LTCC Enumerative Combinatorics

Notes 1 | Alex Fink | Fall 2015

Acknowledgements

These notes have been cobbled together from a variety of sources, including in many cases appropriation of large amounts of text. I am indebted to the original authors, particularly Peter Cameron and Federico Ardila, and ultimately Richard Stanley. Martin Aigner's book also proved useful.

Conventions

$0 \in \mathbb{N}$; I will use $\mathbb{N}_+$ for the set of positive integers. log is the natural logarithm. Rings have unity.

0 Brief introduction to the module

Combinatorics is the science of discrete structures. In enumerative combinatorics, we ask questions about how many structures of a certain kind there are, for example, "how many graphs on n vertices are there?".

As in this case, we are usually faced by a problem with a natural-valued parameter n, or if you like, an infinite sequence of problems indexed by n. So if a_n is the number of solutions to the problem with index n, then the solution of the overall problem is a sequence $(a_0, a_1, \ldots)$ of natural numbers.

One might have philosophical misgivings: how are we to specify this answer, given that it contains an infinite amount of data? One way is to encode the sequence into a single object, a formal power series, sometimes called the *generating function* of the sequence. We gain a lot of technical power from this encoding: generating functions can be manipulated profitably using a host of algebraic, analytic, and other techniques. They will be a lynchpin of this module.

1 What does it mean to have counted something?

A typical counting problem will ask for the cardinality $F(n)$ of a set $\mathscr{F}(n)$ of structures of "size" n. What does it mean to have answered this problem? A few possibilities are these:

(1) An explicit formula. This may be more or less complicated, and in particular may involve a number of summations (or products, or ...).

Answers of this kind, as of others, can vary in how much they satisfy us. To the question "how many subsets has a set of size n?", the answer 2^n is incontestibly good. On the other hand, the summation formula

$$F(n) = \sum_{f \in \mathscr{F}(n)} 1$$

is clearly useless, explicit in name only.

(2) A recurrence relation expressing $F(n)$ in terms of the values of $F(m)$ for zero or more $m < n$. (I pedantically say "zero or more" so as to include the base case.)

(3) A closed form for a generating function for F. The two types of generating function most often used are the *ordinary generating function* $\sum F(n)x^n$, and the *exponential generating function* $\sum F(n)x^n/n!$. These are elements of the ring $\mathbb{Q}[[x]]$ of formal power series.

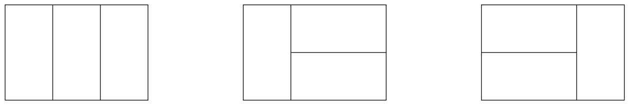
To say that the power series are *formal* is to say that we impose no demand that they converge if a non-zero complex number is substituted for x. Formal power series are discussed further in Section 1.2. If a generating function does converge, it is possible to find the coefficients by analytic methods (differentiation or contour integration).

(4) An asymptotic estimate for $F(n)$ is a function $G(n)$, typically expressed in terms of commonplace functions of analysis, such that the error $F(n) - G(n)$ in the estimate is of smaller order of magnitude than $G(n)$. (If $G(n)$ does not vanish, we can write this as $F(n)/G(n) \to 1$ as $n \to \infty$.) We write $F(n) \sim G(n)$ if this holds.

The process may be continued by providing an asymptotic estimate for $F(n) - G(n)$, and so on; the result is an *asymptotic series* for F. Asymptotic analysis will not be a focus of this module, but some basics are described below in Section 1.3.

1.1 A first example

Let's examine an example in which we'll convert between answers of these various kinds. Let a_n be the number of ways of tiling a $2 \times n$ rectangle with 2×1 or 1×2 dominoes. For instance, $t_3 = 3$, because the following are all the tilings:



To start, we can extract a *recurrence* directly from the problem, via the common trick of considering all the options for an "initial" piece of the structure, and what remains once that initial piece is removed.

Consider a $2 \times n$ rectangle, with $n \geq 1$. Its top-left corner must be covered by one of our two orientations of a domino. If it is vertical, then what remains is a $2 \times (n-1)$ rectangle, with a_{n-1} tilings. If it's horizontal — and let's say $n \geq 2$, so that this case is possible — then it must have another horizontal domino beneath it, This leaves a $2 \times (n-1)$ rectangle, with a_{n-1} tilings. Each of the tilings enumerated by t_n falls into just one of these subsets, so

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

for $n \geq 2$. As for the base case, by inspection $a_0 = a_1 = 1$.

We see that the sequence $(a_n)_{n \geq 0}$ is merely the familiar *Fibonacci sequence*, though perhaps indexed differently to your favourite conventions. (Mine are to take $F_0 = 0, F_1 = 1$.) Does "a_n is the $(n-1)$th Fibonacci number" count as a closed form? That's a matter of taste. We'll see a more clearly closed form shortly; to get it we'll pass through a *generating function*.

Generating functions are a kind of formal power series. The ordinary generating function for a sequence (a_n) is

$$A(x) := \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + \cdots$$

If you're unfamiliar with these objects, think of them as simply data structures: a formal power series is just a way to encapsulate an entire series in a single algebraic object; it is a necklace on which beads corresponding to the individual a_i are threaded. No infinite summation is actually being done.

Our recurrence translates directly to an equation satisfied by $A(x)$, since

$$\begin{aligned} A(x) &= a_0 + a_1 x \ + a_2 x^2 \ + a_3 x^3 + \cdots \\ &= 1 \ + x(a_0 + a_1 x \ \ + a_2 x^2 + \cdots) \\ &= \qquad\quad + x^2(a_0 + a_1 x + \cdots) \\ &= 1 + xA(x) + x^2 A(x) \end{aligned}$$

solves to

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

To foreshadow, we can read the x^1 and x^2 terms here as coming directly from the fact that our tilings are made of 2×1 and 2×2 subunits.

The generating function $A(x)$ lets us give a *closed form* for a_n, through the method of partial fractions. Putting

$$F(x) = \frac{C}{1-\alpha x} + \frac{D}{1-\beta x},$$

in which α and β are the inverse roots $(1+\sqrt{5})/2$ and $(1-\sqrt{5})/2$ respectively of the denominator, we then get $C = 1/2 + 1/(2\sqrt{5})$, $D = 1/2 - 1/(2\sqrt{5})$. Now the familiar geometric series

$$\frac{1}{1-\gamma x} = \sum_{n \geq 0} \gamma^n x^n$$

yields

$$A(n) = \sum_{n \geq 0} \left(\frac{\alpha^n + \beta^n}{2} + \frac{\alpha^n - \beta^n}{2\sqrt{5}} \right) x^n.$$

A proper closed form for a_n, the nth coefficient of this series, is now at hand:

$$a_n = \frac{\alpha^n + \beta^n}{2} + \frac{\alpha^n - \beta^n}{2\sqrt{5}}.$$

For hand computation, the recurrence is less hairy than this closed form. But for *efficient* computation in the complexity sense, the closed form is superior.

Finally, let us extract the *asymptotics* of a_n. We want some easy function — a monomial in n, say, or an exponential — which grows at the same rate as a_n does. In this case, this is easy: since $|\beta| < 1$, the powers β^n tend to zero as $n \to \infty$ and can be neglected. Therefore

$$a_n \sim \frac{5+\sqrt{5}}{10} \cdot \left(\frac{1+\sqrt{5}}{2} \right)^n$$

grows exponentially.

1.2 A few words on formal power series

For any ring R and any indeterminate x, the set

$$R[[x]] = \left\{ \sum_{n \geq 0} r_n x^n : r_n \in R \right\}$$

of formal power series with coefficients in R is a ring. In this module, R will be $\mathbb{Z}$ or $\mathbb{Q}$, or else itself a ring of formal power series, the latter enabling us to use multivariate series. (An interesting choice which will not be a focus here is the representation ring of a group, or certain limits of such rings.)

The ring operations are defined as follows. the sum and product of $A = \sum_{n\geq 0} a_n x^n$ and $B = \sum_{n\geq 0} a_n x^n$ are

$$A+B = \sum_{n\geq 0} (a_n + b_n) x^n,$$
$$AB = \sum_{n\geq 0} (a_n b_0 + a_{n-1} b_1 + \cdots + a_0 b_n) x^n.$$

Note that these agree with the definitions for polynomials, i.e. the polynomial ring $R[x]$ is a subring of $R[[x]]$.

Each of these operations has a combinatorial meaning. They are enrichments of the following two basic counting principles, holding outside the series context. If there are s ways to do S and t ways to do T, then...

Addition there are $s+t$ ways to choose one of S or T, and do it.

Multiplication there are st ways to do both S and T. This holds even if the choices for T are affected by how S was done, so long as there remain t of them (or vice versa).

The addition principle transfers to series in a natural way: if every structure of a certain type is either an S or a T, and A is the generating function for Ses while B is the generating function for Ts, then $A+B$ is the generating function for the structure in question. This is what underlay the recurrence in our first example.

Multiplication of series, not being a coefficientwise operation, clearly has a combinatorial meaning which involves varying the value n of the parameter. At this point we leave as an exercise what this meaning is: bear in mind that the answer depends on whether the series are ordinary or exponential. We will return to the question later, when we will also take up the meanings of many other operations supported by formal power series, under mild conditions: multiplicative inversion, composition, differentiation, etc.

1.3 Asymptotics

We introduce the notation for describing the asymptotic behaviour of functions. Let F and G be functions of the natural number n. For convenience we assume that G does not vanish. We write

- $F = O(G)$ if $F(n)/G(n)$ is bounded above as $n \to \infty$.

- $F = \Theta(G)$ if $F(n)/G(n)$ is bounded both above and below as $n \to \infty$.
- $F = \Omega(G)$ if $F(n)/G(n)$ is bounded below as $n \to \infty$. This item of notation, due to Donald Knuth, unfortunately conflicts with an older meaning still current in number theory, which is the negation of $F = o(G)$ below.
- $F = o(G)$ if $F(n)/G(n) \to 0$ as $n \to \infty$.
- $F = \omega(G)$ if $F(n)/G(n) \to \infty$ as $n \to \infty$.
- $F \sim G$ if $F(n)/G(n) \to 1$ as $n \to \infty$.

Note the anomalous syntax of these notations: if $F = O(G)$ and $F' = O(G)$, we certainly cannot conclude $F = F'$! The expressions $O(G)$, $o(G)$, etc. sometimes appear in other contexts than to the right of an equals sign. The notation $O(G)$, to take an example, should be understood as "some function F such that $F = O(G)$", with the implication that the precise identity of this function is unimportant and not needed in the rest of the text (it is often an error term).

Typically, F is a combinatorial function which is to be understood, and G is a function assembled out of the standard toolbox of analysis: polynomials, exponentials, logarithms, and the like. We give one example here with proof, as an illustration.

Theorem 1.1 (Stirling's formula)

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n.$$

Proof Note that

$$\log(n!) = \sum_{i=1}^{n} \log i$$

which is a Riemann sum for the integral of the logarithm. Nearly the same sum arises in the approximation by the trapezium rule:

$$\begin{aligned}\int_1^n \log x \,\mathrm{d}x &= \sum_{i=1}^{n-1} \frac{\log(i) + \log(i+1)}{2} + \varepsilon \\ &= \log(n!) - \frac{1}{2}\log n + \varepsilon\end{aligned}$$

where ε is an error term governed by the second derivative $-1/x^2$ of $\log x$. To be precise, on each subinterval $[m, m+1]$, the difference between $\log(x)$ and its approximation is

$$\log x - \left(\log m + (x-m)\log(1+\frac{1}{m})\right) \leq \frac{1}{m} - \log(1+\frac{1}{m}) \leq \frac{1}{2m^2}$$

by two uses of Taylor's theorem, and the fact $x-m \leq 1$. So the total error ε is bounded by $\sum_{m=1}^{n-1} 1/2m^2$, which converges to a constant as $n \to \infty$. Since ε is itself monotonically increasing with n, we have $\varepsilon = c - o(1)$ for some constant c. On the other hand, we can integrate

$$\int_1^n \log x \, \mathrm{d}x = n \log n - n + 1$$

and conclude

$$\log n! = (n + \frac{1}{2}) \log n - n - c + o(1)$$

which exponentiates to

$$n! \sim e^c \sqrt{n} \left(\frac{n}{e}\right)^n.$$

To identify the constant $C := e^c$, we can proceed as follows. Consider the integral

$$I_n = \int_0^{\pi/2} \sin^n x \, \mathrm{d}x.$$

Integration by parts shows that

$$I_n = \frac{n-1}{n} I_{n-2},$$

and hence

$$I_{2n} = \frac{(2n)!\pi}{2^{2n+1}(n!)^2},$$
$$I_{2n+1} = \frac{2^{2n}(n!)^2}{(2n+1)!}.$$

On the other hand,

$$I_{2n+2} \leq I_{2n+1} \leq I_{2n},$$

from which we get

$$\frac{(2n+1)\pi}{4(n+1)} \leq \frac{2^{4n}(n!)^4}{(2n)!(2n+1)!} \leq \frac{\pi}{2},$$

and so

$$\lim_{n\to\infty} \frac{2^{4n}(n!)^4}{(2n)!(2n+1)!} = \frac{\pi}{2}.$$

Putting $n! \sim C\sqrt{n}(n/e)^n$ in this result, we find that

$$C^2 \frac{e}{4} \lim_{n\to\infty} \left(1 + \frac{1}{2n}\right)^{-2n-3/2} = \frac{\pi}{2},$$

so that $C = \sqrt{2\pi}$.

The last part of this proof is taken from Alan Slomson, *An Introduction to Combinatorics*, Chapman and Hall 1991. It is more or less the proof of Wallis' product formula for π.