LECTURE 19 – THE GUESS AND CHECK METHOD

JAY PANTONE

OVERVIEW

Consider the functional equation

$$f(z,u) = 1 + uf(z,u) + \frac{z}{u}(f(z,u) - f(z,0)).$$

We have already seen how to solve this functional equation for $f(z,0)$ using the kernel methods and resultant methods. Because of its simplicity we use it now to illustrate the guess-and-check method, though the real strength of the guess-and-check method is that it can be easily applied to very complicated functional equations.

The guess-and-check method proceeds as follows.

(1) *The functional equation $f(z,u)$ has exactly one formal power series solution.* To see this, we first note that that the constant term of any solution is 1, as it is the only term on the right-hand side with no z or u attached. Then, we observe that the coefficient of z^n (which is itself a power series in u) depends only on the coefficient of z^{n-1}.

Another way to say this is that if we start with $F_0(z,u) = 1$ and iterate the functional equation:

$$F_1 = 1 + uF_0(z,u) + \frac{z}{u}(F_0(z,u) - F_0(z,0)) = 1 + u$$

$$F_2 = 1 + uF_1(z,u) + \frac{z}{u}(F_1(z,u) - F_1(z,0)) = 1 + u + u^2 + z$$

$$F_3 = 1 + uF_2(z,u) + \frac{z}{u}(F_2(z,u) - F_2(z,0)) = 1 + u + u^2 + u^3 + (1+2u)z$$

$$\dots$$

then F_n converges to $f(z,u)$ in some appropriate sense.

(2) *Use the functional equation to crank out a lot of terms of $f(z,0)$ by iterating as above.*

(3) *Use these terms to form a conjecture for the defining polynomial of $f(z,0)$ (if it is algebraic) or a linear differential equation for which $f(z,0)$ is a solution (if it is D-finite).* This can be done in a very straightforward manner, which itself has many applications outside of this realm.

(4) *Substitute the guess into the functional equation.* This is now a single equation with a single unknown, so one can solve for $f(z,u)$. It is actually a bit more complicated than this. If $f(z,0)$ is given by a defining polynomial that cannot be explicitly solved, how does one "solve" for $f(z,u)$ – in other words, how does one obtain a defining polynomial for $f(z,u)$ itself? We will discuss this shortly.

(5) *Verify that $f(z,0)$ is as guessed.* Now that $f(z,u)$ is in hand, we can substitute $u=0$ to verify that our guess was correct. We have thus found a power series solution of $f(z,u)$. Given that we knew there existed a unique power series solution, this must be the one.

In subsequent sections, we provide details on how to conjecture a generating function for the univariate terms of a functional equation and how to substitute these conjectures into an algebraic equation.

Guessing. Suppose we have a sequence of initial terms of some formal power series whose origin we do not know. For a concrete example, suppose we are handed the sequence

$$\begin{aligned} S = \{&1,1,2,4,9,21,51,127,323,835,2188,5798,15511,41835,113634,310572,853467,\\ &2356779,6536382,18199284,50852019,142547559,400763223,1129760415,\\ &3192727797,9043402501,25669818476,73007772802,208023278209,\\ &593742784829\}. \end{aligned}$$

In order to try to guess the form of the sequence, we must first pick an *ansatz*, that is, a realm of guesses of a particular type to start our search. The ansatzes that we will consider here are algebraic and D-finite, though one can easily guess other types of equations as well.

Assume for the moment that the generating function $f(z)$ that has S as its initial terms is algebraic.[1] Then, there is some $m \geq 1$ such that

$$p_m(z)f(z)^m + p_{m-1}(z)f(z)^{m-1} + \cdots + p_1(z)f(z) + p_0(z) = 0$$

for some polynomials $p_i(z)$. Refining this, there is some d such that $\deg(p_i(z)) \leq d$ for all i, so that

$$\begin{aligned} 0 =&(a_{m,d}z^d + a_{m,d-1}z^{d-1} + \cdots + a_{m,0})f(z)^m \\ &+ (a_{m-1,d}z^d + a_{m-1,d-1}z^{d-1} + \cdots + a_{m-1,0})f(z)^{m-1} \\ &+ \quad \cdots \\ &+ (a_{0,d}z^d + a_{0,d-1}z^{d-1} + \cdots + a_{0,0}) \end{aligned}$$

for some set $\{a_{i,j}\}$ of $(d+1)(m+1)$ unknown integers.

Since we know that $f(z)$ has initial terms from S, we can write

$$f(z) = 1 + z + 2z^2 + 4z^3 + \cdots + 593742784829z^{29} + O(z^{30}).$$

[1] Of course, there are uncountably many generating functions whose initial terms match S and only countably many of them are algebraic or D-finite. What we're really looking for is the generating function that matches the context from which these terms arise.

Accordingly, we also know the series expansions of $f(z)^k$ up to the coefficient of z^{29} for all k:

$$\begin{aligned}
f(z)^2 &= 1 + 2z + 5z^2 + 12z^3 + \cdots + 3162376205180z^{29} + O(z^{30}) \\
f(z)^3 &= 1 + 3z + 9z^2 + 25z^3 + \cdots + 12135326082669z^{29} + O(z^{30}) \\
&\cdots \\
f(z)^{100} &= 1 + 100z + 5150z^2 + \cdots + 116492167882379391476034307680000z^{29} + O(z^{30}).
\end{aligned}$$

To attempt to form a conjecture, pick an m and a d. Say $d = 3$, and $m = 2$. We're thus declaring that the defining polynomial of $f(z)$ has the form

$$\begin{aligned}
0 = &(a_{2,3}z^3 + a_{2,2}z^2 + a_{2,1}z + a_{2,0})f(z)^2 \\
&+ (a_{1,3}z^3 + a_{1,2}z^2 + a_{1,1}z + a_{1,0})f(z) \\
&+ (a_{0,3}z^3 + a_{0,2}z^2 + a_{0,1}z + a_{0,0}),
\end{aligned}$$

an equation with 12 unknowns.

If we substitute the first 12 known terms of $f(z) = 1 + z + \cdots + 5798z^{11} + O(z^{12})$ into the right-hand side, making sure to truncate the product $f(z)^2$ also to 12 terms, the right-hand side becomes a polynomial in z of degree 14. However, the coefficients of z^{12}, z^{13} and z^{14} should be ignored, as they rely on terms of $f(z)$ that we did not provide. Hence we're really left with a polynomial $P(z)$ in z of degree 11. The first terms are

$$0 = (a_{2,0} + a_{1,0} + a_{0,0}) + (a_{2,1} + 2a_{2,0} + a_{1,1} + a_{1,0} + a_{0,1})z + \cdots .$$

Each term's coefficient must itself be zero for the series to equal zero. This then gives us a system of twelve equations with twelve unknowns that can be solved. The result is a set of coefficients $a_{i,j}$ that give the defining polynomial for some generating function $f(z)$ that matches the 12 initial terms we provided. The problem with this is that any set of 12 equations and 12 unknowns will (almost) always yield a solution, with no regard as to whether the generating function $f(z)$ implied by that solution matches even the next term in the sequence. We make two tweaks to fix this:

(1) If we have k unknowns in the expression, we pass in not just the first k terms of $f(z)$, but $k + T$ terms where T is some tolerance. For example, if $T = 5$ then a solution will only be found if the generating function implied by the first k terms also matches the next T.

(2) Since we can always multiply both sides of the defining polynomial by any rational number and get another solution, we use the convention that the highest order term (in the example above, $a_{2,3}$) equals 1.

Let us repeat the example above with these two constraints. Since we have the first 30 terms of the sequence, let's set $f(z) = 1 + z + \cdots + 3192727797z^{24}$ and we can use the other five terms to check our guess (if we get one). Now, we get a system of 11 unknowns (because we've set $a_{2,3} = 1$) and 25 equations. It does in fact have a solution! It has one degree of freedom:

$$\begin{gathered}
\{a_{0,0} = a_{2,2},\ \ a_{0,1} = 1,\ \ a_{0,2} = 0,\ \ a_{0,3} = 0,\ \ a_{1,0} = -a_{2,2},\ \ a_{1,1} = -1 + a_{2,2}, \\
a_{1,2} = 1,\ \ a_{1,3} = 0,\ \ a_{2,0} = 0,\ \ a_{2,1} = 0,\ \ a_{2,2} = a_{2,2}\}
\end{gathered}$$

We can set $a_{2,2}$ to be anything and still have a valid solution, so let's set $a_{2,2} = 0$. This results in

$$\{a_{1,2} = 1,\ \ a_{1,1} = -1,\ \ a_{0,1} = 1\}$$

with the remainder of the coefficients equal to zero. Therefore, the generating function given by the defining polynomial

$$0 = z^3 f(z)^2 + (z^2 - z)f(z) + z,$$

matches $f(z)$ to at least the first 25 terms. In fact, a series expansion confirms it matches the first 30 terms that we started with. We can divide both sides by z and declare with some confidence that the generating function the yielded our initial 30 terms is given by

$$0 = z^2 f(z)^2 + (z - 1)f(z) + 1.$$

In fact, these terms are the *Motzkin numbers* and their generating is given by this expression.

What would happen if we had picked d and m that were too low? Suppose we had picked $m = 1$ and $d = 3$, so that we were trying to fit $f(z)$ to the form

$$0 = (z^3 + a_{1,2}z^2 + a_{1,1}z + a_{1,0})f(z) + (a_{0,3}z^3 + a_{0,2}z^2 + a_{0,1}z + a_{0,0}).$$

Such an $f(z)$ would necessarily be rational. When attempting to solve the system of equations given by substituting $k + T$ terms, no solution would be found. In this case $T = 1$ is enough to guarantee no solution.

The general schema for conjecturing a form given N known initial terms is to pick a tolerance T (5 is a pretty safe bet), then pick all (m, d) with $m \geq 1$, $d \geq 0$ and $(m + 1)(d + 1) - 1 \leq N + T$. Perform this guessing procedure for each (m, d) until either a solution is found or every pair has failed.

There is no way to known how many terms will be needed to conjecture an algebraic GF (if it even is algebraic). In practice, I've come across examples where hundreds of terms are needed.

Guessing D-finite forms is almost identical, except instead of powers $f(z)^k$ we have derivatives $f^{(k)}(z)$. This necessitates one modification: if the highest order derivative is k, then substituting in N known terms for $f(z)$ does not give N "correct" equations as in the algebraic case, but instead $N - k$. This is essentially because each derivative deletes a term. In order words, to know correctly the z^R term of $f^{(k)}(z)$ you must know correctly the z^{R+k} term of $f(z)$.

Other ansätze are similarly handled. For example, one can conjecture that the EGF of the Bell numbers (which count the total number of set partitions) satisfies

$$0 = f(z)f'(z) - f(z)f''(z) + f'(z)^2$$

with only a few terms.

For the functional equation

$$f(z, u) = 1 + uf(z, u) + \frac{z}{u}(f(z, u) - f(z, 0)),$$

we can easily obtain 30 initial terms of $f(z,0)$ by iteration. With these we can conjecture that $f(z,0)$ satisfies

$$0 = zf(z,0)^2 - f(z) + 1.$$

CHECKING

A conjecture alone does not constitute a rigorous derivation. Reverting back to our initial example, we have now conjectured that the $f(z,u)$ that satisfies

$$f(z,u) = 1 + uf(z,u) + \frac{z}{u}(f(z,u) - f(z,0))$$

has specialization $f(z,0)$ that satisfies

$$0 = zf(z,0)^2 - f(z) + 1.$$

We are lucky that this functional equation can be solved for $f(z)$ by the quadratic method, giving

$$f(z,0) = \frac{1-\sqrt{1-4z}}{2z}.$$

Next, we substitute this conjectured $f(z,0)$ into the functional equation and solve for $f(z,u)$, giving

$$f(z,u) = \frac{1-2u-\sqrt{1-4z}}{2(u^2-u+z)}.$$

This is still a conjecture. Now we check if this proposed $f(z,u)$ does indeed satisfy the functional equation:

$$f(z,u) = 1 + uf(z,u) + \frac{z}{u}(f(z,u) - f(z,0))$$

$$\frac{1-2u-\sqrt{1-4z}}{2(u^2-u+z)} = 1 + u\frac{1-2u-\sqrt{1-4z}}{2(u^2-u+z)} + \frac{z}{u}\left(\frac{1-2u-\sqrt{1-4z}}{2(u^2-u+z)} - \frac{1-\sqrt{1-4z}}{2z}\right).$$

A little algebra verifies this equality.

Therefore we have a function $f(z,u)$ that satisfies the functional equation, and we know the functional equation has exactly one formal power series solution. Here's the one occasional difficulty: how do we know that the proposed $f(z,u)$ is an element of $\mathbb{Q}[[z,u]]$? In this case, it's because there is only one solution for $f(z,u)$ in terms of $f(z,0)$ (because the equation is linear in $f(z,u)$), and therefore this is the one guaranteed to be a formal power series.[2]

We've now rigorously found $f(z,0)$ and $f(z,u)$. To recap, there is guaranteed to be a unique formal power series solution for $f(z,u)$, and we found one, so that's it. We only needed to conjecture the form of $f(z,0)$ to help us find the conjectured form of $f(z,u)$. Once we have that, it's all just verification.

[2]For other techniques to verify that a function is a formal power series, look at Stanley's *Enumerative Combinatorics 2*, Section 6.1, Propositions 6.1.8 and 6.1.9 and Example 6.1.10. Additionally, when you have a minimal polynomial for $f(z,u)$ in hand, one can often make an iteration argument that the result is a formal power series. Or, one can use Puiseux's Theorem to check the smallest exponent with each variable.

CHECKING NON-EXPLICITLY

We were lucky in the previous example that the conjectured form for $f(z,0)$ could be solved explicitly, allowing an explicit expression for $f(z,u)$. This is typically not the case. If $f(z,0)$ has a defining polynomial of minimal degree 10, for example, one must find a way to "solve" for $f(z,u)$ (i.e., find a defining polynomial for $f(z,u)$) by operating on the level of defining polynomials.

To illustrate the difficulty, recall that

$$f(z,0) = \frac{1-\sqrt{1-4z}}{2z}$$

has defining polynomial

$$0 = zf(z,0)^2 - f(z) + 1.$$

What, then is the defining polynomial for the quantity $zf(z,0)$? Or for $\frac{z}{u}f(z,0)$? Or for $f(z,0)^2$? We can answer the first two with some simple identities, but more complicated expressions require the use of resultants. Let $f(z)$ have minimal polynomial $P(z,y)$, so that $P(z,f(z)) = 0$. Let c be a polynomial in z. Then,

(1) $f(z) + c$ is a root of $P(z, y-c)$,

(2) $cf(z)$ is a root of $c^{\deg_y(P)}P(z,y/c)$,

(3) $\frac{1}{c}f(z)$ is a root of $P(z,yc)$.

Now, let $f(z)$ and $g(z)$ have minimal polynomials $P(z,y)$ and $Q(z,y)$, so that $P(z,f(z)) = Q(z,g(z)) = 0$. Then,

(4) $f(z)+g(z)$ is a root of $\mathrm{Res}(P(z,y-t),Q(z,t),t)$,

(5) $f(z)g(z)$ is a root of $\mathrm{Res}(t^{\deg_y(P)}P(z,y/t),Q(z,t),t)$,

(6) $f(z)/g(z)$ is a root of $\mathrm{Res}(P(z,yt),Q(z,t),t)$.

Rules (1)-(3) are straight-forward to prove by substitution. We now prove Rule (4). By definition,

$$\begin{aligned} R(z,y) = \mathrm{Res}(P(z,y-t),Q(z,t),t) &= \prod_{\substack{\alpha:P(z,y-\alpha)=0 \\ \beta:Q(z,\beta)=0}} (\alpha-\beta) \\ &= \prod_{\substack{y-\alpha:P(z,\alpha)=0 \\ \beta:Q(z,\beta)=0}} ((y-\alpha)-\beta) \end{aligned}$$

Since $f(z)$ is one such α and $g(z)$ is one such β, it follows that $R(z,f(z)+g(z)) = 0$ and so $R(z,y)$ is the defining polynomial for $f(z)+g(z)$. (There is a potential problem that R is the zero polynomial, but this cannot happen because then there would be some root $t = a(z)$ such that $P(z,y-a(z)) = Q(z,a(z)) = 0$, which cannot happen if $\deg_y(P) \geq 1$.)

We show now how to apply these resultant techniques in the case of an equation that is linear in $f(z,u)$.[3] We return one last time to the functional equation

$$f(z,u) = 1 + uf(z,u) + \frac{z}{u}(f(z,u) - f(z,0)),$$

which can be rewritten as

$$f(z,u) = \frac{u - zf(z,0)}{u - u^2 - z}.$$

Given that $P(z,y) = zy^2 - y + 1$ is a minimal polynomial for $f(z,0)$, it follows that $-zP(z,-y/z)$ is a minimal polynomial for $-zf(z,0)$ and $-zP(z,-(y-u)/z)$ is a minimal polynomial for $u - zf(z,0)$. Finally, $-zP(z,-(y(u-u^2-z)-u)/z)$ is a minimal polynomial for $f(z,u)$. Expanding,

$$-zP(z,-(y(u-u^2-z)-u)/z) = -(u^2-u+z)^2y^2 - (2u-1)(u^2-u+z)y - u^2 + u - z,$$

which one can check is indeed a minimal polynomial for the explicit $f(z,u)$ calculated above.

Note that this only used rules (1)-(3). We would have needed the others rules for anything more complicated (linear or non-linear). We haven't provided a more complicated example due to time constraints but any of the walks described in Lecture 16 are good examples.

[3] In the non-linear case an extra step is required. It's not very complicated, but we're not going to cover it here. Ask me if you're interested.