Why Generating Functions Rule

An Invitation To Generating Functions

Featuring a Derivation of the

Explicit Formula of the Fibonacci Numbers

Sebastian Wild

September 28, 2012

Inductive proofs are one of the main tools of discrete mathematics, often yielding suprisingly simple proofs for complicated statements. Yet, this simplicity comes at a price: Inductive arguments typically lack the possibility to *derive* a valid statement; we can only *verify* a given one. The theory of $\mathcal{NP}$-hardness suggests that finding a solution is way more complicated than verifying a given one. Hence in this sense, induction is a 'weak' method.

One famous example demonstrating this is the explicit formula for the Fibonacci sequence. The Fibonacci numbers are recursively defined as

$$F_0 = 0, \qquad F_1 = 1, \qquad F_k = F_{k-1} + F_{k-2} \quad \text{for } k \geqslant 2 .$$

From this definition, it is evident that the sequence is non-decreasing and rather fast-growing. Apart from that, the innocent-looking definition does not give us clues how an explicit formula might look like. Here it is:

$$F_k = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^k - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^k \qquad (F_k \text{ explicit})$$

This formula is remarkably ugly; it's not even evident from it that F_k is rational, let alone natural for any $k \in \mathbb{N}$!

Typically, (F_k explicit) simply appears out of thin air and is then proven by induction — leaving it open how to *find* such explicit formulæ. This is where generating functions take off.[1]

[1]The following derivation is taken more or less literally from [GKP94, p. 297ff].

For a sequence $(a_i)_{i\in\mathbb{N}}$ of real numbers, define the **(ordinary) generating function**

$$G(z) := \sum_{i=0}^{\infty} a_i z^i .$$

The prudent reader will insist that — depending on a_i — above series might not converge. In fact, the *function* $G : \mathbb{C} \to \mathbb{C}$ might be undefined for *any* $z \neq 0$.[2] The way out is simple: We don't interpret $G(z)$ as a complex function, but as a purely *algebraic* entity instead: *Formal* power series.

These decent guys have a right to exist independent from convergence issues: Together with componentwise addition and *convolution* (a. k. a. Cauchy product)

$$\left(\sum a_i z^i\right) \cdot \left(\sum b_i z^i\right) := \sum_{i=0}^{\infty} \left[\textstyle\sum_{k=0}^{i} a_k b_{i-k}\right] z^i ,$$

formal power series form a ring. We can derive rules for computation, such that we can work with generating functions in a natural way.[3]

Using the recurrence relation from the definition, we can compute a closed form for the generating function G of the Fibonacci sequence:

$$\begin{aligned}
G(z) := \sum_{i=0}^{\infty} F_i z^i &= F_0 + F_1 z + \sum_{i=2}^{\infty} (F_{i-1} + F_{i-2})\, z^i \\
&= \ 0 \ + \ z \ + z \textstyle\sum_{i=1}^{\infty} F_i z^i \ + z^2 \displaystyle\sum_{i=0}^{\infty} F_i z^i \\
&= \quad z \quad + z\big(G(z) - F_0\big) + z^2 G(z) \\
\iff \qquad G(z) &= z + zG(z) + z^2 G(z) \\
\iff \qquad G(z) &= \frac{z}{1 - z - z^2} .
\end{aligned}$$

This is a rather pleasing term — it doesn't look half as scary as (F_k explicit)!

. . . but wait a second. After all, we'd like to *derive* (F_k explicit). So, doesn't finding such a nice formula simply imply the nasty tricks are yet to come? What can this closed form of G do for us, anyhow?

Of course, we need to find our way back from generating functions to coefficients. In general, there are several more or less involved ways to do so — we'll stick to one that works for rational functions.

[2] As an example, $\sum_{i=0}^{\infty} i! z^i$ has radius of convergence 0, hence its generating function is a not well-defined complex function.

[3] A thorough introduction is given in chapter 2 of [Wil06].

Our goal is to 'massage' our closed form of G to let us apply well-known identies for (power-) series. Actually, in our case, high-school knowledge suffices:[4]

$$\sum_{i=0}^{\infty} c^i = \frac{1}{1-c} \qquad \text{for } |c| < 1 . \tag{geometric}$$

For rational funtions, the massage technique of choice is *partial fraction decomposition*. The denominator of $G(z)$ factors into

$$1 - z - z^2 = (1-\phi z)(1-\hat{\phi} z) \qquad \text{with } \phi = \frac{1+\sqrt{5}}{2} \text{ and } \hat{\phi} = 1 - \phi = \frac{1-\sqrt{5}}{2} .$$

(The attentive reader immediately recognizes ϕ and his brother $\hat{\phi}$ as the bases of the exponents in (F_k explicit). It seems we're finally on a hot scent!
By the way, $\phi \approx 1.61803$ is the famous *golden ratio* — a number that keeps occurring as ratio of lengths in animals and plants, as well as in fine arts.)

We use the following ansatz for partial fractions

$$\frac{z}{1-z-z^2} = \frac{A}{1-\phi z} + \frac{B}{1-\hat{\phi} z} . \tag{part. frac.}$$

Setting $z = 0$ in (part. frac.) yields $B = -A$.

Now, we multiply (part. frac.) with common denominator $1 - z - z^2$ to get

$$\begin{aligned} & z = A(1-\hat{\phi} z) - A(1-\phi z) = Az(\phi - \hat{\phi}) \\ \iff \qquad & A = \frac{1}{\phi - \hat{\phi}} = \frac{1}{\sqrt{5}} . \end{aligned}$$

(Aha, there we have the $1/\sqrt{5}$ ocurring in (F_k explicit) — victory is within our grasp.)
Im summary, we now know

$$G(z) = \frac{z}{1-z-z^2} = \frac{1/\sqrt{5}}{1-\phi z} + \frac{-1/\sqrt{5}}{1-\hat{\phi} z} .$$

[4] Many of those series identities are listed in [Sei94, ("Theoretical Computer Science Cheat Sheet")].
Some careful thought is needed to show that such equalities hold for *formal* power series.
We show the variant of (geometric) $\sum q^i z^i = \frac{1}{1-qz}$. First, note $\sum q^i z^i$, $1 - qz$ and 1 are generating functions for sequences $a_i = q^i$, b_i and $d_i = \delta_{i,0}$ (Kronecker delta) respectively, with $b_0 = 1$, $b_1 = -q$ and $b_i = 0$ for $i \geqslant 2$. Multiplying in the ring, we get

$$(1-qz) \cdot \left(\sum_{i=0}^{\infty} q^i z^i\right) = \sum_{i=0}^{\infty} \left[\sum_{k=0}^{i} b_k q^{i-k}\right] z^i = \sum_{i=0}^{\infty} \left[\begin{smallmatrix} q^i & \text{for } i=0 \\ q^i - q \cdot q^{i-1} & \text{for } i \geqslant 1 \end{smallmatrix}\right] z^i = 1 .$$

So, $\sum q^i z^i$ and $1 - qz$ are reciprocals of each other. Hence, we can define *division* by $1 - qz$ as multiplication with $(1-qz)^{-1}$, such that $\frac{1}{1-qz}$ is a well-defined formal power series.
[Wil06, prop. 2.1] even states: Any generating function for sequence a_i with $a_0 \neq 0$ has a unique reciprocal.

Looking at this last representation of G, we can spot two instances of the right hand side of (geometric):

$$\begin{aligned} G(z) &= \tfrac{1}{\sqrt{5}} \frac{1}{1-(\phi z)} - \tfrac{1}{\sqrt{5}} \frac{1}{1-(\hat{\phi} z)} \\ &= \tfrac{1}{\sqrt{5}} \sum_{i=0}^{\infty} \phi^i z^i - \tfrac{1}{\sqrt{5}} \sum_{i=0}^{\infty} \hat{\phi}^i z^i \\ &= \sum_{i=0}^{\infty} \left[\tfrac{1}{\sqrt{5}} \left(\phi^i - \hat{\phi}^i \right) \right] z^i \\ &= \sum_{i=0}^{\infty} \left[\qquad F_i \qquad \right] z^i , \end{aligned}$$

where the last equation holds by definition of G. From this, we see $F_i = \frac{1}{\sqrt{5}} \left(\phi^i - \hat{\phi}^i \right)$, concluding our derivation of (F_k explicit).

Deriving the explicit formula of the Fibonacci numbers was merely a simple introductary example. The true strength of generating functions often lies in their ability to represent *operations* on number sequences. For example, convolution of sequences corresponds to multiplication of generating functions. More such operations are discussed e. g. in [Wil06].

Another powerful approach is to take a step back and interpret G as a complex function. Of course, we get back all convergence issues we could discuss away so nicely in the algebraic world. In return, we may let loose our knowledge of complex analysis. G is *analytic* within the radius of convergence ρ of the power series $\sum a_i z_i$. Well-bred sequences[5] have $\rho > 0$. For those, Cauchy's integral formula from residual calculus states

$$a_n = \frac{1}{2\pi i} \oint \frac{G(z)}{z^{n+1}} dz \qquad \text{(integrating over some closed path around the origin.)}$$

This offers an elegant and systematic way to get back the coefficients from G.

Often, this allows to derive bounds for a_i even if exact approaches fail.[6]

[5] For sequences $(a_n)_{n \in \mathbb{N}}$ with $a_n = \mathcal{O}(c^n)$ for $n \to \infty$ and some constant c, ρ will actually be at least $\frac{1}{c}$. To see this, note that for $|z| < \frac{1}{c}$, we have

$$\left| \frac{a_{n+1} z^{n+1}}{a_n z^n} \right| \leqslant |cz| < \left| c \cdot \tfrac{1}{c} \right| = 1 \qquad \text{for large } n ,$$

so the series converges absolutely by the ratio test.
As the Fibonacci numbers are non-decreasing, they fulfill $F_k = F_{k-1} + F_{k-2} \leqslant 2F_{k-1}$ and by iteration $F_k \leqslant 2^k$, so $\rho \geqslant \frac{1}{2}$. Actually, from the explicit formula, we know $\rho = \frac{1}{\phi}$.

[6] This idea and many fancy methods derived from it are presented in great depth in [FS09].

References

[FS09] P. Flajolet and R. Sedgewick. *Analytic combinatorics*. Cambridge University Press, 2009.

[GKP94] R.L. Graham, D.E. Knuth, and O. Patashnik. *Concrete mathematics: a foundation for computer science*. Addison-Wesley, 1994.

[Sei94] Steve Seiden. Theoretical Computer Science Cheat Sheet. Technical report, Lousiana State University, 1994.

[Wil06] H.S. Wilf. *generatingfunctionology*. Ak Peters Series. A K Peters, 2006.