LECTURE 7 – COEFFICIENT EXTRACTION FOR RATIONAL GENERATING FUNCTIONS

JAY PANTONE

In general, it is not possible to take a generating function $f(z)$ and extract a closed-form expression for its sequence of coefficients. Notably, rational–and to some degree algebraic– generating functions stand in contrast to this. In the following three lectures, we will learn how to perform the following tasks.

(1) Extract from a rational generating function a closed-form expression for the coefficients. This will yield the asymptotic form for the coefficients for free.

(2) Extract from an algebraic generating function a closed-form expression for the coefficients. This will *not* yield an asymptotic form for the coefficients.

(3) Use Lagrange inversion to extract coefficients from a certain functional equations that can't be solved on their own.

Rational Generating Functions

By virtue of their simplicity, rational generating functions offer complete information about the sequences of coefficients that they encode. As the first theorem shows, the coefficients of every rational generating function satisfy a linear recurrence with constant coefficients.

Theorem 7.1. *Let $f(z) = P(z)/Q(z)$ be a rational generating function with coefficient sequence $\{a_n\}_{n\geq 0}$. Then, $\{a_n\}_{n\geq 0}$ satisfies a linear recurrence with constant coefficients of the form*

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots c_d a_{n-d)},$$

where $d = \deg(Q(z))$ and $c_i \in \mathbb{Q}$, for all $n > \deg(P(z))$.

Proof. As $f(x)$ is a generating function, we may assume that $Q(0) \neq 0$; otherwise $f(z)$ is not a formal power series.

Write $Q(z) = q_0 + q_1 z + \cdots + q_d z^d$ and observe that

$$P(z) = f(z)Q(z)$$

Therefore, for $n > \deg(P(z))$

$$\begin{aligned}
0 &= [z^n]\left(f(z)Q(z)\right) \\
0 &= \sum_{k=0}^{n} \Big([z^{n-k}]f(z)\Big)\Big([z^k]Q(z)\Big) \\
0 &= \sum_{k=0}^{d} \Big([z^{n-k}]f(z)\Big)\Big([z^k]Q(z)\Big) \\
0 &= q_0 a_n + q_1 a_{n-1} + \cdots + q_d a_{n-d},
\end{aligned}$$

where we make the convention that $a_i = 0$ for $i < 0$.

Rearranging, we recover

$$a_n = -\frac{1}{q_0}(q_1 a_{n-1} + q_2 a_{n-2} + \cdots + q_d a_{n-d}).$$

□

Given that the proof is constructive (i.e., not only does it tell us that such a linear recurrence exists but also how to find it), let us calculate an example.

Example: We found in an earlier lecture that the generating function for binary words avoiding k consecutive 1's is

$$W(z) = \frac{1 - z^k}{1 - 2z + z^{k+1}}.$$

By Theorem 7.1, we obtain the recurrence

$$a_n = 2a_{n-1} - a_{n-k-1},$$

for $n \geq k + 1$. Initial values are obtained by expanding the generating function up to the coefficient of z^k. In this case, we see combinatorially that $a_i = 2^i$ for $0 \leq i \leq k - 1$ and $a_k = 2^k - 1$.

Exercise: What is the combinatorial explanation for the recurrence found above?

While a linear recurrence does allow for fast computation of terms, it has one significant drawback. Often one is interested in the asymptotic growth of a combinatorial sequence, and the associated linear recurrence typically offers no hint of this property. Consider for example the Fibonacci numbers, which satisfy the recurrence

$$a_n = a_{n-1} + a_{n-2}.$$

Surprisingly, the exponential growth rate of the sequence $\{a_n\}_{n\geq 0}$ is $\frac{1+\sqrt{5}}{2} \approx 1.618$. The next topic details how to extract a closed-form formula for the coefficients of a rational generating function, allowing us to find such properties.[1]

Theorem 7.2. *For any rational generating function $f(z) = P(z)/Q(z)$, the coefficient sequence $\{a_n\}_{n\geq 0}$ can be written in the form*

$$a_n = \sum_{i=1}^{N} P_i(n)\mu_i^n,$$

where each $P_k(n)$ is a polynomial, and each μ is an algebraic number.

Before proving this theorem, we have to review some results about binomial coefficients.

[1] This is not typical. As we'll see later, the closed-form formula that can be found for algebraic generating functions is usually unhelpful in determining asymptotic behavior.

Definition: The *binomial coefficient* $\binom{n}{k}$ is the number of ways to select k objects from a group of n objects, and

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Theorem 7.3 (Binomial Theorem)**.** *For any non-negative integer n,*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

For our purposes, we need a more general version of binomial coefficients.

Definition: Let k be a positive integer and let r be a real number. Then, the *generalized binomial coefficient* is

$$\binom{r}{k} = \frac{r(r-1)(r-2)\cdots(r-(k-1))}{k!}.$$

We use the convention that $\binom{r}{0} = 1$ and $\binom{r}{k} = 0$ when k is a negative integer. The following identity will prove useful.

Lemma 7.4. *For generalized binomial coefficients,*

$$\binom{-r}{k} = (-1)^k \binom{r+k-1}{k}.$$

Proof. By definition,

$$\begin{aligned} \binom{-r}{k} &= \frac{(-r)(-r-1)(-r-2)\cdots(-r-(k-1))}{k!} \\ &= (-1)^k \frac{r(r+1)(r+2)\cdots(r+(k-1))}{k!} \\ &= (-1)^k \binom{r+k-1}{k}. \end{aligned}$$

Further, if r is a positive integer, then,

$$\binom{-r}{k} = (-1)^k \binom{r+k-1}{k} = (-1)^k \binom{r+k-1}{r-1}.$$

$\square$

With this extended notation, a more general version of the Binomial Theorem can be stated.

Theorem 7.5 (Newton's Generalized Binomial Theorem)**.** *For any real number r,*

$$(x+y)^r = \sum_{k=0}^{\infty} \binom{r}{k} x^{r-k} y^k = x^r + r x^{r-1} y + \frac{r(r-1)}{2!} x^{r-2} y^2 + \frac{r(r-1)(r-2)}{3!} x^{r-3} y^3 + \cdots.$$

When r is a positive integer, the theorem specializes to the original binomial theorem. In all other cases, the expansion yields an infinite number of terms. In this sense, Newton's Generalized Binomial Theorem can be used to give series expansions of generating functions.

Example: The series expansion of $\sqrt{1+z} = (1+z)^{1/2}$ is

$$\begin{aligned}
(1+z)^{1/2} &= \sum_{k=0}^{\infty} \binom{1/2}{k} z^k \, (1)^{1/2-k} \\
&= \binom{1/2}{0} + \binom{1/2}{1} z + \binom{1/2}{2} z^2 + \binom{1/2}{3} z^3 + \cdots \\
&= 1 + \frac{1}{2} z + \frac{\left(\frac{1}{2}\right)\left(-\frac{1}{2}\right)}{2!} z^2 + \frac{\left(\frac{1}{2}\right)\left(-\frac{1}{2}\right)\left(-\frac{3}{2}\right)}{3!} z^3 + \cdots \\
&= 1 + \frac{1}{2} z - \frac{1}{8} z^2 + \frac{1}{16} z^3 + \cdots .
\end{aligned}$$

The next example is fundamental to the process of coefficient extraction from rational generating functions.

Example: Let r be a positive integer. Then, the series expansion of $\dfrac{1}{(1-z)^r} = (1-z)^{-r}$ is

$$\begin{aligned}
(1-z)^{-r} &= \sum_{k=0}^{\infty} \binom{-r}{k} (-z)^k (1)^{-r-k} \\
&= \sum_{k=0}^{\infty} (-1)^k \binom{r+k-1}{k} (-z)^k \\
&= \sum_{k=0}^{\infty} \binom{r+k-1}{k} z^k \\
&= \sum_{k=0}^{\infty} \binom{r+k-1}{r-1} z^k .
\end{aligned}$$

It is important to note that given the restriction on r, the coefficients of the sum are regular binomial coefficients. In fact, for fixed r the coefficients are polynomials.

Example: The series expansion of $\dfrac{1}{(1-z)^4}$ is

$$(1-z)^{-4} = \sum_{k=0}^{\infty} \binom{k+3}{3} z^k = \sum_{k=0}^{\infty} \frac{(k+3)(k+2)(k+1)}{6} z^k = \sum_{k=0}^{\infty} \frac{1}{6}(k^3 + 6k^2 + 11k + 6) z^k .$$

Generally, the generating function $(1-z)^{-r}$ has coefficients $a_n = P(n)$, for a polynomial P of degree $r-1$.

We are now ready to prove Theorem 7.2.

Proof of Theorem 7.2. Let $f(z) = P(z)/Q(z)$ be a rational generating function with coefficient sequence $\{a_n\}_{n \geq 0}$. As before, we assume $Q(0) \neq 0$. Further, we may assume

$\deg(P) < \deg(Q)$: if not, then use long division of polynomials to write

$$f(z) = r(z) + \frac{\hat{P}(z)}{Q(z)}$$

for a polynomial $r(z)$ and a new polynomial $\hat{P}(z)$ with $\deg(\hat{P}) < \deg(Q)$, and proceed as follows with $\hat{P}$ in place of P. As $r(z)$ is a polynomial, this will only affect the first $\deg(r(z)) + 1$ coefficients.

Our goal is now to write $P(z)/Q(z)$ as a sum of terms to which we can apply the expansion of $(1-z)^{-r}$ discussed above. This is accomplished with the technique of *partial fraction decomposition*.[2]

We will not go into to detail on how to perform partial fraction decomposition (because it can be tedious), but the end result is that $P(z)/Q(z)$ can be written as a finite sum

$$f(z) = \sum_{i=1}^{N} \frac{c_i}{(z-\alpha_i)^{r_i}}$$

for complex numbers c_i and α_i and positive integers r_i. After some algebraic manipulation,

$$f(z) = \sum_{i=1}^{N} \frac{c_i}{(-\alpha_i)^{r_i}} \frac{1}{(1-\frac{z}{\alpha_i})^{r_i}}.$$

By Theorem 7.5,

$$\left(1 - \frac{z}{\alpha_i}\right)^{-r_i} = \sum_{k=0}^{\infty} \binom{r_i + k - 1}{r_i - 1} \left(\frac{z}{\alpha_i}\right)^k = \sum_{k=0}^{\infty} \frac{1}{\alpha_i^k} \binom{r_i + k - 1}{r_i - 1} z^k$$

Therefore,

$$[z^n]\left(\frac{c_i}{(-\alpha_i)^{r_i}} \frac{1}{(1-\frac{z}{\alpha_i})^{r_i}}\right) = \frac{c_i}{(-\alpha_i)^{r_i}} \frac{1}{\alpha_i^n} \binom{r_i + n - 1}{r_i - 1}.$$

From this we recover a closed form formula for the coefficients of $f(z)$:

$$\begin{aligned}
[z^n]f(z) &= [z^n] \sum_{i=1}^{N} \frac{c_i}{(-\alpha_i)^{r_i}} \frac{1}{(1-\frac{z}{\alpha_i})^{r_i}} \\
&= \sum_{i=1}^{N} [z^n] \frac{c_i}{(-\alpha_i)^{r_i}} \frac{1}{(1-\frac{z}{\alpha_i})^{r_i}} \\
&= \sum_{i=1}^{N} \frac{c_i}{(-\alpha_i)^{r_i}} \frac{1}{\alpha_i^n} \binom{r_i + n - 1}{r_i - 1}.
\end{aligned}$$

This proves the theorem, with $P_i(n) = \frac{c_i}{(-\alpha_i)^{r_i}} \binom{r_i + n - 1}{r_i - 1}$ and $\mu_i = \alpha_i^{-1}$. □

Maple can be used to calculate partial fraction decompositions.

[2]This should be familiar to anyone who has taken a calculus course on integration.

Maple

```
> f := 1/(1-z-z^2):
> convert(convert(f,fullparfrac),radical);
                          1/2                     1/2
                         5                       5
            - ------------------ + ------------------
                  /     1/2      \     /           1/2\
                  |    5          |    |          5    |
                5 |z - ---- + 1/2|   5 |z + 1/2 + ----|
                  \     2        /     \            2  /
```

Example: The generating function for the Fibonacci numbers is $f(z) = \dfrac{1}{1-z-z^2}$. Setting $\rho_1 = -(\sqrt{5}+1)/2$ and $\rho_2 = (\sqrt{5}-1)/2$, the partial fraction decomposition of $f(z)$ is

$$f(z) = \frac{1}{\sqrt{5}} \cdot \frac{1}{z-\rho_1} - \frac{1}{\sqrt{5}} \cdot \frac{1}{z-\rho_2}.$$

By the constructive proof of Theorem 7.2 with $c_1 = \dfrac{1}{\sqrt{5}}$, $\alpha_1 = \rho_1$, $r_1 = 1$, and $c_2 = -\dfrac{1}{\sqrt{5}}$, $\alpha_2 = \rho_2$, $r_2 = 1$, we recover

$$\begin{aligned}
[z^n]f(z) &= P_1(n)\mu_1^n + P_2(n)\mu_2^n \\
&= \frac{1}{\sqrt{5}(-\rho_1)}\binom{n}{0}\rho_1^{-n} - \frac{1}{\sqrt{5}(-\rho_2)}\binom{n}{0}\rho_2^{-n} \\
&= \frac{5-\sqrt{5}}{10}\left(\frac{1-\sqrt{5}}{2}\right)^n + \frac{5+\sqrt{5}}{10}\left(\frac{1+\sqrt{5}}{2}\right)^n,
\end{aligned}$$

as we stated in the first lecture.

Example: Sometimes you will see oscillatory behavior. Consider for example the generating function

$$f(z) = \frac{1}{1-z^3} = 1 + z^3 + z^6 + \cdots.$$

How are these coefficients expressed in this form? First, we apply partial fraction decomposition to write

$$f(z) = -\frac{1}{3} \cdot \frac{1}{z-1} - \frac{\omega}{3} \cdot \frac{1}{z-\omega} - \frac{\omega^2}{3} \cdot \frac{1}{z-\omega^2},$$

where $\omega = \dfrac{i\sqrt{3}-1}{2}$ and $\omega^2 = \dfrac{-i\sqrt{3}-1}{2}$ are cube roots of unity. We now apply the theorem with

$$\begin{aligned}
c_1 &= -\frac{1}{3} \quad & \alpha_1 &= 1 \quad & r_1 &= 1 \\
c_2 &= -\frac{\omega}{3} \quad & \alpha_2 &= \omega \quad & r_2 &= 1 \\
c_3 &= -\frac{\omega^2}{3} \quad & \alpha_3 &= \omega^2 \quad & r_3 &= 1,
\end{aligned}$$

to obtain

$$\begin{aligned}
[z^n]f(z) &= -\frac{1}{3(-1)}1^n - \frac{\omega}{3(-\omega)}\left(\frac{1}{\omega}\right)^n - \frac{\omega^2}{3(-\omega^2)}\left(\frac{1}{\omega^2}\right)^n \\
&= \frac{1}{3} + \frac{1}{3}\left(\frac{1}{\omega}\right)^n + \frac{1}{3}\left(\frac{1}{\omega^2}\right)^n \\
&= \frac{1}{3} + \frac{1}{3}(\omega^2)^n + \frac{1}{3}\omega^n \\
&= \frac{1}{3}(1 + \omega^n + \omega^{2n}).
\end{aligned}$$

When $n = 3\ell$, this gives

$$[z^n]f(z) = \frac{1}{3}(1 + \omega^{3\ell} + \omega^{6\ell}) = \frac{1}{3}(1 + 1 + 1) = 1,$$

and when n is not a multiple of 3,

$$[z^n]f(z) = 0,$$

because for n not a multiple of 3, $\omega^n + \omega^{2n} = -1$.

When there are multiple roots in the denominator with minimal modulus, this kind of *oscillatory behavior* emerges.