Nishad Deulkar - Rugby High School

Why are *Generating Functions* the most powerful secret of mathematics?

Mathematics is a collection of some of the greatest ideas brought together by some of the greatest minds in history. Some of these ideas seem, at least to us today, like natural extensions of existing maths, whereas other ideas appear to come from absolute nothingness and yet they enlighten us in a way that would be almost impossible to foresee. The topic I want to talk about today is an idea which probably falls in the latter category, and that is generating functions.

A generating function is some polynomial which helps describe some related sequence of numbers, which in its most primitive form, encodes terms of the sequence as coefficients of terms in this polynomial. I say this is primitive because I also want to extend this idea to using polynomials to help solve combinatorial and even geometrical problems, a task which at first glance appears to be nonsensical. It turns out that studying behaviours of polynomials reveals a lot about linked questions in seemingly unrelated areas of mathematics.

A new perspective on expanding brackets

We all learn how to expand brackets in secondary school. Now I'm going to ask a seemingly unrelated problem.

How many strings of 8 digits consisting of 0s and 1s (known as a "binary string") only contain exactly four 0s and four 1s? Also, how many strings of 8 such digits are there all together?

This is a counting problem, which comes under the field of combinatorics. Before we start, what actually is *combinatorics*? The best description of combinatorics that I've seen is that it is the answer to two key questions; "How many different ways are there of doing something?" and "Is something certain to happen?" and in this case we're answering the former of the two questions.

You may be able to answer this question and it's likely you didn't use any polynomials or expand any brackets and you probably found a faster method than the one I'm about to show. Yet I would argue the following method has the most beauty and generalisability.

Suppose I ask you to expand the brackets $(1 + x)^2$. You'd quite quickly tell me that it's $1 + 2x + x^2$ but let's look carefully at what this actually means.

I'm going to do something subtle and re-write this as $(x^0 + x^1)^2 = x^0 + 2x^1 + x^2$. Observe that when multiplying two powers of x, the exponents add together. The coefficient of a particular power of x in the expansion tells us,

"How many ways could we reach this power of x by adding up exponents?"

For example the coefficient of x^1 in the expansion is 2, so there are 2 ways to choose x^0 and x^1 (from our brackets) and reach x^1 (in our expansion).

Let's generalise this idea to our question about binary strings. We have 8 digits and each digit is either a 0 or a 1 so we might consider some arbitrary function (known as a generating function) with some arbitrary variable x,

$$G(x) = (x^0 + x^1)^8$$

The powers of x in the brackets denote our "choices", and the overall power denotes the "number of digits."

Now is the real magic. We want our string to have four 0s and four 1s but this happens if and only if the sum of our digits is 4. But the exponent of x in the expansion of G(x) is precisely the sum of our digits and the coefficient is precisely how many ways we could reach that digital sum. That is to say the answer to our problem is exactly the coefficient of x^4 in the expansion of G(x). Doing this expansion gives,

$$G(x) = x^0 + 8x^1 + 28x^2 + 56x^3 + 70x^4 + 56x^5 + 28x^6 + 8x^7 + x^8$$

So the answer is 70 binary strings with four 1s and 0s. And as for the second part of the problem, how many such binary strings are there, well this is the sum of all the coefficients. In other words,

$$1 + 8 + 28 + 56 + 70 + 56 + 28 + 8 + 1 = 256 \text{ binary strings}$$

(It's no coincidence that $2^8 = 256$ but that's I'll leave that for the reader to investigate!)

Everyone's favourite sequence returns

To continue my conversation about actually using generating functions, I want to talk about one of the most famous sequences, the Fibonacci numbers. The Fibonacci numbers are generated using the following rules,

- The first two terms (indexed from 0) are 0 and 1
- The subsequent terms are the sum of the two previous terms

so the first few terms are,

$$0, 1, 1, 2, 3, 5, 8, 13 \ldots$$

The issue with this definition of the sequence is that if I asked you to give me the 100th term, you would have to calculate all the previous terms first. This begs the question of, is there a way to go directly from the position of a term in the sequence to the term itself (known as a *closed form expression* for the sequence).

Well in fact there is such a closed form known as Binet's formula and it's much more interesting than you might expect. For starters it contains the golden ratio,

$$\varphi = 1.618\ldots = (1 + \sqrt{5}) / 2$$

which would definitely fall into one of the top 5 most famous constants in maths.

What's surprising about this is that the Fibonacci sequence consists of integers, and yet its closed form is in terms of some irrational number. Furthermore the closed form is this mess,

$$(\varphi^n - (-1/\varphi)^n)/\sqrt{5}$$

It seems like pure witchcraft that such a mess gives rise to such a simple sequence, but yet it does.

There are a variety of proofs for this result, but the one I want to show involves the use of a generating function. Firstly, we should establish some notation; let F_n denote the nth term in the Fibonacci sequence (so define $F_0 = 0$, $F_1 = 1$) and let G(x) be a polynomial where the coefficient of the term x^n is F_n so the first few terms are,

$$G(x) = 0x^0 + x^1 + x^2 + 2x^3 + 3x^4 + 5x^5 + 8x^6 + 13x^7 + \ldots$$

The question going through your head right now is probably, why are we doing this? And I agree, defining G(x) as we did seems like a completely arbitrary decision, and again this variable x, seems rather contrived. However, if you just trust me a bit more I'll show you where this is going.

First recall how we defined the Fibonacci numbers, this can be expressed algebraically as,

$$F_n = F_{n-1} + F_{n-2} \text{ for } n \geq 2$$

Hence we can look at G(x) and for the terms of power x^2 or higher, we can replace the coefficient F_n with $F_{n-1} + F_{n-2}$. If we write this out we have,

$$\begin{aligned} G(x) &= 0 + x + (0+1)x^2 + (1+1)x^3 + (1+2)x^4 + (2+3)x^5 + (3+5)x^6 + (5+8)x^7 + \ldots \\ &= 0 + x + x(0 + x + x^2 + 2x^3 + 3x^4 + 5x^5 + 8x^6 + \ldots) + x^2(0 + x + x^2 + 2x^3 + 3x^4 + 5x^5 + \ldots) \end{aligned}$$

but these brackets are just G(x) themselves so,

$$G(x) = x + xG(x) + x^2G(x)$$

and rearranging gives,

$$G(x) = x/(1-x-x^2)$$

Now the way we get Binet's formula is using a partial fraction decomposition and while the details of actually doing a partial fraction decomposition are a bit messy, what we can do is make the following observation, the equation $1-x-x^2 = 0$ has solutions φ and $-1/\varphi$ (denote $\tau = -1/\varphi$ for convenience) so when we do the partial fraction decomposition we get,

$$G(x) = (1/(1-\varphi x) - 1/(1-\tau x))/\sqrt{5}$$

(you can verify these two expressions are actually equal).

The next observation is that a series of numbers known as a geometric series $(ax)^0$, $(ax)^1$, $(ax)^2$, … has a sum of,

$$(ax)^0 + (ax)^1 + (ax)^2 + \ldots = 1/(1-ax)$$

where x is chosen to be such that our series converges (since x was just some arbitrary variable), and a is a constant (in particular $|ax| < 1$). Reversing this sum of a geometric series, we can see that the coefficient of x^n in G(x) is given precisely by,

$$(\varphi^n - (\tau)^n)/\sqrt{5}$$

This is exactly Binet's formula which seems absolutely magical. We introduced this random function in terms of x and managed to deduce a closed form for the Fibonacci numbers purely algebraically.

The impossible cuboid

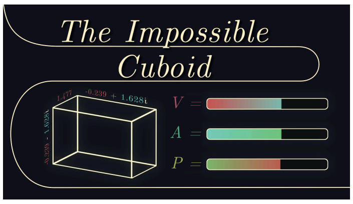
The next use of a generating function (or a similar type of concept) will be looking at a piece of 3D geometry. The problem is,

Does there exist any (rectangular) cuboid with non-zero side lengths, whose Volume, Surface Area and Perimeter (in the same units) are numerically equal?
(Perimeter in this context is the sum of the lengths of the 12 edges)

Short answer, *no*.

But before I delve into a longer written proof, I have made an animated YouTube video (with my YouTube channel called "PolyaMath") discussing this exact problem which can be found here:

No cuboid has an equal Volume, Surface Area and Perimeter. Here's why.
https://www.youtube.com/watch?v=xVtbj5U6KJg&t=11s&ab_channel=PolyaMath



To start to get a feel for the problem, first define the 3 side lengths of such a cuboid as a, b and c. These must be positive real numbers for the cuboid to exist. We can then obtain the following expressions for the volume (V), surface area (A) and perimeter (P),

$$V = abc$$
$$A = 2(ab + bc + ca)$$
$$P = 4(a + b + c)$$

The more experience you've had in the world of maths, the more eerily familiar these expressions seem. These sorts of symmetric expressions appear readily when doing expansions of brackets. In particular, pay attention to the function,

$$G(x) = (x - a)(x - b)(x - c)$$

This function G(x) is a cubic whose roots (in other words solutions to G(x) = 0) are precisely a, b and c. Now expanding G(x) gives,

$$G(x) = x^3 - (a + b + c)x^2 + (ab + bc + ca)x - abc$$

These coefficients are known as Vieta's formulas (this is a special case where the lead coefficient is 1), and they provide a way to go from the roots of a polynomial to the coefficients of a polynomial.

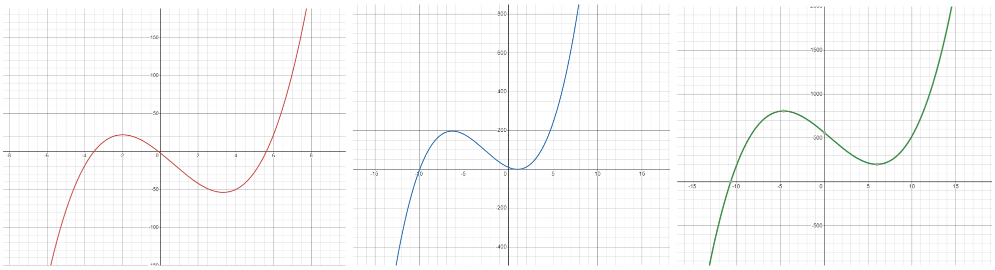
Now I'm going to set the expressions for the volume, surface area and perimeter equal to some positive real constant 4k as follows,

$$abc = 2(ab + bc + ca) = 4(a + b + c) = 4k$$

Now that we've gathered all the ingredients for this recipe, we can start assembling them together. Observe that we can now express G(x) in terms of this single real parameter k to get,

$$G(x) = x^3 - kx^2 + 2kx - 4k$$

If you've seen the graph of a cubic equation before, you will know that it either crosses the x-axis at 3 points, 2 points (one of these will be touching the x-axis) or 1 point.



But the fundamental theorem of algebra states that a polynomial of degree n has exactly n (up to repetition) roots. The key is that this includes complex roots, that is numbers containing the square root of -1.

Recall that the roots of G(x) are exactly a, b and c, but by definition these must be real, not complex so if we find that G(x) always has at least one complex root we'd reach a contradiction to such a cuboid existing. But this is equivalent to showing that G(x) has exactly 1 real root since because G(x) has real coefficients, the other 2 roots must be complex and in fact they are complex conjugates of each other.

Luckily for us, there is just the tool for this. Analogous to how the sign of $b^2 - 4ac$ (the discriminant) for a quadratic $ax^2 + bx + c = 0$ tells us how many real and complex roots we have, there is also a cubic discriminant.

If you've ever heard the tales of the mess that is the cubic formula, you'd probably expect that a cubic discriminant would be a huge and ugly expression and as much as I'd like to tell you it isn't, you're absolutely correct. The discriminant of the cubic $px^3 + qx^2 + rx + s = 0$ is the following algebraic abomination,

$$q^2r^2 - 4pr^3 - 4q^3s - 27p^2s^2 + 18pqrs$$

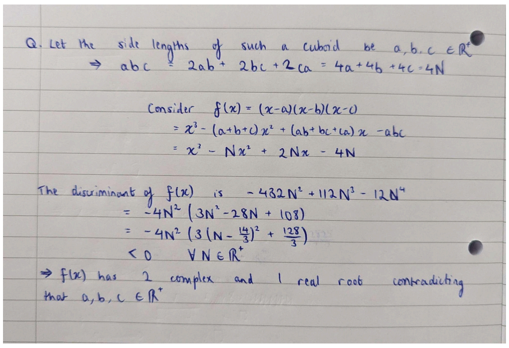
If this is negative, then our cubic has 2 complex roots.

Now we can return back to the problem by substituting the coefficients of G(x) into this formula to get an expression in terms of the parameter k,

$$\begin{gathered}(-k)^2(2k)^2 - 4(1)(2k)^3 - 4(-k)^3(-4k) - 27(1)^2(-4k)^2 + 18(1)(-k)(2k)(-4k)\\ = -432k^2 + 112k^3 - 12k^4\\ = -4k^2(108 - 28k + 3k^2)\\ = -4k^2(3(k - 14/3)^2 + 128/3)\end{gathered}$$

Since squaring any real number gives a non-negative result and since k is positive (so is non-zero), the above expression is always negative for any positive real value of k. Hence G(x) always has 2 complex roots, but since the roots of G(x) are the side lengths of our cuboid, these can't be complex, which gives us our desired contradiction.

I find it almost mesmerising that such a change in perspective from a seemingly geometric problem to pure algebra gives rise to such an elegant solution. In fact when written up formally, this proof doesn't even take up half a page.



Q. Let the side lengths of such a cuboid be $a, b, c \in \mathbb{R}^+$

$\Rightarrow abc = 2ab + 2bc + 2ca = 4a + 4b + 4c = 4N$

Consider $f(x) = (x-a)(x-b)(x-c)$

$= x^3 - (a+b+c)x^2 + (ab+bc+ca)x - abc$

$= x^3 - Nx^2 + 2Nx - 4N$

The discriminant of $f(x)$ is $-432N^2 + 112N^3 - 12N^4$

$= -4N^2(3N^2 - 28N + 108)$

$= -4N^2(3(N - \frac{14}{3})^2 + \frac{128}{3})$

$< 0 \quad \forall N \in \mathbb{R}^+$

$\Rightarrow f(x)$ has 2 complex and 1 real root contradicting that $a, b, c \in \mathbb{R}^+$

Generating functions in modern mathematics

Given that you've kept reading this far, you're probably interested in how these ideas are used to solve real problems, not just these "toy puzzles."

The Millenium Prize Problem

Perhaps the most famous open problem currently is the Riemann Hypothesis. The Riemann Zeta function is given by,

$$\zeta(s) = 1/1^s + 1/2^s + 1/3^s + 1/4^s + \ldots$$

Whilst I could talk for pages and pages about this, the Riemann Zeta function acts as a generating function to help describe the distribution of prime numbers. The prime counting function $\pi(N)$ is approximated by N/ln(N) and knowledge of the zeros of the zeta function helps bound the error term of the prime counting function.

In this way we're saying that the Riemann Zeta function is a sort of generating function which helps describe the distribution of prime numbers! (You may also be familiar with the second form for the Zeta function involving an infinite product and primes).

Integer Partitions

Slightly less well known than the Zeta function, but definitely not unknown, is the counting of integer partitions. Firstly we should introduce some terminology.

- Integer Composition - An integer composition of n is an ordered list of numbers whose sum is n e.g. [1,2,1] is a composition of of 4 and would be considered distinct from [1,1,2] or [2,1,1]
- Integer Partition - An integer partition of n is an unordered list (a set) of numbers whose sum is n so [1,2,1], [1,1,2] and [2,1,1] are considered the same partition of 4

Let C(n) and P(n) denote the number of distinct compositions and partitions of n respectively.

It turns out that C(n) has a very simple closed form which can be found by looking recursively. A composition of n can be given uniquely by considering a composition of n-1 and then we either + 1 to the end of this composition or we physically add 1 to the last term of the composition of n-1. That is to say for every one composition of n-1, there are two compositions of n so,

$$C(n) = 2C(n-1) \text{ and } C(1) = 1$$

$$\text{Hence, } C(n) = 2^{n-1}$$

If compositions are so friendly, you might hope that partitions would be just as nice. However, that is far from the case. There is no known closed form for P(n). The only ways we can count integer partitions is with clever searching algorithms, or with the use of a generating function.

The generating function for P(n) takes many ideas from our very first problem about binary strings and expanding brackets. The generating function that gets used is,

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

This may seem confusing at first, but let's take a look at why this works, in particular, why when we expand this is the coefficient of x^n precisely P(n). If we consider the kth bracket in G(x), this is,

$$(1 + x^{1k} + x^{2k} +...)$$

So the term in the kth bracket represents how many times k appears in the partition of n. We are choosing numbers in the partition in ascending order so we don't count the same partition twice and hence once G(x) is expanded the coefficient of x^n is exactly P(n). (What we've done is found a *bijection* between products of terms in each bracket and partitions of n)

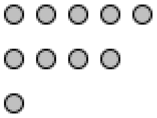
If you're curious, you can expand out the first few terms of G(x) to get,

$$G(x) = 1 + x + 2x^2 + 3x^3 + 5x^4 + 7x^5 + 11x^6 + 15x^7 + ...$$

Using the sum of a geometric series formula that was mentioned before, we can take |x| < 1 and say that,

$$G(x) = 1/(1-x^1)(1-x^2)(1-x^3)...$$

Just as a little extra, a common way of representing partitions is a Ferrers diagram,



(which represents 5 + 4 + 1)

The number of dots in each row is always non-decreasing (going upwards) to avoid overcounting the same partitions twice.
(Interestingly, if you remove this non-decreasing restriction, you can find another way of proving the formula for C(n), which I'll leave as an exercise for the reader)

Again just like the Riemann Zeta function, the integer partition function is rich with explored mathematics and theorems, beyond the scope of this article, but that doesn't take away from the immense power that generating functions have granted us.

I hope that after reading this, you've gained a greater appreciation for some of the mathematics brought to us by some of the greatest minds but also an understanding of how perhaps approachable some of the most advanced mathematics really is. Furthermore, I've only really scratched the surface of problems using generating functions. I didn't even mention probability generating functions (PGFs) which are a whole other rabbit hole to navigate through.

However, to conclude you can rest happily knowing that you have access to one of the most amazing tools ever discovered and it's your turn to explore!