x})$$

Using the binomial expansion, it is not too hard to find that:

$$A(x) = \Sigma(x^n(2^n - 1))$$

And this is a generating function! A function whose power series coefficients are the terms in our sequence. We think this is a great example of the interrelations between different areas of maths as we were able to play around with sequences using linear algebra and arrive at this completely unexpected result.

There are many explanations for what generating functions are and how they work all over the internet as well as in literature. Something that we have never found a good explanation for is how de Moivre came up with the idea. That's not to say those other explanations are not great - they are extremely helpful for learning about what this tool is all about and how they can be applied to several different situations. What we hope we have provided you with is a way that you might have discovered generating functions yourself and an idea of what it feels like to 'discover' maths.

P.S. We would like to say that we are 2 high school students from the UK, so this was our first time putting together something like this (thank you to SoME for the encouragement). We have learnt a lot and we hope you have to, but please be aware there may be a higher incidence of mistakes here than elsewhere for obvious reasons.