Timesharing Dexter

Susan Landau[⋆]

My husband Neil Immerman returned from the 1986 STOC meeting with an interesting proposition. Juris Hartmanis and Dexter Kozen had a small pocket of funds, and they proposed that the two of us visit the Cornell Computer Science Department for a week.

It sounded delightful but we had a complication: our new son, who was all of four months old. We decided to time-share Dexter and split child care (using the rule that during the day, he who was not with the baby would be with Dexter). The Kozens improved upon this, offering that we could stay at their house. So while one of us would be talking research with Dexter in his office, the other would be taking care of the baby while visiting Fran at home.

Thus began Dexter's and my adventure into polynomial decomposition. The week before I arrived at Cornell, I had been thinking about polynomial decomposition, that is, the issue of finding a non-trivial solution to the problem $f(x) = g(h(x))$ (non-trivial means that both $g(x)$ and $h(x)$ are of degree greater than 1). Barton and Zippel had a solution for fields of characteristic 0, noting that if $f(x) = g(h(x))$, then $h(x) - h(y)$ divides $f(x) - f(y)$. They used this — and a refinement, under the assumption that $h(0) = 0, h(x)|(f(x) - f(0))$ (without loss of generality, one can assume that $h(0) = 0$) — to find potential $h(x)$ [2]. Their algorithm was exponential in n, the degree of $f(x)$.

Even with the lack of sleep that accompanies having a baby, I thought I could do better. Lüroth's theorem states that if k is an arbitrary field, the fields between $k(f(x))$ and $k(x)$ are in one-to-one correspondence with the decompositions of $f(x)$. Each field between $k(f(x))$ and $k(x)$ can be expressed as $k(h(x))$ for some composition factor of $f(x)$ [7].

I knew how to find certain subfields of a field rather quickly [6] and I thought I could apply that technique. But my potential solution ran into a difficulty. Instead of being kept awake by our son, I spent my first night in Ithaca awake puzzling over polynomial decomposition and blocks of roots of polynomials. That Monday afternoon I talked with Dexter about the problem, my approach, and the difficulty with it. Dexter hadn't been thinking about polynomials, decomposition, or subfields, but in his inimitable fashion, Dexter immediately got very excited. We got to work.

Let me provide some notation and background. Let k be a field of arbitrary characteristic and let $f(x)$ be a monic separable polynomial (no repeated roots) of degree n with coefficients in k. Let K be the splitting field of $f(x)$ over k, the smallest field containing all the roots of $f(x)$ over k. Futhermore let G be the Galois group of $f(x)$ over k, the set of permutations of the roots that hold the base field k fixed.

[⋆] Visiting Scholar, Department of Computer Science, Harvard University.

R.L. Constable and A. Silva (Eds.): Kozen Festschrift, LNCS 7230, pp. 329–332, 2012.

Evariste Galois showed that there is a one-to-one correspondence between the subgroups of G and the subfields between K and k. (He used this to show that roots of arbitrary polynomials of degree five or greater are not necessarily expressible in radicals.) From previous work [6], as long as $f(x)$ was irreducible over a field of characteristic 0 (and $k[x]$ had a factoring algorithm), I had an efficient method for for computing the fields that lay between k and $k[x]/f(x)$.

My work relied on *block decomposition.* If G is a permutation group on $\Omega = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, the roots of $f(x)$ over k, we let G_α be the subgroup of G that fixes α. The fields between k and $k[x]/f(x)$ — one of which was $k[x]/h(x)$ — correspond to subgroups of G_α. Finding intermediate fields could give a decomposition. But decomposable polynomials may have repeated roots, and Galois fields don't capture this situation.

I thought our week in Ithaca would involve Neil in Dexter's office in the mornings, me there in the afternoons, while the evenings would have Fran, Dexter, Neil and me at home, visiting. I had that partially right. Fran, Dexter, Neil and I were at home in the evenings, and sometimes we all got to visit (mostly over dinner). But on decomposition Dexter was like a dog with a bone: toss the repeated roots problem in the air, let it land, grab it, worry it some more, toss it again, and keep it going. He and I spent the evenings puzzling over, pulling at, pressing on decomposition.

If the approach of Galois fields wouldn't allow repeated roots, generalizing the notion of blocks would.

Let k be a field of arbitrary characteristic and let $f(x)$ be a monic polynomial in $k[x]$ of degree $n = rs$, with $f(x)$ not necessarily irreducible or separable. Let K be the splitting field of $f(x)$ over k, and let G denote the Gaiois group of $f(x)$ over k. Dexter and I defined a *block decomposition* for $f(x)$ a multiset A of multisets of elements of k such that,

- $f(x) = \Pi_{A \in \Delta} \Pi_{\alpha \in A}(x - \alpha)$;
- if $\alpha \in A \in \Delta$ and $\beta \in B \in \Delta$, and $\sigma \in G$ is such that $B = \sigma(A) = \{\sigma(\rho) | \rho \in A\}$.

A block decomposition Δ is an $r \times s$ block decomposition if $|\Delta| = r$ and $|A| = s$ for all $A \in \Delta$. This generalization of block decomposition to multisets meant that $f(x)$ could have repeated roots. Dexter was very happy (the bone stopped being tossed in the air quite so often). This definition enabled Dexter and me to generalize the subfield issue to handle reducible polynomials and polynomials with repeated zeros. Before I present our structure theorem, I need to provide some additional notation for you to gnaw on:

Let:

$f(x) = x^n + a_{rs-1}x^{rs-1} + \ldots + a_0$, with $a_i, 0 \leq i \leq rs - 1$;
$g(x) = x^r + b_{r-1}x^{r-1} + \ldots + b_0$, with $b_j, 0 \leq j \leq r - 1$; and
$h(x) = x^s + x_{s-1}x^{s-1} + \ldots + c_0$, and with $c_k, 0 \leq k \leq s, \in k$.

Furthermore let c_j^m denote the jth elementary symmetric function on m-element multisets:

- $c_j^m = \Sigma_{B \subseteq A, |B|=j} \Pi B$, and
- $c_m = 1$.

Dexter and I showed:

Theorem: Let $f(x) \in k[x]$ be monic of degree $n = rs$. The following two statements are equivalent:

- $f(x) = g(h(x))$ for some $g(x)$ and $h(x)$ in $k[x]$ of degree r and s respectively.
- There is an $r \times s$ block decomposition Δ for $f(x)$ such

that $c_s^j(A) = c_s^j(B) \in k$ for all $A, B \in \Delta$, $O \leq j <\leq s-1$ [5].

Without loss of generality we can assume that $c_0 = 0$. With that assumption, we get that if $f(x) = g(h(x))$, then $f(x)$ and $h(x)$ agree on their first r coefficients. The calculation of the remaining coeffcients of $h(x)$ falls out from the simple recurrence equation for the c_i. From $h(x)$ we can determine $g(x)$. (Because the system is overdetermined, we have to check that candidate $g(x)$ and $h(x)$ actually lead to a decomposition.) Our algorithm decomposes $f(x)$ in $O(n^3)$ in general — a rather impressive improvement from the earlier exponential-time algorithms. The algorithm works even faster if the underlying field supports Fast Fourier Transform ($O(n^2 \log n)$ steps) [5].

The bone had been fully gnawed upon. Dexter was delighted (as was I). There was more to come.

My motivation in considering decomposition was because of its fundamental role in computer algebra. But Dexter's and my result turned out to have other applications as well. In 1985 a cryptosystem was proposed based on polynomials [3]. Because in composition polynomial degrees multiply (rather than add, as is the case for polynomial multiplication), the thought was that perhaps composition could be an RSA-type cryptosystem based on polynomials.

The Kozen-Landau theorem shows that polynomial composition is not a good candidate for such public-key systems. Recently I was told that in the main Maple command "solve" for solving polynomial systems (and pretty much everything else), the algorithm begins by attempting to decompose any polynomials passed as input. This is because even while few polynomials are decomposable, the decomposition method is sufficiently fast that it provides a big win when it succeeds. The implementation is the Kozen-Landau technique [4].

There was yet another consequence of Kozen-Landau. The polynomial $x^4 + x + 1$ is the smallest polynomial over $GF(2)$ that has a non-trivial decomposition: $x^4 + x + 1 = g(h(x))$, with $g(x) = x^2 + x + 1$ and $h(x) = x^2 + x$. Sometime after Neil and I left Ithaca and the Kozen domicile, Fran and Dexter retiled their bathroom shower. They included a strip of 4×4 small green and white tiles running along the wall; it is the cyclic multiplicative group of $GF(16)$ as represented by polynomials $\mathrm{mod}(x^4 + x + 1)$ generated by x:

□	□	□	■	□	□	■	■	□	■	□	■	■	■	■
□	□	■	□	□	■	■	□	■	□	■	■	■	■	□
□	■	□	□	■	■	□	■	□	■	■	■	■	□	□
■	□	□	□	■	□	□	■	■	□	■	□	■	■	■

Even when he showers, Dexter can't get away from decomposing polynomials!

References

1. Alagar, V.S., Thanh, M.: Fast Polynomial Decomposition Algorithms. In: Caviness, B.F. (ed.) EUROCAL 1985, Part II. LNCS, vol. 204, pp. 150–153. Springer, Heidelberg (1985)
2. Baron, D., Zippel, R.: Polynomial Decomposition Algorithms. Journal of Symbolic Computation 1, 159–168 (1985)
3. Cade, J.J.: A New Public-Key Cipher Which Allows Signatures. In: Proceedings of Second SIAM Conference on Applied Linear Algebra, Raleigh, NC (1985)
4. Giesbrecht, M.: Personal Communication, December 1 (2010)
5. Kozen, D., Landau, S.: Polynomial Decomposition Algorithms. Journal of Symbolic Computation 7, 445–456 (1989)
6. Landau, S., Miller, G.L.: Solvability by Radicals is in Polynomial Time. Journal of Computer Systems Science 30, 179–208 (1985)
7. van der Waerden, B.L.: Algebra. Frederick Ungar Publishing Co. (1977)