Functional Decomposition of Polynomials

Joachim von zur Gathen*
Dexter Kozen†
Susan Landau‡

87-851
July 1987

Department of Computer Science
Cornell University
Ithaca, New York 14853-7501

*Supported by NSERC grant 3-650-126-40. Part of this work was done during a visit to Universität des Saarlandes, Saarbrücken.
†Supported by NSF grant DCR-8602663.
‡Supported by NSF grants DCR-8402175 and DCR-8301766.

Functional Decomposition of Polynomials

Joachim von zur Gathen*
Department of Computer Science
University of Toronto
Toronto, Ontario M5S 1A4, Canada

Dexter Kozen†
Department of Computer Science
Cornell University
Ithaca, New York 14853

Susan Landau‡
Department of Mathematics
Wesleyan University
Middletown, Connecticut 06457

1 Introduction

If F is a commutative ring and $g, h \in F[x]$, then $f = g \circ h \in F[x]$ is their *(functional) composition,* and (g, h) is a *(functional) decomposition* of f. Given $f \in F[x]$, there exists an essentially unique *complete decomposition* $f = f_1 \circ f_2 \circ \cdots \circ f_k$, where $f_1, \ldots, f_k \in F[x]$ are indecomposable. This result is valid if F is a field whose characteristic does not divide the degree of f.

This paper deals with the following decomposition problem: given $f \in F[x]$ of degree n, and $r, s \in \mathbf{N}$ with $n = rs$ and $r, s > 1$, decide whether there exist $g, h \in F[x]$ of degree r, s respectively, such that $f = g \circ h$. If so, determine the coefficients of g and h.

For some time, this problem was considered to be computationally hard: a cryptographic protocol was based on its supposed intractability [5]. Barton and Zippel [3] and Alagar and Thanh [1] gave exponential-time algorithms for it (in characteristic zero).

In §2, we present fast sequential and parallel algorithms for this problem. In the "tame" case (when the characteristic p of F does not divide r), we present a sequential algorithm requiring time $O(n \log^2 n \log\log n)$, and $O(n \log^2 n)$ if F supports a Fast Fourier Transform. We show that the problem is in NC, and give a depth-optimal $O(\log n)$-depth circuit for it. In addition, we show that the complete decomposition of f can be computed in sequential $O(n^{1+\epsilon})$ or parallel $O(\log n)$ time.

*Supported by NSERC grant 3-650-126-40. Part of this work was done during a visit to Universität des Saarlandes, Saarbrücken.

†Supported by NSF grant DCR-8602663.

‡Supported by NSF grants DCR-8402175 and DCR-8301766.

In §3, we consider the "wild" case (no restrictions on the characteristic of F). We give a new structure theorem which gives necessary and sufficient conditions for testing decomposability over F. The decomposition problem is shown to be reducible to the problem of factoring univariate polynomials over F. We obtain a range of results, from undecidability over sufficiently general fields to fast sequential and parallel algorithms over finite fields.

A version of the algorithm of Theorem 1 below has been implemented [2,6] and compares favorably with [3]. Dickerson [9] has extended some of these results to multivariate polynomials.

We should give a brief history of the research behind this joint paper. Kozen and Landau [18] gave the first polynomial-time sequential and NC algorithms for this problem in the tame case. The time bounds were $O(n^3)$ sequential, $O(n^2)$ if F supports an FFT, and $O(\log^2 n)$ parallel. They also presented the structure theorem (Theorem 9), reducing the problem in the wild case to factorization, and gave an $O(n^{\log n})$ algorithm for the decomposition of irreducible polynomials over general fields admitting a polynomial-time factorization algorithm, and an NC algorithm for irreducible polynomials over finite fields.

Based on the algorithm of [18], von zur Gathen [17] improved the bounds in the tame case to those stated above. These results are presented in §2. He also gave an improved algorithm for the wild case, yielding a polynomial-time reduction to factorization of polynomials, and observed undecidability over sufficiently general fields. These results are presented in §3.

2 Fast Decomposition in the tame case

We consider the following decomposition problem $\mathrm{DEC}^F_{n,r}$. We have a field F, integers $n, r \in \mathbf{N}$ with r dividing n, and $f \in F[x]$ of degree n. Let $s = n/r$. The problem is to decide whether there exist $g, h \in F[x]$ of degrees $r, s > 1$, respectively, such that $f = g \circ h$, and, in the affirmative case, to determine the coefficients of g and h. We say f is *indecomposable* if no such g and h exist for any r, s. The "tame" case is when the characteristic p of F does not divide r. This section deals only with the tame case.

For the question of uniqueness, we note the following three types of ambiguous decompositions. For any $u \in F[x]$, $\alpha \in F$, and $r, m \geq 2$ we have

$$u \circ (x - \alpha) \circ (x + \alpha) = u$$
$$x^r \circ (x^m \cdot u(x^r)) = (x^m \cdot u^r) \circ x^r$$
$$T_r \circ T_m = T_m \circ T_r$$

where T_r, T_m are Chebyshev polynomials. *Ritt's first theorem* states that a decomposition $f = f_1 \circ \cdots \circ f_k$ with $f_1, \ldots, f_k$ indecomposable is unique up to these ambiguities, i.e., that any two complete decompositions can be obtained from each other using these equalities ([20] for $F = \mathbf{C}$, [11] for $p = 0$, [12] for $p = 0$ or $p > n$).

Decompositions are intimately related to the intermediate fields between $F(f)$ and $F(x)$ [10,20] and between F and a splitting field of f (see Theorem 9).

If $f = g \circ h$ and a_n, c_s are the leading coefficients of f, h, respectively, then

$$\frac{f}{a_n} = \left(\frac{1}{a_n} g(c_s x)\right) \circ \frac{h}{c_s}$$

is a decomposition of a monic polynomial into monic polynomials, and so we can assume that f, g, and h are monic, and furthermore that $h(0) = 0$. Denoting by $P \subseteq F[x]$ the set of monic polynomials, we consider the relation

$$\mathrm{DEC}^F_{n,r} = \{(f,(g,h)) \in P \times P^2 \mid f = g \circ h, \ \deg f = n, \ \deg g = r, \text{ and } h(0) = 0\}.$$

In the tame case, for every f there exists at most one such (g, h), so that we can view $\mathrm{DEC}^F_{n,r}$ as a partial function $P \to P^2$. Furthermore, the problem is rational, i.e., if there exists a field extension $K \supseteq F$ and $(f,(g,h)) \in \mathrm{DEC}^K_{n,r}$, then in fact $g, h \in F[x]$ [12,19]. Both facts may fail in the "wild" case; see Example 7.

Let $M = M_F : \mathbf{N} \to \mathbf{R}$ be such that the product of two polynomials in $F[x]$ of degree at most n can be computed with $O(M(n))$ arithmetic operations. We can choose $M(n) = n \log n \log\log n$ [21], and $M(n) = n \log n$ if F supports a Fast Fourier Transform.

Theorem 1 *Over any field F, the decomposition problem* $\mathrm{DEC}^F_{n,r}$, *with* $\mathrm{char}(F)$ *not dividing r, can be computed with $O(M(n)\log n)$ field operations.*

Proof. Let $f \in F[x]$ be monic of degree $n = rs$. We look for a decomposition $f = g \circ h$, with g, h monic. We first compute the unique candidate h, using that f and h^r agree on the highest s terms, i.e. $\deg(f - h^r) \le n - s$. Writing $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, we let $\tilde{f} = a_0 x^n + \cdots + a_{n-1}x + 1 = x^n \cdot f(\frac{1}{x})$ be the reversal of f, and similarly $\tilde{h} = x^s \cdot h(\frac{1}{x})$. Then

$$x^n h(\frac{1}{x})^r = (x^s h(\frac{1}{x}))^r = \tilde{h}^r,$$

$$\begin{aligned} \deg(f - h^r) \le n - s \quad &\leftrightarrow \quad x^n \cdot ((f - h^r)(\tfrac{1}{x})) \equiv 0 \bmod x^s \\ &\leftrightarrow \quad \tilde{f} - \tilde{h}^r \equiv 0 \bmod x^s. \end{aligned}$$

By [4], $\tilde{h} \bmod x^s$ can be computed with $O(M(n))$ operations. We obtain h from $\tilde{h}$ by reversing the coefficient sequence and setting the constant coefficient to zero.

Now we compute the coefficients b_i of g as a Taylor expansion of f in h: $f = \sum_{0 \le i \le r} b_i h^i$ with $b_i \in F[x]$ of degree less than s, and return $g = \sum_{0 \le i \le r} b_i x^i \in F[x]$ if each $b_i \in F$, and otherwise conclude that no decomposition exists. □

Corollary 2 *Let $\epsilon > 0$. If* $\mathrm{char}(F)$ *does not divide the degree n of f, a complete decomposition of f into indecomposable polynomials can be computed with $O(n^{1+\epsilon})$ operations.*

Open Question 3 Is it possible to improve the running time further, say to $O(M(n))$?

Remark 4 We have stated Theorem 1 only for the case of a field F. It actually works for an arbitrary commutative ring F, provided that r is a unit in F.

Kozen and Landau observed that the general parallelization technique of [22] applies to their construction, and obtained an arithmetic algorithm of depth $O(\log^2 n)$ in the tame case. Using fast parallel arithmetic for polynomials (see [15]), one finds the following results of order-optimal depth.

Theorem 5 *Over any field F, the decomposition problem $\mathrm{DEC}^F_{n,r}$, with $\mathrm{char}(F)$ not dividing r, can be computed on an arithmetic network over F of depth $O(\log n)$.*

Corollary 6 *If $\mathrm{char}(F)$ does not divide the degree n of f, a complete decomposition of f into indecomposable polynomials can be computed in depth $O(\log n)$.*

3 Decomposition in the wild case

The literature contains no algorithm to solve the decomposition problem $\mathrm{DEC}^F_{n,r}$ in the "wild" case, when the characteristic divides r. In this section, we present a reduction of the problem to factoring univariate polynomials. We obtain results at four different levels, from worst (undecidable) to best (polynomial time and poly-logarithmic depth). The first two negative results are meant to explain the restrictions we impose in the positive results.

1. The decomposition problem is undecidable in general.
2. If F is not finitely generated over its prime field, decomposition may require algebraic field extensions of F of exponential degree.
3. If F is finitely generated, we have a polynomial-time algorithm.
4. If F is finite, we have a fast sequential ($O(n^3)$) and a fast parallel ($O(\log^2 n)$) algorithm.

The results of this section are from [17], except for Definition 1 and Theorem 9, which are from [18].

In view of §2, we only have to consider a field F of characteristic $p > 0$, and $\mathrm{DEC}^F_{n,r}$ with p dividing r. In the wild case, both the uniqueness and the rationality of decomposition may fail [10,13]. Here are some simple examples of this wild behavior, which also illustrate the general algorithm.

Example 7 Let $p = r = 2$, $s = 4$, $n = 8$, and $f = x^8 + a_4x^4 + a_2x^2 + a_1x \in F[x]$. "$f = g \circ h$" is equivalent to:

$$a_4 = c_2^2 + b_1, \quad a_2 = c_1^2 + b_1c_2, \quad a_1 = b_1c_1.$$

The algorithm takes the first equation in two unknowns and solves for c_2 in terms of an indeterminate z; later we find an equation for z alone and substitute its solutions for b_1. c_1 is similarly determined from the second equation:

$$c_2 = \sqrt{a_4} + \sqrt{z}, \quad c_1 = \sqrt{a_2} + \sqrt{z}(\sqrt[4]{a_4} + \sqrt[4]{z}).$$

The third equation, taken to the fourth power, then yields:

$$z^7 + a_4 z^6 + a_2^2 z^4 + a_1^4 = 0.$$

We take b_1 to be any of the solutions, and substitute to obtain the corresponding c_1, c_2.

Example 8 Let $F = \mathbf{Z}_3$, $f = x^6 + x^4 - x^3 + x^2 + x \in F[x]$, $h = x^2 + cx$, $g = x^3 + b_2x^2 + b_1x$. Then $v = z^3 + 2z + 1 \in F[z]$ has no linear factors, and hence is irreducible. The high order terms of $g \circ h$ are $x^6 + b_2x^4 + (c^3 + 2b_2c)x^3$; if b_2 and c are in F, then $f \neq g \circ h$. However, let $\gamma \in GF(27)$ be such that $v(\gamma) = 0$, $c = \gamma$, $b_2 = 1$, $b_1 = -\gamma^2 + 1$. Then $f = g \circ h$. This shows that decompositions may exist in algebraic extensions without existing in the ground field. Also, the three conjugate solutions obtained in this way are not "essentially equivalent"; thus Ritt's first theorem also fails in this case.

Our first result is a structure theorem for decomposability. Let F be a field of arbitrary characteristic. Let $f \in F[x]$ be monic of degree $n = rs$, not necessarily irreducible or separable. Let $\hat{F}$ denote the splitting field of f. Let $\mathcal{G}$ denote the Galois group of $\hat{F}$ over F. The following definition reduces to the usual notion of block decomposition for f irreducible and separable.

Definition 1 A *block decomposition for* f is a multiset Δ of multisets of elements of $\hat{F}$ such that

1. $f(x) = \prod_{A \in \Delta} \prod_{\alpha \in A}(x - \alpha)$
2. if $\alpha \in A \in \Delta$, $\beta \in B \in \Delta$, and $\sigma \in \mathcal{G}$ such that $\sigma(\alpha) = \beta$, then

$$B = \{\sigma(\gamma) \mid \gamma \in A\}.$$

A block decomposition Δ is an $r \times s$ *block decomposition* if $|\Delta| = r$ and $|A| = s$ for all $A \in \Delta$.

Let c_k^m denote the k^{th} elementary symmetric function on m-element multisets of elements of F:

$$c_k^m(A) = \sum_{B \subseteq A,\ |B| = k} \prod B.$$

By convention, $c_0^m = 1$.

Theorem 9 *Let $f \in F[x]$ be monic of degree $n = rs$. The following two statements are equivalent:*

1. $f = g \circ h$ *for some* $g, h \in F[x]$ *of degree* r *and* s*, respectively;*

2. there exists an $r \times s$ *block decomposition* Δ *for* f *such that*

$$c_k^s(A) = c_k^s(B) \in F, \; \textit{for all } A, B \in \Delta, \; 0 \le k \le s-1.$$

If f is irreducible, then we need only check the condition of Theorem 9(2) for one $A \in \Delta$; if it holds for one, then it holds for all, since $\mathcal{G}$ is transitive on Δ. The coefficients of h will be the $c_k^s(A)$, $1 \le k \le s-1$. The constant coefficient of h is 0, without loss of generality. The roots of g are $c_s^s(A)$, $A \in \Delta$. The coefficients of g may be obtained by solving a triangular linear system, or by the method of Theorem 1.

Theorem 9(2) gives an algebraic condition that can be used to test decomposability of any f over any field F, provided one can factor over F and thereby construct the splitting field of f. The complexity of the algorithm depends on the complexity of factoring over F.

In order to solve $\mathrm{DEC}_{n,r}^F$, it would be sufficient to compute the decompositions in $F[x]$. However, a satisfactory solution to the decomposition problem should also return the decompositions over algebraic extensions. We define $\overline{\mathrm{DEC}}_{n,r}^F$ to be the computational problem of testing whether a monic input $f \in F[x]$ of degree $n = rs$ has an "absolute" decomposition $f = g \circ h$, where $g, h \in K[x]$ are monic polynomials of degree r, s, respectively, over an algebraic closure K of F. If such a decomposition exists, we also have to compute some standard representations of all decompositions.

Theorem 10 *Let* F *be any field. The problem* $\overline{\mathrm{DEC}}_{n,r}^F$ *of decomposing polynomials over* F *is polynomial-time reducible to the problem of factoring univariate polynomials of degree less than* n *over* F.

Since polynomial-time factorization algorithms are available over finitely generated fields [7], we have:

Corollary 11 *Over a finitely generated field* F*,* $\overline{\mathrm{DEC}}_{n,r}^F$ *can be computed in polynomial time.*

The following undecidability result works over a computable field [14], has inputs encoded over a finite alphabet, and the Turing machine as model of computation. The arithmetic operations and tests are computable.

Theorem 12 *There exists a field* F *such that* $\mathrm{DEC}_{n,r}^F$ *is undecidable.*

If $f(0) = 0$ and $f = g \circ h$, then h is a nontrivial factor of f. However, in the tame case the decomposition problem can be solved without recourse to factoring. In the wild case, our algorithm does use a factoring routine. Is this really necessary?

For an affirmative answer, we fix a prime p, and for simplicity, only consider $F = \mathbf{Z}_p$. We call a polynomial $w = \sum w_i z^i \in F[z]$ "special" if it has degree $1 + p + \cdots + p^e$ for some $e \ge 1$, and

$$w_i \ne 0 \rightarrow \exists j \le e+1 \;\; i = p^j + p^{j+1} + \cdots + p^e.$$

The polynomial

$$w = z^7 + a_4 z^6 + a_2^2 z^4 + a_1^4$$

from the Example 7 is special, with $p = e = 2$. It is conjectured that factoring special polynomials is essentially as hard as factoring general polynomials, and that this conjecture is hard to prove. In any case, we have:

Theorem 13 *The problem of factoring special polynomials is linear-time reducible to the decomposition problem.*

We now work out the cost for decomposition over finite fields. We have a field F with p^m elements. We then consider algorithms using arithmetic operations over $\mathbf{Z}_p$, assume that $F = \mathbf{Z}_p[t]/(v)$ is represented by an irreducible polynomial $v \in \mathbf{Z}_p[t]$ of degree m, and elements of F represented by vectors in $\mathbf{Z}_p^m$. Let τ be an exponent for matrix multiplication over F, so that the product of two $d \times d$ matrices over F can be computed with $O(d^\tau)$ operations in F. [8] shows $\tau < 2.38$.

Theorem 13 noted that factorization of special polynomials is reducible to decomposition. All known methods for factoring, based on Berlekamp's (deterministic) algorithm, require linear algebra and thus $\Omega((mn)^\tau)$ operations (for optimal τ). It turns out that all complete decompositions can be computed in essentially the same time bound; any improvement would therefore be major progress. The standard algorithms for factoring univariate polynomials (see e.g. [16]) yield the following bounds.

Theorem 14 *Let F be a finite field with p^m elements, $p = \mathrm{char}(F)$, q the largest power of p dividing r. Then $\overline{\mathrm{DEC}}_{n,r}^F$ can be solved with $O((mn)^\tau)$ operations in $\mathbf{Z}_p$, and with $O(M(n) \log n\, M(m))$ operations, if q does not divide $s = n/r$.*

Corollary 15 *Let $\epsilon > 0$. Absolute indecomposability of polynomials of degree at most n over $GF(p^m)$ can be tested with $O((mn)^{\tau+\epsilon})$ operations.*

Corollary 16 *If F is a finite field with p^m elements and $p = \mathrm{char}(F)$, then $\overline{\mathrm{DEC}}_{n,r}^F$ can be solved on an arithmetic network over $\mathbf{Z}_p$ of depth $O(\log^2(mn))$ and size $(mn)^{O(1)}$.*

Recall that a decomposition $f = f_1 \circ \cdots \circ f_k$ is *complete* if each f_i is indecomposable. Since $f_k, f_{k-1} \circ f_k, \cdots$ may be over larger and larger fields, it is somewhat surprising that we can calculate all complete absolute decompositions of a polynomial (i.e. those over an algebraic closure) quickly.

Theorem 17 *Let F be a finite field with p^m elements and characteristic p, $\epsilon > 0$, and $f \in F[x]$ of degree n. For p and n sufficiently large, all complete decompositions of f over F and all complete absolute decompositions can be computed with $O((mn)^{\tau+\epsilon})$ operations in F. If $p^2 \not| n$, they can be computed with $O((mn)^{1+\epsilon})$ operations.*

In the preceding theorem, p may have to be large. For small p, we have:

Corollary 18 *Let p be a prime, F a finite field with p^m elements and characteristic p. All complete absolute decompositions of a polynomial in $F[x]$ of degree at most n can be computed with $O(m^3n^7)$ operations in $\mathbf{Z}_p$.*

Further details, proofs, and precise bounds may be found in the journal versions of this paper.

Acknowledgments

We are grateful to Arash Baratloo of Cornell and Bruce Char of the University of Waterloo for their implementation of the algorithm of Theorem 1.

References

[1] V.S. Alagar and M. Thanh, "Fast polynomial decomposition algorithms," *Proc.* EUROCAL85, Lect. Notes in Comput. Sci. 204, Springer-Verlag, Heidelberg, 1985, 150-153.

[2] A. Baratloo, private communication, Cornell Univ., December 1986.

[3] D.R. Barton and R.E. Zippel, "Polynomial decomposition algorithms," *J. Symb. Comp.* 1 (1985), 159-168.

[4] R.P. Brent and H.T.Kung, "Fast algorithms for manipulating formal power series," J. Assoc. Comput. Mach. 25 (1978), 581-595.

[5] J.J. Cade, "A public key cipher which allows signatures," *Proc. 2nd SIAM Conf. on Appl. Linear Algebra*, Raleigh, 1985.

[6] B. Char, private communication, Univ. of Waterloo, December 1986.

[7] A.L. Chistov and D.Yu. Grigoryev, "Polynomial-time factoring of the multivariable polynomials over a global field," LOMI preprint E-5-82, Leningrad, 1982.

[8] D. Coppersmith and S. Winograd, "Matrix multiplication via arithmetic progressions," *Proc. 19th ACM Symp. Theory of Comput.,* New York, 1987, 1-6.

[9] M. Dickerson, "Polynomial decomposition algorithms for multivariate polynomials," Tech. Rep. TR87-826, Dept. Comput. Sci, Cornell Univ., April 1987.

[10] F. Dorey and G. Whaples, "Prime and composite polynomials," *J. Algebra* 28 (1974), 88-101.

[11] H.T. Engstrom, "Polynomial substitutions," *Amer. J. Math* 63 (1941), 249-255.

[12] M.D. Fried and R.E. MacRae, "On the invariance of chains of fields," *Ill. J. Math.* 13 (1969), 165-171.

[13] M.D. Fried and R.E. MacRae, "On curves with separated variables," *Math. Ann.* 180 (1969), 220-226.

[14] A. Fröhlich and J.C. Shepherdson, "Effective procedures in field theory," *Phil. Trans. Royal Soc.*, Ser. A 248 (1955-56), 407-432.

[15] J. von zur Gathen, "Parallel arithmetic computations: a survey," *Proc. 12th Int. Symp. Math. Found. Comput. Sci.*, Bratislava, Lect. Notes in Comput. Sci. 233, Springer, 1986, 93-112.

[16] J. von zur Gathen, "Factoring polynomials and primitive elements for special primes," *Theor. Comput. Sci.* 51 (1987), to appear.

[17] J. von zur Gathen, "Functional decomposition of polynomials," Tech. Rep., Sonderforschungsbereich 124, Universität Saarbrücken, July 1987.

[18] D. Kozen and S. Landau, "Polynomial decomposition algorithms," Tech. Rep. TR86-773, Dept. Comput. Sci., Cornell Univ., August 1986; *J. Symb. Comp.*, to appear.

[19] H. Levi, "Composite polynomials with coefficients in an arbitrary field of characteristic zero," *Amer. J. Math.* 64 (1942), 389-400.

[20] J.F. Ritt, "Prime and composite polynomials," *Trans. Amer. Math. Soc.* 23 (1922), 51-66.

[21] A. Schönhage, "Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2," *Acta Informatica* 7 (1977), 395-398.

[22] L.G. Valiant, S. Skyum, S. Berkowitz, and C. Rackoff, "Fast parallel computation of polynomials using few processors," *SIAM J. Comput.* 12:4 (1983), 641-644.