Math Club Notes: 2007 February 28

1 How many multiplications to evaluate a determinant?

A question on my CMPUT 204 (Algorithms) midterm explained how to evaluate a determinant by using the Laplace expansion along the first row to reduce the problem to evaluating some determinants of smaller order. We were asked to formulate a recurrence for a_n, the number of multiplications needed to compute an $n \times n$ determinant by this method.[1]

To compute one of the $(n-1) \times (n-1)$ subdeterminants involves a_{n-1} multiplications. There are n subdeterminants (one for each entry in the first row), so that's na_{n-1} multiplications. Then we have to multiply each of those subdeterminants by the corresponding entry in the first row, which is another n multiplications.

(We have to negate some of the subdeterminants; we don't count that because negation is a much faster operation than multiplying, on conventional hardware at least.)

So we have the following recurrence:

$$\begin{aligned} a_1 &= 0\,, \\ a_n &= na_{n-1} + n \qquad \text{for } n \geq 2. \end{aligned}$$

(Of course, computing a 1×1 determinant involves no multiplications at all.)

The midterm also asked us what we can say about the order of growth of a_n relative to $n!$. All they wanted us to do was to note that, since $a_n > na_{n-1}$, we expect that $a_n > n!$ for sufficiently large n. More formally:

> For $n = 3$, we have
>
> $$a_3 = 3a_2 + 3 = 3(2a_1 + 2) + 3 = 9 > 6 = 3!\,.$$
>
> If $n \geq 4$ and $a_{n-1} > (n-1)!$, then
>
> $$a_n = na_{n-1} + n > n(n-1)! + n = n! + n > n!\,.$$
>
> By induction, $a_n > n!$ for all $n \geq 3$.

A glance at the first few values confirms that we haven't made some stupid error:

n	1	2	3	4	5	6	7
$n!$	1	2	6	24	120	720	5040
a_n	0	2	9	40	205	1236	8659
$2n!$	2	4	12	48	240	1440	10080

[1] There are more efficient ways to evaluate determinants; the point is to analyze this one.

It turns out, as the third row of the table suggests, that we also have $a_n < 2n!$ for all $n \geq 1$. They didn't expect us to notice or prove this on the midterm, so we had a look at it in Math Club instead.

1.1 Attempt 1: Induction

First we tried to repeat what worked so well for proving $a_n > n!$.

For $n = 1$, we have

$$a_1 = 0 < 2 = 2 \cdot 1! \,.$$

If $n \geq 2$ and $a_{n-1} < 2(n-1)!$, then

$$a_n = n a_{n-1} + n < 2n(n-1)! + n = 2n! + n \ldots$$

Curses.

1.2 Attempt 2: Induction again

Maybe, we thought, we can repair the inductive proof by proving something slightly stronger[2] than $a_n < 2n!$, something that looks like $a_n \leq 2n! - b_n$. To figure out what b_n should be, let's just write out the inductive step, and see what we need.

If $a_{n-1} \leq 2(n-1)! - b_{n-1}$, then

$$a_n = n a_{n-1} + n \leq n(2(n-1)! - b_{n-1}) + n = 2n! - n b_{n-1} + n \ldots$$

and at this point we want to write "$= 2n! - b_n$", since the point of the inductive step is to show $a_n \leq 2n! - b_n$. So we want b_n to be such that

$$2n! - n b_{n-1} + n = 2n! - b_n \,.$$

Simplifying and rearranging, we want

$$b_n = n b_{n-1} - n \,.$$

Hm. We had hoped that the condition on b_n would tell us what the b_n have to be, but the condition turned out to be very much the same kind of thing as the recurrence we were trying to analyze in the first place.

[2] We've seen this idea of strengthening the inductive hypothesis before: see the first section of our notes for 2006 February 9.

1.3 A solution

We didn't notice this in our meeting, but it turns out it *is* easier to find suitable b_n, since in fact we only need $b_n \le nb_{n-1} - n$, not $b_n = nb_{n-1} - n$. For example, $b_n = 2$ will work for $n \ge 2$. Thus we obtain the following solution:

For $n = 2$, we have

$$a_2 = 2 = 2 \cdot 2! - 2 \,.$$

If $n \ge 3$ and $a_{n-1} \le 2(n-1)! - 2$, then

$$a_n = na_{n-1} + n \le n(2(n-1)! - 2) + n = 2n! - n < 2n! - 2 \,.$$

By induction, $a_n \le 2n! - 2$ for all $n \ge 2$.

1.4 Attempt 3: Expansion

Next we unpacked the recurrence a few times, to see what pattern emerged.

$$\begin{aligned}
a_n &= na_{n-1} + n \\
&= n\big((n-1)a_{n-2} + n - 1\big) + n \\
&= n(n-1)a_{n-2} + n(n-1) + n \\
&= n(n-1)\big((n-2)a_{n-3} + n - 2\big) + n(n-1) + n \\
&= n(n-1)(n-2)a_{n-3} + n(n-1)(n-2) + n(n-1) + n
\end{aligned}$$

Repeating this $n-1$ times, we turn our recurrence into a sum:

$$a_n = n + n(n-1) + n(n-1)(n-2) + \cdots + n(n-1)(n-2)\cdots(2) \,.$$

Radoslav noticed a good way to write this sum:

$$a_n = n! \left(\frac{1}{(n-1)!} + \frac{1}{(n-2)!} + \frac{1}{(n-3)!} + \cdots + \frac{1}{1!} \right) \,.$$

He also remembered seeing a similar sum before:

$$e = \frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots \,.$$

Putting this all together yields...

1.5 A more righteous solution

First we show, by induction on n, that

$$a_n = n! \sum_{k=1}^{n-1} \frac{1}{k!} \qquad \text{for all } n \ge 1. \tag{1}$$

For $n = 1$, the sum is empty, hence zero; and $a_1 = 0$. If the result holds for $n-1$, then

$$a_n = na_{n-1} + n = n(n-1)! \sum_{k=1}^{n-2} \frac{1}{k!} + n = n! \left(\sum_{k=1}^{n-2} \frac{1}{k!} + \frac{n}{n!} \right) = n! \sum_{k=1}^{n-1} \frac{1}{k!} ,$$

which completes the proof of (1). An immediate corollary is that

$$a_n \le n! \sum_{k=1}^{\infty} \frac{1}{k!} = n! \left(e - \frac{1}{0!} \right) = n!(e-1) < 2n! .$$

1.6 Another road to the more righteous solution

The recurrence can lead directly to the sum, if you know the right trick. Faced with

$$a_n = na_{n-1} + n ,$$

we can divide by $n!$ and obtain

$$\frac{a_n}{n!} = \frac{a_{n-1}}{(n-1)!} + \frac{1}{(n-1)!} .$$

Now let $c_n = a_n/n!$; then we have the recurrence

$$\begin{aligned} c_1 &= 0 \\ c_n &= c_{n-1} + \frac{1}{(n-1)!} \qquad \text{for } n \ge 2, \end{aligned}$$

which is obviously just a sum in disguise.

This trick — dividing by something to convert a problematic coefficient into part of a new variable and thus convert a recurrence into a sum — is a standard one. For example, to solve the recurrence

$$h_0 = 0 \qquad\qquad h_n = 2h_{n-1} + 1$$

(which arises in the well-known Towers of Hanoi problem), divide by 2^n to obtain

$$\frac{h_n}{2^n} = \frac{h_{n-1}}{2^{n-1}} + \frac{1}{2^{n-1}} ,$$

which immediately yields a sum for $h_n/2^n$, and thence a solution for h_n.

(This technique was also one of many deployed in the Mystical Dream Cactus problem: see our notes for 2005 October 27.)

2 A preliminary observation on "coefficient pinning" rings

Definition 1 Let R be a subring of $\mathbb{R}$, and let p be a polynomial with coefficients in $\mathbb{R}$. We say that p *fixes* R if $p(t) \in R$ for all $t \in R$.

It's easy to see that, if all the coefficients of p are in R, then p fixes R. We noted in our meeting of January 24 that the converse is not true; for example, the polynomial $\frac{1}{2}t^2 + \frac{1}{2}t$ fixes $\mathbb{Z}$, but not all its coefficients are in $\mathbb{Z}$. Naturally, we wonder whether there are any rings for which the converse holds.

Definition 2 Let R be a subring of $\mathbb{R}$. We say that R *pins coefficients* if every polynomial which has real coefficients and fixes R must have coefficients which are all in R.

Of course, $\mathbb{R}$ pins coefficients, but trivially, since we have framed everything in terms of polynomials with real coefficients.[3] Is there a smaller ring which pins coefficients?

I thought I had a proof that $\mathbb{Q}$ pins coefficients, but (as we discovered in the meeting) it has a serious gap. Radoslav and I think we might have found an alternative proof strategy; we might look at it next meeting.

We did succeed in proving one thing. Consider the polynomial $p(t) = t$. Obviously p fixes every ring, so any ring which pins coefficients must contain the coefficients of this polynomial, that is, any such ring must contain 1. From closure under addition, and additive inverses, it then follows that such a ring contains all integers. Since, as we've already seen, $\mathbb{Z}$ itself doesn't pin coefficients, we have the following preliminary result:

> Every ring which pins coefficients contains $\mathbb{Z}$ as a proper subring.

Thus we need not waste our time on rings such as $2\mathbb{Z}$.

[3] A more general formulation of the problem would express pinning coefficients as a property that a ring has with respect to some specified superring.

3 Two equivalent but rather different-seeming statements

A problem from our list: Let E be a measurable subset of $\mathbb{R}^n$. Show that the following are equivalent conditions on E:

(a) For any open set $G \subset \mathbb{R}^n$ which meets E, we have $m(G \cap E) > 0$.

(b) For any continuous functions $f, g\colon E \to \mathbb{R}$, if $f = g$ a.e., then $f = g$.

The proof is, as we will see, straightforward. The interest of the problem is just that the two statements give quite different impressions, so it's a little surprising that they're equivalent (and that it's not a big deal to prove it).

It is perhaps most convenient to prove the two implications by contraposition.

(not (a) $\Rightarrow$ not (b)) Suppose that there exists an open set $G \subset \mathbb{R}^n$ such that $G \cap E \neq \varnothing$ and $m(G \cap E) = 0$. Define $f, g\colon E \to \mathbb{R}$ by

$$f(x) = 0 \qquad \text{and} \qquad g(x) = \operatorname{dist}(x, G^C)\,.$$

(The special case $G = \mathbb{R}^n$, for which this g is ill-defined, is left to the reader.) We compute that

$$x \in E \text{ and } f(x) \neq g(x) \iff x \in E \text{ and } g(x) \neq 0 \iff x \in G \cap E\,,$$

since G is open. Thus the hypothesis that $G \cap E \neq \varnothing$ means that $f \neq g$, while the hypothesis that $m(G \cap E) = 0$ means that $f = g$ a.e.; the existence of such f and g establishes the negation of (b).

(not (b) $\Rightarrow$ not (a)) Suppose $f, g\colon E \to \mathbb{R}$ are continuous functions such that $f = g$ a.e. and $f \neq g$. Since $\mathbb{R} \setminus \{0\}$ is open, its preimage under the continuous function $f - g$ is open in the relative topology of E, that is, for some open set $G \subset \mathbb{R}^n$ we have

$$G \cap E = (f-g)^{-1}(\mathbb{R} \setminus \{0\}) = \{x \in E\colon (f-g)(x) \neq 0\} = \{x \in E\colon f(x) \neq g(x)\}\,.$$

Thus the hypothesis that $f = g$ a.e. means that $m(G \cap E) = 0$, while the hypothesis that $f \neq g$ means that $G \cap E \neq \varnothing$; the existence of such G establishes the negation of (a), which completes the proof.