Introduction to the theory of computation
week 4

21st June 2005

Fibonacci sequence

Last week we looked briefly at a recursively-defined function that came from the world of applied rabbit-breeding:

$$F(n) = \begin{cases} 0, & n = 0 \\ 1, & n = 1 \\ F(n-2) + F(n-1), & n > 1 \end{cases}$$

This allowed Fibonacci and his colleagues to calculate $F(n)$, the number of breeding pairs of rabbits after n breeding periods, if they began with 0 and 1 breeding pairs, respectively, during the 0th and 1st breeding periods.[1] The Fibonacci sequence is full of patterns and connections. For example:

Claim: Let $P(n)$ be "$\sum_{i=0}^{n} F(i) = F(n+2) - 1$." Then, for all $n \in \mathbf{N}$, $P(n)$.[2]

Here's another pattern in the Fibonacci sequence.

Claim: Let $P(n)$ be "$\sum_{i=0}^{n} F(2i+1) = F(2(n+1))$." Then $P(n)$ is true for all $n \in \mathbf{N}$.[3]

Notice that in the induction step of both proofs I used the recursive definition of $F(n)$, so I had to reassure myself that the value of n I was using was greater than 1, so that the recursive definition applied.

Counting strings

Suppose you want to know how many binary strings of length n do not have adjacent zeros. You could probably use combinatorial methods (if you had learned them) to work this out, but you would need to either prove (or have other reason to believe) those identities. Another approach is to use a recursive formula to count the number of eligible strings of each length.

Clearly the number of strings of length 0 without adjacent 0s is 1 (considering the empty string to be a string in its own right turns out to be useful). How many strings of length 1 are there without adjacent 0s?[4] If $n > 1$ there are 2 cases to consider: does the string end in 1 or 0? Each eligible string ending in 1 corresponds to a string of length $n-1$ that has no adjacent 0s. Each eligible string ending in 0 corresponds to a string of length $n-2$ with the suffix 10 added. Putting these ideas together gives us

$$G(n) = \begin{cases} 1, & n = 0 \\ 2, & n = 1 \\ G(n-2) + G(n-1), & n > 1 \end{cases}$$

That looks something like that Fibonacci sequence, just with different starting values. What is $G(n)$ in terms of $F(n)$? It is possible to establish, using induction, the seemingly self-evident fact that $G(n)$ is defined for every $n \in \mathbf{N}$, and that it counts the number of strings of length n that have no adjacent 0s.

You could write a computer program to calculate $G(n)$ or $F(n)$ simply by dealing with the cases $n = 0$ and $n = 1$ and then calculating the higher values iteratively. It may seem inconvenient that in order to find the the value of $G(387)$ you must first find the value of $G(n)$ for every $0 \leq n < 387$, but this is just a linear computation for a computer. Here is a much better paper-and-pencil approach for $F(n)$ (the Fibonacci sequence), which you can probably adapt to $G(n)$.

Closed form for $F(n)$

The course notes, on pages 79–80, prove that

$$F(n) = (\phi^n - \hat{\phi}^n)/\sqrt{5},$$

... where $\phi = (1+\sqrt{5})/2$ and $\hat{\phi} = (1-\sqrt{5})/2$. The notes prove this using induction, and it is worth your while to read over the proof. However, you are probably left with a nagging question: how in the world did anyone ever come up with the original conjecture about $F(n)$ involving ϕ and $\hat{\phi}$?

The terms for $F(n)$ satisfy the recurrence relation $F(n) = F(n-1) + F(n-2)$, and empirically they seem to increase by some geometric ratio r, somewhere between 1.5 and 2. Now we operate in wild conjecture mode and wonder whether there is some number r that satisfies $r^n = r^{n-1} + r^{n-2}$. Numbers have nice properties, including divisibility, so if we had such an r, then

$$r^2 = r + 1.$$

This is a quadratic formula, and you can solve it for 2 real roots: $r_0 = (1+\sqrt{5})/2$ and $r_1 = (1-\sqrt{5})/2$. Both r_1 and r_2 satisfy our original recurrence relation, as will any linear combination:

$$\begin{aligned} r_0^n + r_1^n &= r_0^{n-1} + r_1^{n-1} + r_0^{n-2} + r_0^{n-2} \\ \alpha r_0^n &= \alpha r_0^{n-1} + \alpha r_0^{n-2} \\ \alpha r_0^n + \beta r_1^n &= \alpha r_0^{n-1} + \beta r_1^{n-1} + \alpha r_0^{n-2} + \beta r_1^{n-2}. \end{aligned}$$

This give us enough degrees of freedom to match $\alpha r_0^n + \beta r_1^n$ to our initial data, $F(0) = 0$ and $F(1) = 1$:

$$\begin{aligned} \alpha r_0^0 + \beta r_1^0 = 0 &\Rightarrow \alpha = -\beta \\ \alpha r_0^1 + \beta r_1^1 = 1 &\Rightarrow \alpha(r_0 - r_1) = 1 \Rightarrow \alpha = \frac{1}{\sqrt{5}}, \beta = -\frac{1}{\sqrt{5}}. \end{aligned}$$

Your solution ensures that $\alpha r_0^n + \beta r_1^n$ matches $F(n)$ when n is either 0 or 1, and since this linear combination satisfies the recurrence relation, we know that it matches $F(n)$ for $n > 1$ as well. The same r_1 and r_2 must work for $G(n)$, but α and β will be different.

Defining sets by induction

One way to define the natural numbers is as the SMALLEST set that satisfies these two conditions:

1. $0 \in \mathbf{N}$
2. if $t \in \mathbf{N}$, then $t + 1 \in \mathbf{N}$.

Many sets satisfy these two conditions,[5] but since (according to the principle of induction) any set that satisfies these conditions contains $\mathbf{N}$, from a set-containment point-of-view $\mathbf{N}$ is the smallest set that does so: no proper subset of $\mathbf{N}$ has these two properties. Another way of saying the same thing is that $\mathbf{N}$ is the intersection of all the sets that satisfies these two conditions.

If that seems like a lot of trouble just to define $\mathbf{N}$, consider this approach to defining the set of well-formed arithmetic expressions involving x, y, and z (see example 4.1 in the Course Notes).

DEFINITION: Let E be the smallest set that satisfies:

BASIS: $x, y, z \in E$.

INDUCTION STEP: If $e_1, e_2 \in E$, then the following four expressions are also in E:

1. $(e_1 + e_2)$
2. $(e_1 - e_2)$
3. $(e_1 \times e_2)$
4. $(e_1 \div e_2)$

You must have the requirement that E be the smallest set that satisfies the basis and induction step, otherwise all sorts of extraneous elements such as $-w$ might find their way into E.

A reasonable thing to worry about is whether this sort of definition really defines a set, or just defines ways of augmenting the simplest elements that never really converges to a set. There are a couple of theorems to counteract this worry. One show the existence of a set defined this way by converging to it from the outside (see Theorem 4.2 in the Course Notes).

THEOREM: Let S' be a set, B be a subset of S', m be some positive integer with $f_1, \ldots, f_m$ operators on S' with arity $k_1, \ldots, k_m$. Then there is a unique subset $S \subset S'$ that satisfies

1. $B \subset S$
2. S is closed under $f_1, \ldots, f_m$
3. $S \subset S''$ for any $S'' \subset S'$ that satisfies the first two conditions.

In this theorem, B is the set containing the simplest elements, and operators $f_1, \ldots, f_m$ are the rules for building new elements from old. The set S' is chosen big enough to be closed under all the f_i, and then we are guaranteed a unique smallest set S that satisfies our definition. To prove this, let S be the intersection of every S'' that satisfies 1 and 2, and it's easy to show that S then satisfies all three conditions.

In our example of well-formed expressions over x, y, and z our simplest set $B = \{x, y, z\}$, our largest set S' could be the set of all possible strings over the alphabet $\{x, y, z, +, \times -, \div (,)\}$ and we had $m = 4$ binary operators: $\text{Plus}(e_1, e_2) = (e_1 + e_2)$, $\text{Minus}(e_1, e_2) = (e_1 - e_2)$, $\text{Times}(e_1, e_2) = (e_1 \times e_2)$, and $\text{Div}(e_1, e_2) = (e_1 \div e_2)$.The theorem above guarantees that there is a unique smallest set that is closed under Plus, Minus, Times, and Div that also contains B.

The theorem just given proves the existence of a set S, but it seems a bit unsatisfying, we don't feel we know a lot about S. An equivalent construction builds S by enlarging the basis set B, as follows.

$$\begin{aligned} S_0 &= B \\ S_1 &= S_0 \cup \{f_i(a_1, \ldots, a_{k_i}) : (a_1, \ldots, a_{k_i}) \in S_0, 1 \le i \le m\} \\ &\vdots \\ S_n &= S_{n-1} \cup \{f_i(a_1, \ldots, a_{k_i}) : (a_1, \ldots, a_{k_i}) \in S_{n-1}, 1 \le i \le m\} \end{aligned}$$

Then $\cup_{i \in \mathbf{N}} S_i$ (the infinite union of the S_i) is the smallest subset of S' that contains B and is closed under $f_1, \ldots, f_m$.

Constructing sets inductively allows us to use induction on them. This flavour of induction is called STRUCTURAL INDUCTION. Use the set of well-formed arithmetics expressions over $\{x, y, z\}$ (see above) as an example, and denote the number of instances of the variables x, y, z in the expression e as $\mathbf{vr}(e)$, and the number of instances of operators from $\{+, -, \times \div\}$ in e as $\mathbf{op}(e)$. Try out a few and you might try to prove the following predicate:

CLAIM: Let $P(e)$ be "$\mathbf{vr}(e) = \mathbf{op}(e) + 1$." Then $\forall e \in E, P(e)$.

PROOF (STRUCTURAL INDUCTION ON e): Suppose e is defined in the basis. Then $e \in x, y, z$, so $\mathbf{vr}(e) = 1$ and $\mathbf{op}(e) = 0$, so the claim holds for the basis.

INDUCTION STEP: Assume $P(e_1)$ and $P(e_2)$ are true for arbitrary expressions e_1 and $e_2 \in E$, and that $e = e_1 \oplus e_2$, where $\oplus \in \{+, -, \times \div\}$. Observe that the number of variables in e is the sum of the number of variables in e_1 and e_2, while e has one more operator than the sum of the number of operators in e_1 and e_2, so

$$\begin{aligned} \text{by observation above} \quad \mathbf{vr}(e) &= \mathbf{vr}(e_1) + \mathbf{vr}(e_2) \\ \text{by IH} \quad &= \mathbf{op}(e_1) + 1 + \mathbf{op}(e_2) + 1 \\ \text{by observation above} \quad &= \mathbf{op}(e) + 1 \end{aligned}$$

Thus $P(e_1)$ and $P(e_2)$ imply $P(e)$, so the induction step preserves the claim.
I conclude that $P(e)$ is true for all $e \in E$. QED.

Notes

[1] And other useful quantities, such as the maximum depth of an AVL tree with n nodes.

[2] Proof (induction on n): If $n = 0$, then $P(n)$ asserts that the sum $F(0) = 0 = F(2) - 1 = 1 - 1$, which is clearly true so the base case $P(0)$ holds.

Inductive step: For some arbitrary natural number n, assume $P(n)$. I must now show that $P(n) \Rightarrow P(n+1)$. The sum $\sum_{i=0}^{n+1} F(i)$ can be broken up into two terms:

$$\begin{aligned} \sum_{i=0}^{n+1} F(i) &= \left(\sum_{i=0}^{n} F(i)\right) + F(n) \\ \text{by IH} \qquad &= F(n+2) - 1 + F(n+1) \\ \text{by defn of } F(n+3), n+3 > 1 \qquad &= F(n+3) - 1 \end{aligned}$$

This is exactly what $P(n+1)$ claims, so $P(n) \Rightarrow P(n=1)$.
I conclude that $P(n)$ is true for all $n \in \mathbf{N}$. QED.

[3] Proof (induction on n): Suppose $n = 0$, then $P(0)$ claims that the sum $F(1) = F(2)$, which is true since (by definition) $F(1) = F(2) = 1$. Thus the base case $P(0)$ holds.

Induction step: For some arbitrary natural number n assume $P(n)$. I must show that this implies $P(n+1)$. The sum $\sum_{i=0}^{n+1} F(2i+1)$ can be broken up into two terms, and then the IH and the definition of $F(n)$ can be applied:

$$\begin{aligned} \sum_{i=0}^{n+1} F(2i+1) &= \left(\sum_{i=0}^{n} F(2i+1)\right) + F(2(n+1)+1) \\ \text{by IH} \qquad &= F(2(n+1)) + F(2n+3) \\ \text{by defn of } F(2n+4), 2n+4 > 1 \qquad &= F(2n+4) = F(2(n+1+1)) \end{aligned}$$

This is exactly what $P(n+1)$ claims, so $P(n) \Rightarrow P(n+1)$.
I conclude that $P(n)$ is true for all $n \in \mathbf{N}$. QED.

[4] Two — 0 and 1.

[5] $\mathbf{Z}, \mathbf{R}$, and $\mathbf{C}$ do, as does any superset of $\mathbf{N}$.