J. Symbolic Computation (1990) **10**, 437–452

Functional Decomposition of Polynomials: the Wild Case

JOACHIM VON ZUR GATHEN

Department of Computer Science, University of Toronto
Toronto, Ontario M5S 1A4, Canada
gathen@theory.toronto.edu

(*Received* 6 *June* 1988)

If g and h are polynomials of degrees r and s over a field, their functional composition $f = g(h)$ has degree $n = rs$. The functional decomposition problem is: given f of degree $n = rs$, determine whether such g and h exist, and, in the affirmative case, compute them. An apparently difficult case is when the characteristic p of the ground field divides r. This paper presents a polynomial-time *partial* solution for this "wild" case; it works, e.g., when $p^2 \nmid r$.

1. Introduction

If F is a field and $g, h \in F[x]$, then $f = g \circ h = g(h) \in F[x]$ 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 $f_1, \cdots, f_k \in F[x]$ are indecomposable polynomials. This result is valid if the characteristic p of F does not divide the degree of f. These facts and the history of the problem can be found in the references given below.

Formally, we consider the following decomposition problem: given $f \in F[x]$ of degree n, and $r, s \in \mathbb{N}$ with $n = rs$, decide whether there exist $g, h \in F[x]$ of degrees r, s, respectively, such that $f = g \circ h$. Barton & Zippel (1985) and Alagar & Thanh (1985) presented (exponential-time) algorithms if $\mathrm{char}(F) = 0$. For the general "tame" case, where p does not divide r, a polynomial-time algorithm was given by Kozen & Landau (1989) (a first version of which appeared in 1986); variants are in the later papers Gutiérrez *et al.* (1989) and von zur Gathen (1990). For the "wild" case, where p divides r, Kozen & Landau (1989) derive from their "structure theorem" an algorithm over fields with a factorization procedure for univariate polynomials. They obtain a polynomial-time algorithm if f is irreducible and F a finite field; in fact, even a fast parallel NC-algorithm. For F arbitrary with a polynomial-time factorization procedure and f irreducible, they can find a *complete decomposition* into indecomposable polynomials in time $O(n^{\log n})$. *Ritt's First*

This work was supported by National Science and Engineering Council of Canada, grant A-2514, and Fundación Andes, beca C-10246. Parts of it were done during visits to Universität des Saarlandes, Saarbrücken, Germany, and to Pontificia Universidad Católica, Santiago, Chile, and as a Visiting Fellow at the Computer Sciences Laboratory, Australian National University, Canberra, Australia.

0747-7171/90/110437+16 $03.00/0

Theorem gives a uniqueness property in the tame case (see the references above); for lack of such a property the (computational) connection between complete decompositions and decomposition with r and s given is not clear in the wild case. (The terminology of "tame" and "wild" is borrowed from number theory, regarding r as some "ramification index"; see e.g., Hasse 1980.)

The polynomial-time methods for the tame case are based on Kozen & Landau's approach of directly solving the equations obtained from comparing coefficients in "$f = g \circ h$". The present paper extends this approach to the wild case, in which we always have $p \leq r < n$. We obtain an algorithm only for the following special case. Write $\deg g = r = qt$ with q a power of p and $p \nmid t$. We will throughout the paper assume that $q \geq p$; otherwise we are in the tame case. Then g is called "simple" (for lack of a better word) if

$$g = x^r + b_{r-i}x^{r-i} + b_{r-i-1}x^{r-i-1} + \cdots + b_0$$

with $b_{r-i} \neq 0$ and either $p \nmid i$ or $i \geq q$. Furthermore, $g = x^r$ is simple. Thus when $p^2 \nmid r$, so that $q = p$, every g is simple; $x^{tp^2} + x^{tp^2-up} + \cdots$ is not simple if $u < p$.

The main result of this paper is a polynomial-time reduction from "simple" decompositions $f = g \circ h$ with g simple to factorization of polynomials with degree less than n. Thus over finite fields, we have a (deterministic) polynomial-time algorithm. It does not yield information about decompositions with g not simple.

The algorithm solves one by one the polynomial equations arising from comparing coefficients of $x^n, x^{n-1}, \ldots$ in "$f = g \circ h$". All partially constructed solutions are maintained until recognized as not leading to an actual decomposition. Giesbrecht (1988) has shown that no such approach can lead to a general polynomial-time algorithm, by exhibiting polynomials with more than a polynomial number of (non-simple) decompositions. Giesbrecht concentrates on the very wild case of "additive polynomials", where nonzero coefficients occur only at exponents which are powers of p. Fortunately, this case turns out to have enough internal structure to allow interesting conclusions such as the above.

The present work can be summarized as exhibiting a further significant case of polynomial decomposition which is reasonably easy to solve; the general case still awaits a polynomial-time solution.

For perspective, we note that over sufficiently general ("computable") fields the existence of a decomposition is undecidable—in marked contrast to the tame case, which can be solved over any field just by field arithmetic—and that decompositions may require field extensions of exponentially large degree. This explains, in a sense, the restrictions imposed for solving the problem.

The algorithm requires the factorization of certain univariate polynomials. Conversely, we exhibit a special class of polynomials whose factorization problem is linear-time reducible to the problem of finding simple decompositions.

Some of the present results were reported in von zur Gathen, Kozen & Landau (1987), with the qualifier "simple" erroneously omitted.

2. Reducing simple decomposition to factoring

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, respectively, such that $f = g \circ h = g(h)$ is the composition of g with h, and, in the affirmative case, to compute g and h. f is

indecomposable if no such g and h exist. The "wild" case is when the characteristic p of F divides r.

We may assume without loss of generality that f, g, h are monic, and that $h(0) = 0$. Denoting by $\mathcal{M} \subseteq F[x]$ the set of monic polynomials, we consider the relation

$$\mathrm{DEC}_{n,r}^{F} = \{(f,(g,h)) \in \mathcal{M} \times \mathcal{M}^2 : f = g \circ h, \deg g = r, \deg h = s, \text{and } h(0) = 0\}.$$

Formally, the computational problem has $f \in \mathcal{M}$ and $r, s \in \mathbf{N}$ as input, and as output the set of all $(g,h) \in \mathcal{M}^2$ with $(f,(g,h)) \in \mathrm{DEC}_{n,r}^{F}$. In the introduction, it was defined when g is simple, and when a decomposition is simple. $\mathrm{sDEC}_{n,r}^{F}$ denotes the set of all simple decompositions.

We fix the following notation for the rest of the paper: $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, $g = x^r + b_{r-1}x^{r-1} + \cdots + b_0$, $h = x^s + c_{s-1}x^{s-1} + \cdots + c_1 x$, and $u_k = x^s + c_{s-1}x^{s-1} + \cdots + c_{s-k+1}x^{s-k+1}$ is the high-order part of h, for $0 \le k < s$. We write $r = qt$, where $q \ge p$ is a power of p and $p \nmid t$. Thus $n = qst$ and $u_0 = 0$.

In the wild case, both the uniqueness and the rationality of decomposition may fail (Fried & MacRae 1969, Dorey & Whaples 1974). Here are some simple examples of this wild behaviour.

EXAMPLE 2.1. To illustrate the algorithm below, let us take $p = r = q = 2$, $s = 4$, $n = 8$, 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 4th power, then yields:

$$z^7 + a_4z^6 + a_2^2z^4 + a_1^4 = 0.$$

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

EXAMPLE 2.2. 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 c is in F, then $f \neq g \circ h$. However, let $\gamma \in \mathbf{F}_{27}$ 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 on uniqueness in characteristic zero (Ritt 1922) also fails in this case. □

EXAMPLE 2.3. Our algorithm would not find the following non-simple decomposition. Let $p = s = 2, r = 4, n = 8, f = x^8 + a_4x^4 + a_2x^2 + a_1x \in \mathbf{F}_8[x]$. Then "$f = g \circ h$" is equivalent to

$$0 = b_3, a_4 = c_1^4 + b_2, a_2 = b_2c_1^2 + b_1, a_1 = b_1c_1.$$

It is straightforward to solve these equations:

$$c_1^7 + a_4 c_1^3 + a_2 c_1 + a_1 = 0, b_1 = c_1^6 + a_4 c_1^2 + a_2, b_2 = c_1^4 + a_2.$$

When $a_4 = a_2 = 0$ and $a_1 = 1$, the seven solutions are given by arbitrary $c_1 \in \mathbb{F}_8^\times$ (so that $c_1^7 = 1$) and $b_2 = c_1^4, b_1 = c_1^6$. Then f is simple, but each of the decompositions is not simple. Unfortunately, it is not clear how to replace the output-driven condition "g is simple" by a condition on the input f (see Proposition 4.2). The algorithm below determines values of the c_k's, using one equation after the other, leaving at each stage the value of at most one b_i (the "leading" one after b_r) undetermined; in this example that would be b_2. However, the first set of four equations in this example can only be solved after taking each of them into account. Thus both b_2 and b_1 are left undetermined until c_1 is computed. The present solution for the simple case might be extended by generalizing the above trivial solution in a systematic way. □

To each power of x in "$f = g \circ h$" corresponds one equation in the coefficients of f, g, and h. We will consider these equations in descending order: $x^n, x^{n-1}, \cdots$. We write $\operatorname{coeff}(v, i)$ for the coefficient of x^i in $v \in F[x]$. The following equations form the basis of the algorithm. For $1 \le k < s$, $1 \le i < q$, and $j \in \mathbb{N}$, we have

$$\begin{aligned} \operatorname{coeff}(h^r, n - qk) &= (\operatorname{coeff}(h^t, st - k))^q = \\ (tc_{s-k} + \operatorname{coeff}(u_k^t, st - k))^q &= tc_{s-k}^q + \operatorname{coeff}(u_k^r, n - qk), \end{aligned} \tag{2.1}$$

$$\operatorname{coeff}(h^r, n - j) = 0 \text{ if } q \nmid j, \tag{2.2}$$

$$\operatorname{coeff}(h^{r-i}, n - is - k) = -ic_{s-k} + \operatorname{coeff}(u_k^{r-i}, n - is - k), \tag{2.3}$$

$$\operatorname{coeff}(h^{r-i}, n - j) = 0 \text{ if } 0 \le j < is. \tag{2.4}$$

In (2.1), we use $h^r = (h^t)^q$ and $\operatorname{coeff}(h^t, st - k) = tc_{s-k} + \operatorname{coeff}(u_k^t, st - k)$, and the fact that $(a+b)^q = a^q + b^q$ for $a, b \in F[x]$. Similarly, for (2.2) we use that $h^r = (h^t)^q = \sum_i \tilde{h}_i x^{iq}$ if $h^t = \sum_i \tilde{h}_i x^i$. In (2.3), only u_{k+1}^{r-i} can contribute, since

$$\deg((h - u_{k+1})^{r-i}) \le (r - i)(s - k - 1) < n - is - k,$$

using that $i + 1 \le q \le r$. The contribution is $(r - i)c_{s-k} = -ic_{s-k}$ from the summand $c_{s-k}x^{s-k} \cdot (x^s)^{r-i-1}$ which occurs $r - i$ times when the power is multiplied out; no other summand involving $c_{s-k}x^{s-k}$ contributes, since its degree is too small. Finally, (2.4) follows from the fact that $\deg h^{r-i} \le s(r - i) = n - si$.

The algorithm proceeds in stages $S_1, \cdots, S_{q-1}$. Stage S_i computes all solutions with $b_{r-1} = \cdots = b_{r-i+1} = 0$ and $b_{r-i} \ne 0$ by determining an initial (high-order) part of any possible h, then b_{r-i}, and finally the rest of h and g. Most of the complications arise in the computation of b_{r-i}. Stage S_{i-1} passes the leading part of h (namely those c_{s-k} with $k < (i-1)s/q$) to S_i. Step 2 calculates some new c_{s-k} (with $k < is/q$). Step 4 deals with a special case, where b_{r-i} can be determined from a linear equation. For the general case, we let z be an indeterminate value for b_{r-i}, and compute in step 5 (within stage S_i) values γ_{s-k} corresponding to c_{s-k} (for $(i-1)s/q \le k < is/(q-1)$) depending on z, using the equations in z and γ_{s-k} now corresponding to (2.1) through (2.4). (The same equations are used in the special case, only z is then not an indeterminate, but has already been given a value.) In step 6, the resulting equation $v = 0$ for z is computed and factored,

then solved in step 8, and several specific nonzero values $\alpha_1, \cdots, \alpha_m$ are determined for z, and the algorithm continues with $b_{r-i} = \alpha_j$ for each j separately. Step 9 determines the remaining c_{s-k}. Given a candidate $h \in F[x]$ of degree s with $h(0) = 0$, there is at most one $g \in F[x]$ with $f = g \circ h$; this g is computed in step 10 by Taylor expansion as in von zur Gathen (1990). The algorithm terminates for the solutions of stage S_i.

The normal control flow is as follows. Step 1 is an initialization. Stage S_i (for $1 \le i < q$) starts in step 2 and proceeds to steps 3 through 11. At that point, all decompositions for stage S_i have been output, and control returns to step 2 for stage S_{i+1}. Four exceptional situations may arise; they are handled by "goto" statements. In steps 4 or 6 it may become clear that stage S_i terminates permaturely (either because $b_{r-i} = 0$ is forced, or because non-simple decompositions may exist); control then passes to step 2. In step 5 we may already know b_{r-i}; then we skip to step 9. Finally, for the last value of i, namely $i = q$, we finish the computation of h in step 2, skip to step 10 to calculate g, and terminate.

The main technical problem is finding an equation v as required, and proving that it is nontrivial, i.e., that v is not the constant zero.

The algorithm generalizes that of Kozen & Landau (1989) for the tame case, which performs step 2 (with $i = 1, q = 1, t = r$) to calculate h, then a variant of step 10 to obtain g; the reader is encouraged to study their algorithm first. A generalization of the present algorithm beyond the simple wild case might first compute h and several (not just one) coefficients of g, then the remainder of g.

If F is a field of characteristic $p > 0$, K an algebraic closure of F, and q a power of p, then

$$F^q = \{a^q : a \in F\},\ F^{1/q} = \{a \in K : a^q \in F\},\ F^{1/p^\infty} = \bigcup_{i \in \mathbf{N}} F^{1/p^i} \subseteq K.$$

If F is finite (or perfect), then $F^{1/p^\infty} = F$.

Algorithm **Simple decomposition.**

Input: $r, s \in \mathbf{N}$ with $r, s \ge 2$, and $f = \sum a_i x^i \in F[x]$ monic of degree $n = rs$.

Output: Representations of all decompositions (g, h) of f, with $(f, (g, h)) \in \mathrm{sDEC}^K_{n,r}$, where K is an algebraic closure of F. (Thus $f = g \circ h$, and g is simple.) If non-simple decompositions possibly exist, then a corresponding message is given.

1. Write $r = qt$ with q a power of $p = \mathrm{char}(F)$ and $p \nmid t$. If $q = 1$, use some algorithm for this tame case, and stop. Set $i = 0$.

2. Replace i by $i + 1$. For $(i-1)s/q \le k < is/q$, compute $c_{s-k} \in F^{1/q}$ from:

$$tc^q_{s-k} = a_{n-qk} - \mathrm{coeff}(u^r_k, n - qk) \in F.$$

   If $i = q$ [so that h is known], set $j = m = 1$, $h^{(1)} = h$, and go to step 10.

3. Let z be an indeterminate over F, and $L = F(z)^{1/p^\infty}$. Set a flag $\mathcal{F}$ to **false**. [$\mathcal{F}$ indicates whether a value has been determined for z.]

4. If $q \nmid is$, replace z by a_{n-is}, and set $\mathcal{F} =$ **true**. If $a_{n-is} = 0$, then set $b_{r-i} = 0$ and go to step 2.

5. For $is/q \le k < is/(q-1)$, compute $\gamma_{s-k} \in L$ from:

$$t\gamma_{s-k}^q = a_{n-qk} - \operatorname{coeff}(\eta_k^r + z\eta_k^{r-i}, n-qk),$$

$$\text{where } \eta_k = \sum_{0 \le l < is/q} c_{s-l}x^{s-l} + \sum_{is/q \le l < k} \gamma_{s-l}x^{s-l}.$$

[Thus η_k now plays the role of u_k.] If $\mathcal{F} = \textbf{true}$, then set $j = m = 1$, $c_{s-k}^{(1)} = \gamma_{s-k}$, $u_k^{(1)} = u_k$ for k as above, $b_{r-i}^{(1)} = b_{r-i}$, and go to step 9. [In this case, z has been replaced by a value from K in step 4, and $\eta_k = u_k \in F^{1/p^\infty}$.]

6. If $p \mid i$, output "a non-simple decomposition possibly exists", set $b_{r-i} = 0$, and and go to step 2. If $p \nmid i$, let $e \in \mathbf{N}$ be such that $q^e \mid s$ and $q^{e+1} \nmid s$. If $\mathcal{F} = \textbf{false}$, let $\kappa = is \cdot (1-q^{-e})/(q-1) \in \mathbf{N}$, and

$$v = \frac{t^e}{i^{e+1}} \cdot \left(iz\gamma_{s-\kappa} + a_{n-is-\kappa} - z \cdot \operatorname{coeff}(\eta_\kappa^{r-i}, n-is-\kappa)\right)^{q^e} \in L,$$

[It turns out that $v \in F[z]$ is a monic polynomial of degree $d = (q^{e+1}-1)/(q-1) < 2q^e$, which will now be used to determine a value for z.] Factor v over F into irreducible monic polynomials $v_1, \cdots, v_\mu$ of degrees $d_1, \cdots, d_\mu$ with $d_1 + \cdots + d_\mu = d$. Order these polynomials so that $z, v_1, \cdots, v_m$ are pairwise distinct, $m \le \mu$, and $\{z, v_1, \cdots, v_m\} = \{z, v_1, \cdots, v_\mu\}$. [Step 4 dealt with the possible factor z, for which $b_{r-i} = 0$.]

7. For $1 \le j \le m$, do steps 8, 9, and 10.

8. If $\mathcal{F} = \textbf{false}$, let $\alpha_j = z \bmod v_j \in E_j = F[z]/(v_j)$ be a root of v_j. We now have values $b_{r-i}^{(j)} = \alpha_j \ne 0$ and calculate $c_{s-k}^{(j)} = \gamma_{s-k}(\alpha_j)$ for the γ_{s-k} computed in step 5, and the corresponding $u_k^{(j)} = \eta_k(\alpha_j)$. [We do not keep track of the other $d_j - 1$ solutions conjugate to α_j.]

9. For $is/(q-1) \le k < s$, compute $c_{s-k}^{(j)}$:

$$c_{s-k}^{(j)} = \left(ib_{r-i}^{(j)}\right)^{-1} \cdot \left(-a_{n-is-k} + \operatorname{coeff}((u_k^{(j)})^r + b_{r-i}^{(j)}(u_k^{(j)})^{r-i}, n-is-k)\right).$$

[We now have all coefficients of a candidate $h^{(j)}$ for a decomposition.]

10. Compute the corresponding $g^{(j)}$ by Taylor expansion. If $f = g^{(j)} \circ h^{(j)}$, then return the solution $(g^{(j)}, h^{(j)})$. If $i = q$, then stop.

11. Set $b_{r-i} = 0$ and goto step 2.

In order to solve $\mathrm{sDEC}_{n,r}^F$, it would be sufficient to run the algorithm only on those coefficients computed in steps 2, 5, and 8 that turn out to be in F, corresponding to some linear factors v_j in step 6. However, a satisfactory solution to the decomposition problem should also return the decompositions over algebraic extensions; the above algorithm does this. We let K be an algebraic closure of F, define $\overline{\mathrm{DEC}}_{n,r}^F = \mathrm{DEC}_{n,r}^K \restriction F[x] \times K[x]^2$, and consider the computational problem of testing whether a monic input $f \in F[x]$ of degree $n = rs$ has an "absolute" decomposition $f = g \circ h$ with $(f,(g,h)) \in \mathrm{DEC}_{n,r}^K$; similarly

$\overline{\text{sDEC}}^F_{n,r}$ for g simple. If τ is an automorphism of K over F and $\bar{\tau}$ its extension to $K[x]$, then also $f = \bar{\tau}(g) \circ \bar{\tau}(h)$. If such a decomposition exists, we also have to compute representations of all decompositions; only one representative for each set of conjugate solutions is required. A representation of a decomposition now consists of an irreducible polynomial $v \in F[z]$ and $g', h' \in F[x, z]$ with $\deg_x g' = r$, $\deg_x h' = s$, $\deg_z g' < \deg v$, $\deg_z h' < \deg v$, corresponding to $g = g' \bmod v \in (F[z]/(v))[x] \subseteq E[z]$, where $E = F[z]/(v)$, and $h = h' \bmod v \in E[z]$ with $f = g \circ h$.

The following fact will be used without explicit reference in the sequel.

FACT 2.4. *Let F be a field of characteristic $p > 0$, $a \in F$, and $q \in \mathbf{N}$ a power of p. Then there exists at most one $b \in F$ such that $b^q = a$. If F is finite with u elements and $u^i \geq q$, then $b = a^{u^i/q}$ satisfies the equation. If $a \in \mathbf{Z}_p$, then $a^q = a$.*

PROOF. For all $b \in F$, $(x - b)^q = x^q - b^q$. □

The next lemma shows that v in step 6 is not the zero polynomial, so that only a finite number of values for z has to be considered. Recall $L = F(z)^{1/p^\infty}$, $q^e \mid s$, $q^{e+1} \nmid s$, and define $R = F^{1/q}[z]$, and $\sigma_j = 1 + q + \cdots + q^{j-1} = (q^j - 1)/(q - 1)$ for $0 \leq j \leq e$.

The numbers κ_j defined in the lemma below are the threshold values at which something interesting happens to the γ_{s-k}'s. We divide the set of all k in stage S_i, namely $\kappa_0 = 0 \leq k < is/(q - 1)$, into intervals $[\kappa_j, \kappa_{j+1})$, for $0 \leq j \leq e$. Recall that a γ_{s-k} in general involves high-degree roots of z and of field elements. (i) states that within each interval, a certain power of γ_{s-k} (with exponent q^j) is actually a polynomial in z, with coefficients at most qth roots of elements of F, and whose degree is at most σ_j. This yields the crucial fact (ii) about the threshold value $k = \kappa_j$. For this value of k, the q^jth power of γ_{s-k} is actually a polynomial in $F[z]$ (no roots in F required) of degree exactly σ_j (if $p \nmid i$), and we determine its leading coefficient as $(i/t)^{\sigma_j}$. The central point is that this coefficient is nonzero; this translates into the condition "$p \nmid i$" in the definition of simple decomposition.

LEMMA 2.5. *Let $1 \leq i < q$, for $0 \leq j \leq e$ define $\kappa_j = is \cdot \sigma_j q^{-j} \in \mathbf{N}$, and $\kappa_{e+1} = \lceil is/(q - 1) \rceil$. Let $0 \leq j \leq e$.*

(i) If $\kappa_j \leq k < \kappa_{j+1}$, then $\gamma_{s-k}^{q^j} \in R$ and $\deg_z \gamma_{s-k}^{q^j} \leq \sigma_j$.

(ii) There exists $\delta_j \in F[z]$ such that

$$\gamma_{s-\kappa_j}^{q^j} = \left(\frac{iz}{t}\right)^{\sigma_j} + \delta_j \in F[z],$$

and $\deg_z \delta_j < \sigma_j$.

(iii) v as computed in step 6 (with $p \nmid i$) of **Simple decomposition** *is a monic polynomial in $F[z]$ of degree $\sigma_{e+1} = (q^{e+1} - 1)/(q - 1)$.*

(iv) Let (g, h) be a solution computed in step 10, and $E \supseteq F$ be the field generated by the coefficients of g and h. There exists a field F_1 with $F \subseteq E \subseteq F_1 \subseteq K$ and $[F_1 : F^{1/q}] \leq \sigma_{e+1}$.

PROOF. We have $\kappa = \kappa_e$ in step 6, $\kappa_0 = 0$, $\kappa_1 = is/q$, and

$$q \mid \kappa_j \iff j < e.$$

Set $\gamma_{s-k} = c_{s-k} \in R$ for $k < is/q$.

Assume that $\kappa_j \le k < \kappa_{j+1}$. (2.1), (2.3), and the fact that $\operatorname{coeff}(h^{r-l}, n - qk) = 0$ for $is/q \le k < is/(q-1)$ and $l > i$ imply

$$t\gamma_{s-k}^q = a_{n-qk} - \operatorname{coeff}(\eta_k^r, n - qk) - z \cdot \operatorname{coeff}(\eta_k^{r-i}, n - qk).$$

Abbreviate

$$\rho = \operatorname{coeff}(\eta_k^t, st - k),\ \pi = \operatorname{coeff}(\eta_k^{r-i}, n - qk),$$

so that

$$t\gamma_{s-k}^{q^j} = a_{n-qk}^{q^{j-1}} - \rho^{q^j} - (z\pi)^{q^{j-1}}. \tag{2.5}$$

If a term $\gamma_{s-l}x^{s-l}$ in η_k contributes to π, then

$$\begin{aligned} n - qk &\le s - l + (r - i - 1)s = n - is - l \implies \\ is + l \le qk &= q\kappa_{j+1} + q(k - \kappa_{j+1}) = is + \kappa_j + q(k - \kappa_{j+1}). \end{aligned} \tag{2.6}$$

Since $k < \kappa_{j+1}$, we have $l < \kappa_j$ for any l satisfying (2.6). No mixed terms $\gamma_{s-l_1} \cdot \gamma_{s-l_2}$ with $l_1, l_2 \ge \kappa_1$ contribute to π, since $q \ge 2$ implies that

$$2(s - \frac{is}{q}) + (r - i - 2)s < n - \frac{isq}{q-1}.$$

Concerning ρ, again no mixed terms $\gamma_{s-l_1} \cdot \gamma_{s-l_2}$ with $l_1, l_2 \ge is/q$ contribute, since

$$2(s - \frac{is}{q}) + (t - 2)s \le st - \frac{is}{q-1}.$$

We now prove claim (i) by induction on k. It holds for $k < \kappa_1$, and now let $k \ge \kappa_1$. Suppose that γ_{s-l} contributes to ρ, and define m by $\kappa_m \le l < \kappa_{m+1}$; then $m \le j$ since $l < k$. By the induction hypothesis, $\gamma_{s-l}^{q^m} \in R$ has degree at most σ_m, so that $\gamma_{s-l}^{q^j} = (\gamma_{s-l}^{q^m})^{q^{j-m}}$ has degree at most $q^{j-m} \cdot \sigma_m \le \sigma_j$. It follows that

$$\rho^{q^j} \in R,\ \deg_z(\rho^{q^j}) \le \sigma_j.$$

From (2.6), we find

$$\pi^{q^{j-1}} \in R,\ \deg_z(\pi^{q^{j-1}}) \le \sigma_{j-1}.$$

It follows from (2.5) that $\gamma_{s-k}^{q^j} \in R$ has degree at most $\max\{\sigma_j, q^{j-1} + \sigma_{j-1}\} = \sigma_j$. Thus (i) is proven.

Claim (ii) is clear for $j = 0$ (where $\gamma_{s-\kappa_0} = \gamma_s = 1$), and for an induction we assume $j \ge 1$. Set

$$\varphi = \operatorname{coeff}(\eta_{\kappa_{j-1}}^{r-i}, n - q\kappa_j),$$

Condition (2.6) and fact (2.3) imply that

$$\pi = \operatorname{coeff}(\eta_{\kappa_j}^{r-i}, n - q\kappa_j) = -i\gamma_{s-\kappa_{j-1}} + \varphi.$$

Then from (2.5) and the inductive hypothesis we have

$$\gamma_{s-\kappa_j}^{q^j} = t^{-1} \cdot \left(a_{n-q\kappa_j}^{q^{j-1}} - \rho^{q^j} + i(z\gamma_{s-\kappa_{j-1}}\Big)^{q^{j-1}} - (z\varphi)^{q^{j-1}}\right) =$$

$$\frac{i}{t} z^{q^{j-1}} \left(\frac{iz}{t}\right)^{\sigma_{j-1}} + \frac{i}{t} z^{q^{j-1}} \delta_{j-1} + t^{-1} \cdot \left(a_{n-q\kappa_j}^{q^{j-1}} - \rho^{q^j} - (z\varphi)^{q^{j-1}}\right).$$

It remains to show that the last four summands are in $F[z]$ and have small degree. The second summand is in $F[z]$ and has degree at most

$$q^{j-1} + (\sigma_{j-1} - 1) = \sigma_j - 1.$$

Also, $\rho^{q^{j-1}} \in R$, and the degree of $\rho^{q^j} \in F[z]$ is bounded by $q \cdot \sigma_{j-1} = \sigma_j - 1$. Finally, $\varphi^{q^{j-2}} \in R$ has degree at most σ_{j-2}, and

$$q^{j-1} + \deg \varphi^{q^{j-1}} \leq q^{j-1} + q \cdot \sigma_{j-2} = \sigma_j - 1.$$

This proves (ii).

To prove claim (iii) of the lemma, let

$$\psi = \left(\operatorname{coeff}(\eta_{\kappa_e}^{r-i}, n - is - \kappa_e)\right)^{q^{e-1}}.$$

Again, no mixed terms contribute to ψ, since

$$s - l_1 + s - l_2 + (r - i - 2) \cdot s < n - is - \kappa_e$$

for $l_1, l_2 \geq is/q$. By (i), ψ is in R and has degree at most σ_{e-1}. Thus

$$v = \frac{t^e}{i^{e+1}} \cdot \left(i(z\gamma_{s-\kappa_e})^{q^e} + a_{n-is-\kappa_e}^{q^e} - z^{q^e}\psi^q\right) =$$

$$\frac{t^e}{i^{e+1}} \cdot iz^{q^e} \cdot \left(\frac{iz}{t}\right)^{\sigma_e} + \frac{t^e}{i^{e+1}} \cdot (iz^{q^e}\delta_e + a_{n-is-\kappa_e}^{q^e} - z^{q^e}\psi^q).$$

The first summand is $z^{\sigma_{e+1}}$, and the second summand is a polynomial in $F[z]$ of degree less than σ_{e+1}.

For claim (iv), take the solution $(g^{(j)}, h^{(j)})$ given by some α_j in step 8, and $F_1 = F^{1/q}[\alpha_j]$. Then all $c_{s-k}^{(j)} \in F_1$, and $[F_1 : F^{1/q}] \leq \sigma_{e+1}$. □

THEOREM 2.6. *Let F be any field. The algorithm* **Simple decomposition** *reduces the problem* $\overline{\text{sDEC}}$ *of finding simple decompositions of polynomials over F to the problem of factoring univariate polynomials of degree less than n over F.*

PROOF. To prove correctness of the algorithm, first note that c_{s-k} resp. γ_{s-k} are uniquely determined in steps 2 and 5, by Fact 2.4. From the following equivalences, it is clear that the equations in steps 1 through 5 and 9 follow from (2.1) through (2.4):

$$n - qk > n - is \iff k < \frac{is}{q},$$

$$n - qk > n - is - k \iff k < \frac{is}{q-1},$$

$$n - qk < n - is - k \iff k > \frac{is}{q-1}.$$

When $1 \le i < q$ and $\kappa = \kappa_e \in \mathbf{N}$ as in step 6, then $q \nmid \kappa$. From (2.2) and (2.3), we have

$$a_{n-is-\kappa} = -ib_{r-i}c_{s-\kappa} + b_{r-i} \cdot \operatorname{coeff}(u_\kappa^{r-i}, n - is - \kappa).$$

Thus $v(z) = 0$ for any value for z leading to a decomposition. We have now proved that the coefficients in any decomposition satisfy the equations used in the algorithm. On the other hand, any candidate produced by the algorithm is tested in step 10, so that the algorithm produces exactly one representative for each set of conjugate solutions. □

REMARK 2.7. Any solution computed in the algorithm must satisfy

$$a_{n-is-k} = z \cdot \operatorname{coeff}(\eta_{k+1}^{r-i}, n - is - k)$$

for $1 \le k < s$ with $q \nmid is + k$. Any practical implementation would incorporate all these checks, which may determine z much earlier than **Simple decomposition** does, or find that no simple decomposition exists before step 10. However, these checks may all be trivial "$0 \stackrel{?}{=} z \cdot 0$", and do not help for our worst-case analysis. Here are some of these checks; step i' should go after the end of step i of the algorithm.

2'. If there exists some k with $0 \le k < is$, $q \nmid k$, and $a_{n-k} \ne 0$, then return "no solution" and stop the algorithm.

3'. If $c_{s-l} \ne 0$ for some l with $1 \le l < is/q$ and $q \nmid is + l$, let k be the smallest such l, and do the following. Replace z by a_{n-is-k}/c_{s-k}, and set $j = m = 1$ and $\mathcal{F} =$ **true**; if $a_{n-is-k} = 0$, then set $b_{r-i} = 0$ and go to step 2, else go to step 5.

8'. If

$$\operatorname{coeff}((u_k^{(j)})^r + b_{r-i}^{(j)}(u_k^{(j)})^{r-i} - f, n - k) \ne 0$$

for some $0 \le k < isq/(q-1)$, then stop. [This α_j does not lead to a decomposition.]

3. Simple decomposition in the wild case

We now put the reduction of Section 2 to work. 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 simple decomposition problem is undecidable in general.

2. If F is not finitely generated over its prime field, $\overline{\text{sDEC}}$ 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 ($O(n^4)$) and a fast parallel ($O(\log^2 n)$) algorithm. If p^2 does not divide n, we obtain $O(n^{1+\epsilon})$ sequential and $O(\log n)$ parallel time.

We have to specify the model of computation somewhat more precisely. We fix a field F. The undecidable example of Proposition 3.1 below works over a "computable field" (Fröhlich & Shepherdson 1955), has inputs encoded over a finite alphabet, and the Turing machine as model of computation. The arithmetic operations and zero-tests are Turing-computable. Example 3.2 and Theorem 3.3 deal with the purely algebraic question whether fields of exponentially large degree may be required (the answer is: yes and no); presumably exponentially large degrees make the problem infeasible in any model of computation.

The positive results deal with finitely generated fields, where polynomial-time Boolean factorization procedures are known (Chistov & Grigoryev 1982). Finite fields are of special interest.

Fix a field F of characteristic $p > 0$. We denote by p-ROOT the problem of deciding, on input $a \in F$ and $e \in \mathbf{N}$, whether a has a p^eth root $b \in F$ with $b^{p^e} = a$, and, in the affirmative case, of computing the unique such b. In other words, the polynomial $x^{p^e} - a$ has to be factored; the input length is p^e plus the length sufficient to encode a. FACTOR is the problem of computing a complete factorization of a polynomial in $F[x]$, given its coefficients. We have reductions

$$p\text{-ROOT} \leq \text{sDEC} \leq \text{FACTOR}.$$

The last is given by the algorithm, and the first by mapping an input a, e for p-ROOT to $f = x^{2p^e} + ax^{p^e}$ (for odd p; $f = x^{3\cdot 2^e} + ax^{2^e}$ will do for $p = 2$). Then f has the unique decomposition $f = x^{p^e} \circ (x^2 + \sqrt[p^e]{a}x)$ with degrees p^e and 2, which is simple.

PROPOSITION 3.1. *For any prime $p \geq 3$, there exists a field F of characteristic p such that $\text{sDEC}^F_{p,2}$ is undecidable.*

PROOF. Let $p \geq 3$ be a prime. A construction by Fröhlich & Shepherdson (1955) leads to infinite ("computable") fields F of characteristic p, for which the decision problem: "given $a \in F$, is a a pth power?" is undecidable; see von zur Gathen (1984a), Remark 5.10. By the reduction to sDEC, the latter question is also undecidable. □

Similarly, $\text{sDEC}^F_{2,3}$ is undecidable for some fields F of characteristic 2. This construction can be modified so that for every prime p and every $S \subseteq \mathbf{N}$, we have a field F_S of characteristic p such that the decision problem for S is linear-time reducible to $\overline{\text{sDEC}}^{F_S}_{p,2}$. Thus there are fields over which the decomposition problem is NP-hard, exponential-space hard, ...

We will now see that the problem may produce very large field extensions, if the field is not finitely generated over its prime field.

EXAMPLE 3.2. Let p be a prime, $y_1, y_2, \ldots$ indeterminates over $\mathbf{Z}_p$, $F = \mathbf{Z}_p(y_1, y_2, \ldots)$, and K an algebraic closure of F. For any power $r > 2$ of p, we exhibit polynomials $f_r, g_r \in F[x]$, $h_r \in K[x]$ such that $(f_r, (g_r, h_r)) \in \text{DEC}^K_{n,r}$, where $n = r^3 + r$, $f_r = g_r \circ h_r$ is the unique decomposition of f_r over K, and the coefficients of h_r generate a field of degree

at least $2^{\sqrt[3]{n}}$ over F. Let $z_i = y_i^{1/r} \in K$ for $i \in \mathbf{N}$, $s = r^2+1$, $g_r = x^r$, $h_r = x^s + z_{s-1}x^{s-1} + \cdots + z_{s-r}x^{s-r} \in K[x]$, and $f_r = g_r \circ h_r = x^n + y_{s-1}x^{n-r} + \cdots + y_{s-r}x^{n-r^2} \in F[x]$. Step 1 of **Simple decomposition** with $i = 1$ determines the leading coefficients of h, and one checks that $b_{r-i} = 0$ for $1 \le i \le r$ in any solution g, so that (g_r, h_r) is the only solution. The field generated by the coefficients of h_r has degree $r^r > 2^{\sqrt[3]{n}}$ over F. □

THEOREM 3.3. *Let F be finitely generated over $\mathbf{Z}_p$, say by m generators, K an algebraic closure of F, $f \in F[x]$ of degree $n = rs$, and $E \subseteq K$ the field over F generated by the coefficients of one particular solution (g,h) as computed by the algorithm* **Simple decomposition** *on input f. Then $[E : F] < n^{m+1}$.*

PROOF. Let $\lambda_1, \ldots, \lambda_m \in F$ generate F as a field over $\mathbf{Z}_p$. Then $F^{1/q}$ is generated over F by $\lambda_1^{1/q}, \ldots, \lambda_m^{1/q}$, and thus $[F^{1/q} : F] \le q^m$. Using Lemma 2.5 (iv), we find

$$[E : F] \le q^m \cdot (q^{e+1} - 1)/(q-1) < r^m rs < n^{m+1}. \quad \square$$

COROLLARY 3.4. *Over a finitely generated field F, $\overline{\text{sDEC}}$ can be computed in polynomial time.*

PROOF. Polynomial-time factorization algorithms are available over finitely generately fields (Chistov & Grigoryev 1982). By Theorem 3.3, the required field extensions have polynomial degree. □

We next analyze the cost of the algorithm. We denote by $M(n)$ the number of field operations in F sufficient to multiply two polynomials in $F[x]$ of degree n, and use $M(n) = n \log n \log\log n$ for any field (Schönhage & Strassen 1971, Schönhage 1977, Cantor & Kaltofen 1987). For a field F, let $S_F(d)$ be a number of operations in F sufficient to factor a univariate polynomial over F of degree at most d, and $R_F(q)$ to extract a qth root in F. In particular, $R_F(q) \le S_F(q)$. We assume polynomial bounds, so that e.g. $S_F(2d) = O(S_F(d))$.

THEOREM 3.5. *Let r be a divisor of n, q the largest power of* $\text{char}(F)$ *dividing r, and q^e the largest power of q dividing $s = n/r$. Algorithm* **Simple decomposition** *for* $\overline{\text{sDEC}}$ *can be performed with the following number of operations in F.*

(i) $O(n^3(\log n \log\log n)^2 + qS_F(q^e) + sR(q))$,

(ii) $O(M(n)\log n + sR(q))$, *if* $p^2 \nmid n$.

PROOF. During the algorithm, we may have to compute in field extensions E_j of F of degree $d \le \sigma_{e+1}$. In the following, let E denote such a field extension. A qth root in $E^{1/q}$ of an element in E can be computed in $O(dR_F(q))$ operations in F. One arithmetic operation in E can be performed with $O(M(d)\log d)$ operations in F. If $d_1, \cdots, d_m$ with $d_1 + \cdots + d_m \le \sigma_{e+1} = (q^{e+1} - 1)/(q-1) < 2q^e$ are the degrees of the field extensions computed in step 8, then

$$\sum_{1 \le j \le m} M(d_i)\log d_i = O(M(q^e)\log q^e),$$

and similarly for the other cost functions R and S. Thus in the estimate we can assume the worst case: only one field extension, of maximal degree σ_{e+1}.

Let $1 \le i < q$. We estimate step by step the number B_i of operations in F during stage S_i of **Simple decomposition**. The asymptotic estimates "O" involve absolute constants only. In step 1, we use repeated squaring, retaining only the highest is coefficients. For the required coefficients of η_k^{r-i} in step 5, we compute the highest $qk < qis/(q-1) \le qs$ coefficients of η_k^{r-i} by repeated squaring and truncating the lower coefficients after each step. By Lemma 2.4 (i), $\eta_k \in F^{1/q^{j+1}}[z^{1/q^j}]$ has degree at most σ_j in z^{1/q^j}, if $\kappa_j \le k < \kappa_{j+1}$. We obtain the following number of operations in F.

2. $O\left(\left(\frac{is}{q} - \frac{(i-1)s}{q-1}\right) \cdot (R_F(q) + M(s)\log r)\right) = O\left(s/q \cdot (R_F(q) + M(s)\log r)\right)$.

5. $$\sum_{\substack{is/q \le k < is/(q-1) \\ \kappa_j \le k < \kappa_{j+1}}} O\left(\log r M(\deg_{z^{1/q^j}} \eta_k) \cdot M(qs) + (\deg_{z^{1/q^j}} \gamma_{s-k}) R(q)\right)$$
$$= O\left(M(qs)\log r \textstyle\sum_{1 \le j \le e} ((\kappa_{j+1} - \kappa_j) M(\sigma_j) + \sigma_j R(q))\right)$$
$$= O\left(M(qs)\log r \textstyle\sum_{1 \le j \le e} q^{-j} M(q^j) + q^e R(q)\right)$$
$$= O\left(e \cdot (M(qs)\log r \log s \log\log s + q^e R(q))\right).$$

6. $S_F(\sigma_{e+1}) = O(S_F(q^e))$ plus terms as above.

9. $O\left(s \cdot \log r M(n) M(q^e)\right) = O\left(sn^2 (\log n \log\log n)^2\right)$.

10. $O\left(M(n)\log n \cdot M(q^e)\right)$, by Fact 2.1 (iv) of von zur Gathen (1990).

Using that $q^e \le s$, we find the total cost as

$$O\left(n^3 + e \cdot (M(qs)\log r \log s \log\log s + q^e R(q)) + S_F(q^e) + \frac{s}{q} R(q)\right).$$

Adding up for the $q-1$ values of i, claim (i) follows.

If $p^2 \nmid n$, then either $q = 1$ and we are in the tame case with cost $O(M(n)\log n)$ (von zur Gathen 1990), or $q = p$ and thus $p \nmid i$ in step 6. Thus no factorization is required, and only steps 1 through 5 and 9 through 11 have to be accounted for. For the better time bound, step 2 is implemented with $O(\frac{s}{q} R_F(q) + M(is)\log t)$ operations, using Newton iteration for all equations

$$tc_{s-k} = a_{st-k}^{1/q} - \operatorname{coeff}(u_k^t, st-k). \quad \square$$

We have used the estimate $O\left(sn^2(\log n \log\log n)^2\right)$ for step 9. With an appropriate Newton iteration, one can in fact implement it with $O(\log r M(s) M(q^e))$ operations in $F^{1/q}$, which improves the first summand in the estimate (i) to $M(n)^2 \log n$.

For $f \in F[x]$ of degree n, r dividing n, and K an algebraic closure of F, let us consider the number

$$d_r = \#\left(\mathrm{s}\overline{\mathrm{DEC}}_{n,r} \cap (\{f\} \times K[x]^2)\right)$$

of simple decompositions of f.

COROLLARY 3.6. *In the above notation, we have* $d_r < 2n$.

PROOF. Writing $r = qt$, $q^e \mid s$, and $q^{e+1} \nmid s$ as usual, we have at most

$$q \cdot \sigma_{e+1} < q \cdot 2q^e \leq 2rs = 2n$$

simple decompositions. □

This result contrasts with Giesbrecht's (1988) examples of polynomials with more than polynomially many (non-simple) decompositions.

COROLLARY 3.7. *For a finite field $F = GF(p^m)$ of characteristic p, algorithm* **Simple decomposition** *for $\overline{\mathrm{sDEC}}_{n,r}$ can be performed with $O(m^3n^4)$ operations in $\mathbf{Z}_p$, and with $O(M(n)M(m)\log n)$ operations if $p^2 \nmid r$. In parallel, it can be implemented on an arithmetic circuit over $\mathbf{Z}_p$ of depth $O(\log^2(mn))$ and size $(mn)^{O(1)}$.*

PROOF. Since we may assume that $p \leq n$, we have $S_F(q^e) = O(n^3)$, and $R_F(q) = O(\log(p^m) + \log q) = O(m \log n)$. For the required parallel algorithms, see von zur Gathen (1984b). □

4. Reducing special factorization to simple decomposition

If $f(0) = g(0) = 0$ 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 $\sigma_{e+1} = 1 + p + \cdots + p^e$ for some $e \geq 1$, $w_0 \neq 0$, and

$$w_i \neq 0 \implies \exists j \leq e+1 \quad i = p^j + p^{j+1} + \cdots + p^e.$$

If $a_1 \neq 0$, then our old friend

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

from Example 2.1 is special, with $e = 2$. It is conjectured that factoring special polynomials is essentially as hard as factoring general polynomials.

THEOREM 4.1. *The problem of factoring special polynomials is linear-time reducible to the decomposition problem.*

PROOF. For $0 \leq j \leq e+1$, let $\tau_j = p^{e+1-j} + p^{e-j} + \cdots + p^e = \sigma_j \cdot p^{e-j+1}$ (with $\tau_0 = 0$), and $w = \sum_{0 \leq j \leq e+1} v_j z^{\tau_j}$ be special and monic. Let

$$a_{p^j} = (-1)^{j+1} v_j, \quad f = \sum_{0 \leq j \leq e+1} a_{p^j} x^{p^j} \in F[x]$$

of degree $n = p^{e+1}$, and let $r = p$, $s = n/p = p^e$. Let K be an algebraic closure of F. We claim:

$$\forall g, h \in K[x] \ \ (f,(g,h)) \in \mathrm{DEC}_{r,s}^K \iff$$

$$\exists \alpha \in K \ \ w(\alpha) = 0 \text{ and } g = x^p + \alpha x \text{ and } h = \sum_{0 \leq j \leq e} c_{p^j} x^{p^j} \text{ and}$$

$$c_{p^e-j}^{p^j} = \sum_{0 \le i \le j} (-1)^i \alpha^{r_i} a_{p^e+1-j+i} \text{ for } 0 \le j \le e. \tag{4.1}$$

This claim implies that the decomposition problem for f requires the output of a representation of each root in K of w (up to conjugates), from which we can read off the complete factorization of w. Since each root α of w is nonzero, each composition factor g is simple.

For "$\Longleftarrow$", one simply checks that (4.1) implies

$$(c_{p^e-j-1}^p + \alpha c_{p^e-j} - a_{p^e-j})^{p^j} = 0,$$

so that

$$c_{p^e-j-1}^p + \alpha c_{p^e-j} = a_{p^e-j} \tag{4.2}$$

for $0 \le j \le e$, $c_{p^e} = 1 = a_n$, and $0 = w(\alpha) = \alpha c_1 - 1$, so that indeed $f = g \circ h$.

For "$\Longrightarrow$", let $(f,(g,h)) \in \mathrm{DEC}_{n,p}^K$. One first checks inductively that $b_{p-1} = \cdots = b_2 = 0$, using that

$$0 = a_{n-is} = \mathrm{coeff}(g \circ h, n - is) = b_{p-i}$$

for $1 \le i \le p-2$. Now $f = g \circ h$ implies equations (4.2), which, together with $b_1 c_1 = a_1$, imply (4.1). □

The definition of "simple decomposition" is in terms of the decomposition factor g, which is part of the output. The following is a sufficient (but not necessary) criterion in terms of the input f for a decomposition to be simple.

PROPOSITION 4.2. *Let $(f,(g,h)) \in \mathrm{DEC}_{n,r}^F$, $p = \mathrm{char}(F)$, $q \ge p$ the largest power of p dividing r, assume $p \nmid s$, and let*

$$l = \min\{\lambda : \lambda = n \text{ or } (a_{n-\lambda} \neq 0 \text{ and } q \nmid \lambda)\}.$$

If $p \nmid l$, then g is simple.

PROOF. As usual, we write $g = x^r + b_{r-i}x^{r-i} + \cdots + b_0$, with $b_{r-i} \neq 0$. We may assume that $1 \le i < q$. Since $q \nmid is$, we have $\mathrm{coeff}(h^r, n - is) = 0$, and thus

$$a_{n-is} = \mathrm{coeff}(b_{r-i}h^{r-i}, n - is) = b_{r-i} \neq 0.$$

Thus $l \le is$, and $p \nmid i$ implies that g is simple. □

Conclusion

While the tame case of polynomial decomposition has found a satisfactory solution, the general wild case remains open. Kozen & Landau (1989) have given an (exponential-time) algorithm over fields with a (polynomial-time) factorization procedure, and the present results show how to compute all simple decompositions in polynomial time. It would be interesting to have more general polynomial-time methods. Giesbrecht's (1988) examples of more than polynomially many decompositions indicate that a totally new approach may be required.

Further directions of research concern decompositions of multivariate polynomials or rational functions, and polynomials over more general rings; most of these questions still need both a mathematical understanding and algorithms. Dickerson (1989) applies polynomial decomposition to the inversion of automorphisms of polynomial rings.

References

V.S. Alagar and M. Thanh, Fast polynomial decomposition algorithms. In Proc. EUROCAL 85, Lecture Notes in Computer Science **204**, Springer Verlag, Heidelberg, 1985, 150-153.

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

D.G. Cantor and E. Kaltofen, Fast multiplication of polynomials over arbitrary rings. Tech. Rep. 87-35, Dept. of Computer Science, Rensselaer Polytechnic Institute, 1987, 16 pp. Acta Inf., to appear.

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.

M. Dickerson, The Inverse of an Automorphism in Polynomial Time. Proc. 30th Ann. IEEE Symp. Foundations of Computer Science, Research Triangle Park NC, 1989, 82-87.

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

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

A. Fröhlich and J.C. Shepherdson, Effective Procedures in Field Theory, Phil. Trans. Royal Soc. Ser. A **248** (1955-56), 407-432.

J. von zur Gathen, Hensel and Newton methods in valuation rings. Math. Comp. **42** (1984a), 637-661.

J. von zur Gathen, Parallel algorithms for algebraic problems. SIAM J. Comput. **13** (1984b), 802-824.

J. von zur Gathen, Functional decomposition of polynomials: the tame case. J. Symb. Comp. **9** (1990), 281-299.

J. von zur Gathen, S. Landau, and D. Kozen, Functional decomposition of polynomials. Proc. 28th Ann. IEEE Symp. Foundations of Computer Science, Los Angeles CA, 1987, 127-131.

M. Giesbrecht, Some results on the functional decomposition of polynomials. Tech. Rep. 209/88, Dept. of Computer Science, University of Toronto, 1988.

J. Gutiérrez, T. Recio, and C. Ruíz de Velasco, Polynomial decomposition algorithm of almost quadratic complexity. Springer Lecture Notes in Comp. Sci. **357** (1989), 471-476.

H. Hasse, *Number Theory*. Grundlehren der math. Wiss. **229**, Springer Verlag, 1980.

D. Kozen and S. Landau, Polynomial decomposition algorithms. J. Symb. Comp. **7** (1989), 445-456.

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

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

A. Schönhage and V. Strassen, Schnelle Multiplikation grosser Zahlen. Computing **7** (1971), 281-292.