Notes on Linear Recurrence Sequences

April 8, 2005

As far as preparing for the final exam, I only hold you responsible for knowing sections 1, 2.1, 2.2, 2.6 and 2.7.

1 Definitions and Basic Examples

An example of a linear recurrence sequence is the Fibonacci numbers $F_0, F_1, F_2, ...$, where $F_0 = 0$, $F_1 = 1$, and $F_{n+1} = F_n + F_{n-1}$ for $n \geq 2$; so, the sequence begins

$$0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8, ...$$

In general, a linear recurrence sequence $X_0, X_1, ...$ obeys the rule

$$X_n \ = \ a_0 X_{n-1} + a_1 X_{n-2} + \cdots + a_{k-1} X_{n-k} \tag{1}$$

for $n \geq k$, where $a_0, ..., a_{k-1}$ are constants. The values $X_0, ..., X_{k-1}$ are initial conditions.

An example is, say $k = 3$, $a_0 = 1$, $a_1 = 2$, $a_2 = 3$, $X_0 = 0$, $X_1 = 1$, $X_2 = 2$. This produces the recurrence relation

$$X_n = X_{n-1} + 2X_{n-2} + 3X_{n-3}.$$

So, the sequence is

$$X_0, X_1, X_2, ... \ = \ 0, 1, 2, 4, 11, 25, ...$$

2 A Formula for X_n

2.1 The Characteristic Polynomial

The simplest of all linear recurrence sequences are geometric progressions, which are defined by the rule

$$X_0 = 1,\ X_{n+1} = aX_n,$$

in other words

$$X_0, X_1, X_2, ... \ = \ 1, a, a^2, a^3, ...$$

Such a sequence has the property that

$$\frac{X_{n+1}}{X_n} \ = \ a,$$

that is, the ratio of successive terms is a.

This property (successive term ratios are constant) is not shared by the Fibonacci numbers; however, one can speculate that the ratio of successive Fibonacci numbers tends to a limit. That is, does there exist a number φ such that

$$\lim_{n\to\infty} \frac{F_{n+1}}{F_n} \ = \ \varphi \ ?$$

It turns out that the answer is YES; and, remarkably, just knowing that the limit exists is enough to find it: Indeed, if n is a very big integer, then

$$\frac{F_{n+1}}{F_n} \ \approx \ \varphi, \text{ and } \frac{F_n}{F_{n-1}} \ \approx \ \varphi.$$

Now,

$$F_{n+1} = F_n + F_{n-1} \implies \frac{F_{n+1}}{F_n} \ = 1 + \frac{F_{n-1}}{F_n}.$$

This last equation tells us that

$$\varphi \ \approx \ 1 + \frac{1}{\varphi}.$$

In fact, we get equality here by letting n tend to infinity; so,

$$\varphi^2 - \varphi - 1 \ = \ 0.$$

The limit φ is thus either

$$\frac{1+\sqrt{5}}{2}, \text{ or } \frac{1-\sqrt{5}}{2}.$$

The fact that this second ratio is negative means that it cannot be our φ; and so,

$$\varphi \ = \ \frac{1+\sqrt{5}}{2}.$$

The polynomial $f(x) = x^2 - x - 1$ is called the characteristic polynomial for F_n. More generally, if we have a sequence defined as in (1), then the characteristic polynomial is defined to be

$$x^k - a_0 x^{k-1} - a_1 x^{k-2} - \cdots - a_{k-1}. \tag{2}$$

If

$$\lim_{n\to\infty} \frac{X_{n+1}}{X_n} \text{ exists,}$$

then this limit will be a root of the polynomial (2). However, there are examples of sequences where this limit fails to exist; for example,

$$X_{n+1} \;=\; X_n - X_{n-1}, \text{ with initial conditions } X_0 = 0, X_1 = 1.$$

The sequence here is

$$X_0, X_1, X_2, ... \;=\; 0, 1, 1, 0, -1, -1, 0, 1, 1, 0, -1, -1, 0, ...$$

2.2 Using Matrices to Determine F_n

We begin with a really interesting relation:

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} F_{m+1} \\ F_m \end{bmatrix} \;=\; \begin{bmatrix} F_{m+2} \\ F_{m+1} \end{bmatrix}.$$

It is not immediately obvious what this gives us, but notice what happens if we multiply both sides by that $0-1$ matrix:

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^2 \begin{bmatrix} F_{m+1} \\ F_m \end{bmatrix} \;=\; \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} F_{m+2} \\ F_{m+1} \end{bmatrix} \;=\; \begin{bmatrix} F_{m+3} \\ F_{m+2} \end{bmatrix}.$$

In fact, if we repeat this a couple of times we get

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n \begin{bmatrix} F_{m+1} \\ F_m \end{bmatrix} \;=\; \begin{bmatrix} F_{m+n+1} \\ F_{m+n} \end{bmatrix}.$$

So, for $m = 0$ we get

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n \begin{bmatrix} 1 \\ 0 \end{bmatrix} \;=\; \begin{bmatrix} F_{n+1} \\ F_n \end{bmatrix}.$$

On the other hand, we know from linear algebra that to compute a high power of a matrix (such as our $0-1$ matrix), the task is fairly easy once we

have diagonalized. First, we must find the eigenvalues, which are determined by the characteristic polynomial: We begin by letting

$$A \;=\; \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}.$$

Then, the characteristic polynomial is

$$\begin{vmatrix} 1-\lambda & 1 \\ 1 & -\lambda \end{vmatrix} \;=\; (1-\lambda)(-\lambda) - 1 \;=\; \lambda^2 - \lambda - 1.$$

Notice that this polynomial is the characteristic polynomial we defined in the previous section!

Now, we know that

$$A \;=\; S \begin{bmatrix} \varphi & 0 \\ 0 & \varphi' \end{bmatrix} S^{-1},$$

where φ and φ' are roots of the characteristic polynomial, and where S is the matrix whose columns are eigenvectors of A corresponding to these eigenvalues φ and φ'; in fact,

$$S \;=\; \begin{bmatrix} \varphi & \varphi' \\ 1 & 1 \end{bmatrix}, \text{ and } S^{-1} \;=\; \frac{1}{\sqrt{5}} \begin{bmatrix} 1 & -\varphi' \\ -1 & \varphi \end{bmatrix}.$$

Call this diagonal matrix Λ. Then,

$$A^n \;=\; (S\Lambda S^{-1})(S\Lambda S^{-1}) \cdots (S\Lambda S^{-1}) \;=\; S\Lambda^n S^{-1} \;=\; S \begin{bmatrix} \varphi^n & 0 \\ 0 & (\varphi')^n \end{bmatrix} S^{-1}.$$

So, with a little work, we find that the second entry of the column vector

$$A^n \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

is

$$\frac{1}{\sqrt{5}} \left(\varphi^n - (\varphi')^n \right).$$

Which is a very nice formula, I hope you will agree!

2.3 A Comment about this Formula

Since

$$|\varphi'| \ < \ 1,$$

we know that as n tends to infinity, the term $(\varphi')^n$ tends to 0. So, for $n \geq 1$, we will have F_n is the nearest integer to

$$\frac{\varphi^n}{\sqrt{5}}.$$

In fact, the larger n is, the closer that this number is to an integer, which is rather strange: How many irrational numbers φ do you know of with the property that $\varphi^n/\sqrt{5}$ is always near to an integer? For example,

$$\frac{\varphi^{10}}{\sqrt{5}} \ = \ 55.003635..., \text{ and } \frac{\varphi^{13}}{\sqrt{5}} \ = \ 232.9991401....$$

It also turns out to be the case that

$$\varphi^n + (\varphi')^n \text{ is an integer,}$$

So, powers of φ should also be near to an integer. For example,

$$\varphi^{13} \ = \ 521.0019162..., \ \varphi^{16} \ = \ 2206.999531...$$

There is a general class of irrational numbers $\varphi > 1$ with the remarkable property that the powers φ^n all get closer and closer to an integer. They are called Pisot numbers.

2.4 A Formula for Special Sequences X_n

As with the Fibonacci numbers, we have that the system

$$X_{n+1} \ = \ aX_n + bX_{n-1}$$

satisfies

$$\left[\begin{array}{cc} a & b \\ 1 & 0 \end{array} \right]^n \left[\begin{array}{c} X_1 \\ X_0 \end{array} \right] \ = \ \left[\begin{array}{c} X_{n+1} \\ X_n \end{array} \right].$$

The characteristic polynomial of this matrix is the same as the characteristic polynomial for the sequence X_n we defined in a previous section.

Now, if the roots of this polynomial are distinct, then we know that A can be diagonalized, and then we get

$$\left[\begin{array}{c} X_{n+1} \\ X_n \end{array} \right] \ = \ S \left[\begin{array}{cc} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{array} \right] S^{-1}.$$

So, it is easy to see that X_n is some linear combination of λ_1^n and λ_2^n; that is,

$$X_n \;=\; A\lambda_1^n + B\lambda_2^n.$$

If the matrix cannot be diagonalized, things are more subtle.

Example. Suppose that X_n is defined by the rule

$$X_{n+1} \;=\; 3X_n - 2X_{n-1},\; X_0 = 0,\; X_1 = 1.$$

Then, the characteristic polynomial is

$$x^2 - 3x + 2,$$

which has the roots $x = 1$ and $x = 2$. So,

$$X_n \;=\; A + B2^n.$$

Setting $n = 0$, we find

$$0 \;=\; X_0 \;=\; A + B,$$

so $A = -B$; and, setting $n = 1$, we find

$$1 \;=\; X_1 \;=\; A + 2B.$$

So, $B = 1$ and $A = -1$. So,

$$X_n \;=\; 2^n - 1.$$

More generally, we may use the matrix form of an arbitrary sequence

$$X_n \;=\; a_0X_{n-1} + \cdots + a_{k-1}X_{n-k}.$$

We get

$$\begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_{k-1} \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}^n \begin{bmatrix} F_{k-1} \\ F_{k-2} \\ \vdots \\ F_0 \end{bmatrix} = \begin{bmatrix} F_{k-1+n} \\ F_{k-2+n} \\ \vdots \\ F_n \end{bmatrix}.$$

It turns out that the characteristic polynomial of this matrix equals the characteristic polynomial of the sequence X_n. Now, if the matrix can be diagonalized, as with the case of Fibonacci numbers, then the sequence must have the form

$$X_n \;=\; A_1\lambda_1^n + A_2\lambda_2^n + \cdots + A_t\lambda_t^n, \tag{3}$$

where $\lambda_1, ..., \lambda_t$ are the eigenvalues of A (Note: We may have $t < k$, because some of the eigenvalues could be repeated.)

2.5 Exceptional Sequences

There are some sequences which do not have the form (3). For example, consider the sequence

$$X_n \;=\; 4X_{n-1} - 4X_{n-2}.$$

The corresponding matrix here is

$$A \;=\; \begin{bmatrix} 4 & -4 \\ 1 & 0 \end{bmatrix},$$

which cannot be diagonalized.

2.6 Generating Functions

As before, we suppose that

$$X_n \;=\; a_0X_{n-1} + \cdots + a_{k-1}X_{n-k}.$$

Then, consider the sum

$$f(x) \;=\; \sum_{n=0}^{\infty} X_n x^n.$$

Suppose that $m \geq k$. Then, we observe that

$$\begin{aligned} f(x) &= \cdots + X_m x^m + \cdots \\ xf(x) &= \cdots + X_{m-1}x^m + \cdots \\ x^2 f(x) &= \cdots + X_{m-2}x^m + \cdots \\ &\vdots \quad \cdots + X_{m-k}x^{m-k} + \cdots \end{aligned}$$

So, then, for $m \geq k$ we find that

$$\begin{aligned} (1 - a_0x - a_1x^2 - \cdots - a_{k-1}x^k)f(x) &= \cdots + (X_m - a_0X_{m-1} - \cdots - a_{k-1}X_{m-k})x^m + \cdots \\ &= \cdots + 0x^m + \cdots. \end{aligned}$$

So, the coefficient is 0. So, we must have that

$$(1 - a_0x - a_1x^2 - \cdots - a_{k-1}x^k)f(x) \;=\; g(x),$$

where $g(x)$ is some polynomial of degree at most $k-1$. It follows that

$$f(x) \;=\; \frac{g(x)}{1 - a_0x - \cdots - a_{k-1}x^k}.$$

The polynomial on the denominator is the characteristic polynomial of the sequence X_n, written backwards (that is, the coefficients are written in reverse order). Another way of expressing this polynomial is as follows: Let

$$h(x) = 1 - a_0 x - \cdots - a_{k-1} x^k,$$

and let

$$p(x) = x^k - a_0 x^{k-1} - \cdots - a_{k-1}.$$

Then,

$$h(x) \;=\; x^k p(1/x).$$

It follows that the roots of $h(x)$ are the reciprocals of the roots of $p(x)$ (note that 0 is never a root of the polynomial).

It turns out that the generating function of a sequence X_n is a rational function $A(x)/B(x)$ if and only if X_n is a linear recurrence sequence.

2.7 The General Case

Now suppose that the characteristic polynomial $p(x)$ factors as follows

$$p(x) \;=\; (x-\lambda_1)^{\alpha_1}(x-\lambda_2)^{\alpha_2}\cdots(x-\lambda_t)^{\alpha_t},$$

where the λ_i's are all distinct, and the $\alpha_i \geq 1$. Note that

$$\alpha_1 + \cdots + \alpha_t \;=\; k.$$

Then,

$$h(x) \;=\; (1-\lambda_1 x)^{\alpha_1}\cdots(1-\lambda_t x)^{\alpha_t}.$$

So, by the theory of partial fractions, we know that there exist constants

$$A_{1,1}, ..., A_{1,\alpha_1};\;\; A_{2,1}, ..., A_{2,\alpha_2};\;\; ...;\;\; A_{t,1}, ..., A_{t,\alpha_t}$$

such that

$$f(x) \;=\; \frac{g(x)}{h(x)} \;=\; \sum_{i=1}^{t}\left(\frac{A_{i,1}}{1-\lambda_i x} + \frac{A_{i,2}}{(1-\lambda_i x)^2} + \cdots + \frac{A_{i,\alpha_i}}{(1-\lambda_i x)^{\alpha_i}}\right). \quad (4)$$

Now, the term

$$\frac{A_{i,j}}{(1-\lambda_i x)^j}$$

is the $(j-1)$st derivative of

$$\frac{A_{i,j}}{(j-1)!\lambda_i^{j-1}(1-\lambda_i x)} \;=\; \frac{A_{i,j}}{(j-1)!\lambda_i^{j-1}} \sum_{m=0}^{\infty} \lambda_i^m x^m.$$

So, the coefficient of x^m in

$$\frac{A_{i,j}}{(1-\lambda_i x)^j}$$

is just

$$\frac{A_{i,j} m(m-1)\cdots(m-j+2)\lambda_i^m}{(j-1)!},$$

(when $j=1$ this is to be $A_{i,j}$) which can be expressed as

$$q(m)\lambda_i^m,$$

where $q(m)$ is some polynomial of degree $j-1$ in m. So, the coefficient of x^m in

$$\frac{A_{i,1}}{1-\lambda_i x} + \frac{A_{i,2}}{(1-\lambda_i x)^2} + \cdots + \frac{A_{i,\alpha_i}}{(1-\lambda_i x)^{\alpha_i}}$$

is of the form

$$q_i(m)\lambda_i^m,$$

where $q_i(m)$ is some polynomial of degree at most $\alpha_i - 1$ in m. Combining this with (4), we deduce that

$$X_m \;=\; q_1(m)\lambda_1^m + q_2(m)\lambda_2^m + \cdots + q_t(m)\lambda_t^m, \tag{5}$$

where $q_i(m)$ is a polynomial in m of degree $\alpha_i - 1$.

2.8 The Non-Homogeneous Case

Before we give a non-trivial application of the formula (5) for the mth term in a general recurrence sequence, we work out the non-homogeneous case: Up until now we have been dealing with the "homogeneous case" of linear recurrence sequences, which can be described as follows: A recurrence relation of the form

$$X_n \;=\; a_0 X_{n-1} + \cdots + a_{k-1} X_{n-k}$$

can be rewritten as

$$X_n - a_0 X_{n-1} - \cdots - a_{k-1} X_{n-k} \;=\; 0.$$

The left-hand-side is linear in $X_n, ..., X_{n-k}$, with coefficients $1, -a_0, ..., -a_{k-1}$, while the right hand side is 0. This is what we mean by "homogeneous".

But now we can ask about sequences Y_n which satisfy

$$c_0 Y_n + c_1 Y_{n-1} + \cdots + c_k Y_{n-k} \;=\; Z_n, \tag{6}$$

where Z_n is some sequence.

In the case where $Z_n = c$ is a constant we can reduce the problem of finding a formula for Y_n to the homogeneous case as follows: We observe that

$$(c_0 Y_{n+1} + \cdots + c_k Y_{n-k+1}) - (c_0 Y_n + \cdots + c_k Y_{n-k}) \;=\; 0.$$

The left hand side is then a linear combination of $Y_{n-k}, ..., Y_{n+1}$; and so, we are back to the homogeneous case.

The question now becomes: Which sequences Z_n can you always reduce to the homogeneous case? And it turns out that if Z_n is itself the nth term of a homogeneous linear recurrence sequence, then the reduction goes through. Perhaps the easiest way to see this, and to deduce a formula for such sequences Y_n, is to work with generating functions.

Suppose that $f(x)$ is the generating function for X_n; that is,

$$f(x) \;=\; \sum_{n=0}^{\infty} X_n x^n.$$

Then, (6) is telling us that the coefficient of x^n in the power series expansion of

$$(c_0 + c_1 x + \cdots + c_k x^k) f(x)$$

is

$$c_0 X_n + \cdots + c_k X_{n-k} \;=\; Y_n.$$

However, this only holds for $n \geq k$, because X_m is only defined for when $m \geq 0$.

So, in general, what we get is that

$$(c_0 + c_1 x + \cdots + c_k x^k) f(x) \;=\; r(x) + \sum_{n=0}^{\infty} Y_n x^n,$$

where $r(x)$ is some polynomial of degree at most $k-1$.

Now, the power series with terms $Y_n x^n$ is just the generating function for Y_n, which we are assuming is a homogeneous linear recurrence sequuence;

and so, the generating function for Y_n is a rational function $A(x)/B(x)$ (where A and B are polynomials). It follows that

$$f(x) \;=\; \frac{r(x)}{c_0 + \cdots + c_k x^k} + \frac{A(x)}{(c_0 + \cdots + c_k x^k)B(x)},$$

which is a rational function. It follows that X_n is a homogeneous linear recurrence sequence.

2.9 An Application

Here we give a rather simpleminded application to illustrate the principles in the previous section. This application amounts to deriving a formula for

$$S_n \;=\; 1 + 2 + \cdots + n.$$

This sequence satisfies the non-homogeneous recurrence

$$S_n - S_{n-1} \;=\; n \tag{7}$$

for $n \geq 1$ (we define $S_0 = 0$).

Now, if we let

$$f(x) \;=\; \sum_{n=0}^{\infty} S_n x^n$$

be the generating function for S_n, then we observe that the relation (7) implies that

$$(1-x)f(x) \;=\; r(x) + \sum_{n=0}^{\infty} n x^n,$$

where $r(x)$ is some polynomial of degree at most 0, and so is a constant. Clearly, $r(x) = 0$. So, we have

$$f(x) \;=\; \frac{1}{1-x} \sum_{n=0}^{\infty} n x^n.$$

Now, we know that

$$\frac{1}{1-x} \;=\; \sum_{n=0}^{\infty} x^n;$$

and so, differentiating term-by-term we have that

$$\frac{1}{(1-x)^2} \;=\; \sum_{n=1}^{\infty} n x^{n-1}.$$

So,

$$\frac{x}{(1-x)^2} \;=\; \sum_{n=0}^{\infty} nx^n$$

It follows that

$$f(x) \;=\; \frac{x}{(1-x)^3}.$$

Now, to get a formula for the coefficient of x^n in this sequence, we observe that by differentiating $1/(1-x)^2$ term-by-term, we get

$$\frac{2}{(1-x)^3} \;=\; \sum_{n=0}^{\infty} n(n-1)x^{n-2}.$$

So,

$$\frac{x}{(1-x)^3} \;=\; \sum_{n=0}^{\infty} \frac{n(n+1)}{2}x^n,$$

and it follows that

$$S_n \;=\; \frac{n(n+1)}{2},$$

as is well known.

3 Linear Recurrence Sequences and Finite State Machines

It turns out that these recurrence relations are intimately related to regular grammars and finite state machines; however, there is a fair amount of background which is necessary in order to say much about this. Here, we will be content just to describe this connection in a very special case, namely where X_n is the Fibonacci sequence.

We begin by reminding ourselves of the following basic fact about Fibonacci numbers:

Theorem 1 *The number of length n strings of 0's and 1's containing no consecutive 1's is F_{n+2}. For example, in the case $n = 3$, the strings are 000,100,010,001, and 101, of which there are 5; and, indeed, $F_{n+2} = F_5 = 5$*

For completeness, we give here the induction proof of this result:

Proof. The claim is clearly true for $n = 0$ and $n = 1$. For $n = 0$, there is only one string, namely the empty string, and, indeed, $F_{0+2} = F_2 = 1$. For $n = 1$ there are two strings, namely 0 and 1, and $F_{1+2} = F_3 = 2$.

Suppose, for proof by mathematical induction that the claim holds for all $0 \leq n \leq k$, where $k \geq 1$. Now consider the collection of all strings of length $k+1$ of 0's and 1's with no consecutive 1's. We can divide this set of strings into two groups, according to whether the $(k+1)$st character is a 0 or a 1: If the $(k+1)$st character is a 0, then the first k characters can be any string with no consecutive 1's, and there are F_{k+2} such strings. If the $(k+1)$st character is a 1, then the kth character must be a 0 in order to avoid consecutive 1's, and then the first $k-1$ characters can be anything so long as there are no consecutive 1's; so, there are $F_{k-1+2} = F_{k+1}$ possibilities for these first $k-1$ characters. In total, the number of length $k+1$ strings is $F_{k+1} + F_{k+2} = F_{k+3} = F_{(k+1)+2}$; and so the induction step is proved, and the claim holds by mathematical induction. ■

Now we give a proof based on finite state machines: The set of strings of 0's and 1's without consecutive 1's is an example of what is called a *language* in theoretical computer science, where $\Sigma = \{0, 1\}$ is the *alphabet*. Moreover, this language is special in that it can be recognized by a finite state machine. Such languages are said to be *regular*.

Basically, a finite state machine is a graph, together with a pointer pointing to a certain location in the string, and a state variable which indicates which state the machine is in. The vertices in the graph represent states and at a given instant in time the machine is said to have state variable equal to one of these vertices. The edges in the graph are directed, and each edge corresponds to a character in the alphabet; thus, leading out of each vertex in the graph there can be at most $|\Sigma|$ edges (assuming that the machine is what is called *deterministic*, which we will assume). The states of the graph are designated one of three types: a start state, some halt states, and normal states. The machine's state variable will change as the characters in the string are read, and each time that a character is "read", the pointer advances one position to the right in the string. The pointer never goes to the left. By the time the pointer reaches the last character in the string, if the state variable equals one of these halt vertices, then the machine halts and says "This string is in the language"; and if, by the time the pointer reaches the end of the string the machine's state variable is not equal to one of these halt vertices, then the machine reports "This string is not in the language".

Technically, each vertex should have exactly $|\Sigma|$ edges leading out of it, one for each possible character in the alphabet. For our definition of a finite state machine, we allow vertices that do not have a full set of $|\Sigma|$ edges leading away from them. If the machine happens to be in one of these

underfull states, and if the next character that the pointer points to does not correspond to one of these $< |\Sigma|$ edges, then our machine halts, and reports that the string is not in the language, no matter if the state the machine is in a halt state.

Now, a machine (in our sense) for generating strings of 0's and 1's without consecutive 1's can be described by two states, both of which are halt states, and one is (of course) a start state. The start vertex we label A, and the other vertex we label B. The edges for this graph are as follows: There is an edge leading from vertex A to itself, which corresponds to the character 0; there is an edge leading from vertex A to vertex B, which corresponds to the character 1; and, there is an edge leading from vertex B back to vertex A, which corresponds to the character 0.

Let us now see what happens if the machine is fed a string with consecutive 1's: Say the string is 11. The machine starts in state A, and when it reads that first one, it transitions to state B, and the pointer advances so that it is over that second 1. Then, when the machine reads that second 1, there is nowhere that it can go, because there is only one edge leading away from vertex B, and that edge corresponds to the character 0. So, the machine halts, and reports that the string is not in the language.

Consider now what happens if the string is 011. In this case, when the machine reads that first 0, it transitions from state A back to state A; and then, when it reads that 11, it will end up halting in state B and reporting that the string is not in the language.

We now count the number of strings of length n that are in the language: This is the number of paths of length n from vertex A to itself plus the number of paths of length n from vertex A to vertex B. Here a path means a sequence like $ABAAB$, which means that we transition from vertex A to vertex B, and then from B to A, and from vertex A to vertex A, and finally from vertex A to vertex B. The length of this path is 4, because we transition along 4 edges.

Now, as we know, the number of paths of length n from one vertex to another is some entry in the power of an adjacency matrix. In our case, the adjacency matrix is

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix},$$

where the entry in the ith row and jth column is 1 if and only if there is an edge leading from vertex i to vertex j. Then, the $A^k_{i,j}$ equals the number of paths of length k from vertex i to vertex j. We are interested in

$$A^k_{1,1} + A^k_{1,2},$$

which is the sum of the entries in the first row of A^k.

As we know,

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^k \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} F_{k+1} \\ F_k \end{bmatrix},$$

which is telling us that the first column of A^k has entries F_{k+1} and F_k. Since the matrix A is symmetric (that is, A equals its transpose), we know then that the first row equals $[F_{k+1}\ F_k]$. So, the number of strings of length n in our language, which is the sum of the entries in the first row of A^n, is

$$F_{n+1} + F_n = F_{n+2}.$$

We state here a general result without proof:

Theorem 2 *Suppose that $\mathcal{L}$ is a regular language with some finite alphabet Σ. Then, there exist numbers $\lambda_1, ..., \lambda_k$ and polynomials $p_1(x), ..., p_k(x)$ such that the number of strings of length n lying in $\mathcal{L}$ is given by*

$$p_1(n)\lambda_1^n + p_2(n)\lambda_2^n + \cdots + p_k(n)\lambda_k^n.$$

This puts heavy restrictions on the structure of regular languages, and in the next section we will use it to give an alternative (sketch of a) proof of a classic result on balanced parentheses.

3.1 An Application to Automata Theory

One of the classic results from theoretical computer science concerning regular grammars (rules which generate regular languages) is that the language of balanced parentheses is not regular; that is, there is no finite state machine which can decide whether or not a string of ('s and)'s is balanced. By "balanced" here we mean, for example ((()())()). An example of a string which is not balanced is (()(.

Now, as we know, the number of balanced parentheses of length $2k$ is the Catalan number

$$C_k = \frac{1}{k+1}\binom{2k}{k}.$$

Using Stirling's formula (which gives an asymptotic formula for $n!$), one can prove that

$$\binom{2k}{k} \sim \frac{2^{2k}}{\sqrt{\pi k}}.$$

This means that

$$\lim_{k\to\infty} \frac{\binom{2k}{k}}{2^{2k}/\sqrt{\pi k}} \;=\; 1.$$

So,

$$C_k \;\sim\; \frac{2^{2k}}{k\sqrt{\pi k}}.$$

It turns out that this cannot have the form given by Theorem 2, because $1/k\sqrt{k\pi}$ does not grow like a polynomial. [1]

Thus, the language of balanced parentheses is not regular.

4 An Algebraic Combinatorial Interpretation of Second Order Linear Recurrence Sequences

We give here a way to interpret general second order linear recurrence sequences in terms of strings. Basically, we generalize the result connecting F_{n+2} to n length strings. But how?

The idea is to look at formal sums of strings of α's and β's, containing no consecutive α's, where we do not apply commutativity of multiplication. For example, consider the formal "sum" of strings of length 3 of such strings: We get

$$\beta\beta\beta + \alpha\beta\beta + \beta\alpha\beta + \beta\beta\alpha + \alpha\beta\alpha.$$

Note that there are five terms in this formal sum. Now suppose that X_{n+2} is the formal sum of all such strings of length n, where we define $X_0 = 0$, $X_1 = 1$, and $X_2 = \beta$. Then, we see that

$$X_3 \;=\; \alpha + \beta,\; X_4 \;=\; \beta\beta + \alpha\beta + \beta\alpha,$$

and so on.

Now we address the following question: If we are given the formal sums $X_0, ..., X_n$, how can be construct the formal sum X_{n+1}?

The idea is as follows: A string of α's and β's of length n has nth character either equal to β or equal to α. If the nth character is β, then the first $n-1$ characters can be any combination of α's and β's without consecutive α's; so, the formal sum of all these strings ending in β is $X_{n-3}\beta$.

[1] Actually, things are a little more complicated, because even though $2^{2k}/k\sqrt{\pi k}$ cannot be a single term $p(2k)\lambda^{2k}$, where $p(x)$ is a polynomial, it still could be the sum of several terms of this form; however, with more work one can show that C_k cannot be a sum of such terms.

If the nth character is α, then the $(n-1)$st character must be β, and the first $n-2$ characters then can be anything, so long as there are no consecutive α's; so, the formal sum of strings ending in α is $X_{n-4}\beta\alpha$. So, the formal sum of all strings of length n of α's and β's, no consecutive α's, is

$$X_{n-3}\beta + X_{n-4}\beta\alpha.$$

However, from the way we defined the sequence X_n, we must have that this also equals X_{n-2}. So, we have that

$$X_{n-2} \;=\; X_{n-3}\beta + X_{n-4}\beta\alpha;$$

or

$$X_{n+1} \;=\; X_n\beta + X_{n-1}\beta\alpha. \tag{8}$$

Now the idea is to think of β and $\beta\alpha$ as numbers, rather than just characters. So, if we have a sequence

$$X_{n+1} \;=\; c_0X_n + c_1X_{n-1},$$

we can solve for α and β so as to put this into the form (8); in fact,

$$\beta \;=\; c_0, \text{ and } \alpha \;=\; \frac{c_1}{c_0}.$$

(Here we assume $c_0 \neq 0$.) So, this general recurrence can be interpreted as a formal sum of strings of α's and β's much the same way that Fibonacci numbers can be interpreted as counting certain strings of length n composed of 0's and 1's.

There is a problem, though, and that is that we have the initial conditions $X_0 = 0$ and $X_1 = 1$, and it would be good to have an interpretation for arbitrary initial conditions. Well, there is a way to do this, but we will not bother with it here, and will be content with what we already have.

There is also a way to interpret (8) in terms of finite state machines; basically, X_n corresponds to certain weighted paths through some graph.

5 Exponential Generating Functions

It turns out that not only is there a nice form for the generating function of a sequence X_n, but there is also a nice form for the exponential generating function. Recall that the exponential generating function for a sequence X_n is defined to be

$$E(x) \;=\; \sum_{n=0}^{\infty} \frac{X_n}{n!}x^n.$$

Let us start with the Fibonacci numbers. From the equation

$$F_n \;=\; \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right),$$

one can easily deduce that its corresponding exponential generating function is

$$\frac{1}{\sqrt{5}}\left(e^{\varphi x} - e^{\varphi' x}\right),$$

where

$$\varphi \;=\; \frac{1+\sqrt{5}}{2}, \text{ and } \varphi' \;=\; \frac{1-\sqrt{5}}{2}.$$

It turns out that all linear recurrence sequence have exponential generating functions which have a similar form to this; however, there is a much nicer way of expressing it, than just as a sum of exponentials. In fact, one can express it as a single exponential! To do this, we need to define the exponential of a matrix: Given an $n \times n$ matrix A, we define e^{Ax} to be a certain $n \times n$ matrix (here, x is a variable [scalar], not a column vector):

$$e^{Ax} \;=\; I + Ax + \frac{A^2}{2!}x^2 + \frac{A^3}{3!}x^3 + \cdots,$$

where I denotes the $n \times n$ identity matrix. This matrix exponential satisfies a number of properties, and here are a few of them

(i) If we let $\mathbf{O}$ denote a zero matrix, then $e^{\mathbf{O}x} = I$, the $n \times n$ identity matrix.

(ii) If A and B are $n \times n$ matrices, then e^{Ax} and e^{Bx} are $n \times n$ matrices, and their product is $e^{Ax}e^{Bx} = e^{(A+B)x}$.

(iii) For any matrix A, e^{Ax} is an invertible matrix, as its inverse is e^{-Ax}. This is an easy consequence of (i) and (ii).

(iv) $\frac{d}{dx}e^{Ax} = Ae^{Ax}$.

Now, in the case of Fibonacci numbers, we have that F_n is the the $2,1$ entry of the matrix

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n.$$

One can show then that the exponential generating function for F_n is the $2,1$ entry of the matrix e^{Ax}.

More generally, suppose that

$$X_n \;=\; c_0 X_{n-1} + \cdots + c_{k-1}X_{n-k}.$$

Then, the exponential generating function for X_n turns out to be

$$[0\ 0\ \cdots\ 0\ 1]e^{Ax}\begin{bmatrix} X_{k-1} \\ X_{k-2} \\ \vdots \\ X_0 \end{bmatrix},$$

where

$$A\ =\ \begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_{k-2} & c_{k-1} \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix}.$$

6 The Irrationality of $e^{\sqrt{2}}$

The exponential generating function for the Fibonacci numbers

$$\frac{e^{\varphi x}}{\sqrt{5}} - \frac{e^{\varphi' x}}{\sqrt{5}} \tag{9}$$

has the property that the coefficients of powers of x in are rational numbers. Here we will use a similar fact about $e^{\sqrt{2}}$ to prove that it is irrational!

Let us begin by reviewing the proof that e is irrational: If e were rational, say $e = p/q$, then $q!e = (q-1)!p$ is an integer. But, since

$$e\ =\ 2 + \frac{1}{2} + \frac{1}{3!} + \frac{1}{4!} + \cdots,$$

we have that

$$q!e\ =\ q!\left(2 + \frac{1}{2} + \frac{1}{3!} + \cdots + \frac{1}{q!}\right) + q!\left(\frac{1}{(q+1)!} + \frac{1}{(q+2)!} + \cdots\right).$$

Now,

$$q!\left(2 + \frac{1}{2} + \frac{1}{6} + \cdots + \frac{1}{q!}\right)\ \text{is an integer,}$$

and

$$\begin{aligned} q!\left(\frac{1}{(q+1)!} + \frac{1}{(q+2)!} + \cdots\right) &= \frac{1}{q+1} + \frac{1}{(q+1)(q+2)} + \frac{1}{(q+1)(q+2)(q+3)} + \cdots \\ &< \frac{1}{q+1} + \frac{1}{(q+1)^2} + \frac{1}{(q+1)^3} + \cdots \end{aligned}$$

$$\begin{aligned} &\leq \quad \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots \\ &= \quad 1. \end{aligned}$$

So,

$$q!e \;=\; I + \delta,$$

where I is an integer, and $0 < \delta < 1$. So, $q!e$ cannot be an integer, and we conclude that e is irrational.

Now we repeat the argument for $e^{\sqrt{2}}$. We begin by observing that if $e^{\sqrt{2}}$ is rational, then so is $e^{-\sqrt{2}}$ (being the reciprocal of $e^{\sqrt{2}}$). So, if $e^{\sqrt{2}}$ is rational, so is

$$\begin{aligned} e^{\sqrt{2}} + e^{-\sqrt{2}} \quad &= \quad \sum_{n=0}^{\infty} \frac{(\sqrt{2})^n + (-\sqrt{2})^n}{n!} \\ &= \quad 2 \sum_{m=0}^{\infty} \frac{2^m}{(2m)!}. \end{aligned}$$

Next, we want to see how many power of 2 divide $(2m)!$. We begin by letting $w(n)$ denote the number of times that 2 divides n; so, $2^{w(n)}$ divides 2, but $2^{w(n)+1}$ does not divide 2. Then, there is a simple, but useful formula for $w(n)$: We have that

$$w(n) \;=\; \sum_{\substack{j \geq 1 \\ 2^j | n}} 1.$$

The power to which 2 divides $n!$, then, is

$$\sum_{h=1}^{n} w(h) \;=\; \sum_{h=1}^{n} \sum_{\substack{j \geq 1 \\ 2^j | h}} 1 \;=\; \sum_{j \geq 1} \sum_{\substack{h \leq n \\ 2^j | h}} 1 \;=\; \sum_{j \geq 1} \left\lfloor \frac{n}{2^j} \right\rfloor.$$

We note that this last sum over j is actually a finite sum, because for j sufficiently large $n/2^j$ will be less than 1, and therefore $\lfloor n/2^j \rfloor = 0$.

So, 2 divides $(2m)!$ about

$$\sum_{j \geq 1} \frac{2m}{2^j} \;=\; 2m$$

times. With a little bit of work, one can show that, more precisely, if $t(n)$ is the number of times that 2 divides $n!$, then

$$n - \ell - 1 \;\leq\; t(n) \;\leq\; n - 1,$$

where ℓ is the unique integer satisfying

$$2^{\ell-1} \ < \ n \ \leq \ 2^{\ell}.$$

When $n = 2^{\ell}$ the upper bound $t(n) = n - 1$ attained, and when $n = 2^{\ell} - 1$ the lower bound $t(n) = n - \ell - 1$ is attained.

It turns out that this implies (with some work) that for $n = 2^{\ell} - 1$,

$$\frac{(2m)!}{2^m} \text{ divides } \frac{(2n)!}{2^n},$$

for all integers $m \leq n$. Thus, if we let

$$I \ = \ \frac{(2n)!}{2^n} \sum_{m \leq n} \frac{1}{(2m)!/2^m}, \tag{10}$$

then I is an integer.

To show that

$$\frac{e^{\sqrt{2}} + e^{-\sqrt{2}}}{2} \ = \ \sum_{m=0}^{\infty} \frac{1}{(2m)!/2^m},$$

cannot be rational, it suffices to show that for infinitely many $j \geq 1$, if we let $n = 2^j - 1$, then

$$\frac{(2n)!}{2^n} \left(\frac{e^{\sqrt{2}} + e^{-\sqrt{2}}}{2} \right) \ = \ I + \delta$$

is not an integer, where I is as in (10), and where

$$\delta \ = \ \frac{(2n)!}{2^n} \sum_{m=n+1}^{\infty} \frac{2^m}{(2m)!}.$$

Thus, we just need to show that δ is not an integer: We have that

$$\delta \ = \ \frac{2}{n+1} + \frac{4}{(n+1)(n+2)} + \frac{8}{(n+1)(n+2)(n+3)} + \cdots \ < \ \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots \ = \ 1$$

for $n \geq 3$. So, δ is not an integer for $\delta \geq 3$, and we conclude that $e^{\sqrt{2}}$ is irrational.