The Number of Decomposable Univariate Polynomials

Extended Abstract

Joachim von zur Gathen
B-IT, Universität Bonn, 53113 Bonn, Germany
gathen@bit.uni-bonn.de
http://cosec.bit.uni-bonn.de/

JOACHIM VON ZUR GATHEN (2009). The Number of Decomposable Univariate Polynomials — Extended Abstract. In *Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation ISSAC '09, Seoul, Korea*, JOHN P. MAY, editor, 359–366. ACM Press. ISBN 978-1-60558-609-0. Preprint (2008) available at http://arxiv.org/abs/0901.0054. Full version in *Combinatorics, Probability and Computing* (2014), Special Issue, to appear.

ABSTRACT

A univariate polynomial f over a field is *decomposable* if it is the composition $f = g \circ h$ of two polynomials g and h whose degree is at least 2. We determine an approximation to the number of decomposable polynomials over a finite field. The tame case, where the field characteristic p does not divide the degree n of f, is reasonably well understood, and we obtain exponentially decreasing error bounds.

The wild case, where p divides n, is more challenging and our error bounds are weaker. A centerpiece of our approach is a decomposition algorithm in the wild case, which shows that sufficiently many polynomials are decomposable.

Categories and Subject Descriptors: F.2.1 [Numerical Algorithms and Problems]: Computations in finite fields; G.2.1 [Combinatorics]: Counting problems; I.1.2 [Algorithms]: Algebraic algorithms.

General Terms: Algorithms.

Keywords: computer algebra, polynomial decomposition, finite fields, combinatorics on polynomials

1. INTRODUCTION

It is intuitively clear that the decomposable polynomials form a small minority among all polynomials (univariate over a field). The goal in this work is to give a quantitative version of this intuition. That is, we want to approximate the number of decomposables over a finite field, together with a good relative error bound.

For this task, one readily obtains an upper bound. The challenge then is to find an essentially matching lower bound. Von zur Gathen (1990a,b) introduced the notion of *tame* for the case where the field characteristic does not divide the degree n, and *wild* for the complementary case, in analogy with ramification indices. Algorithmically, the tame case is well understood since the breakthrough result of Kozen & Landau (1986); see also von zur Gathen, Kozen & Landau (1987); Kozen & Landau (1989); Kozen, Landau & Zippel (1996); Gutierrez & Sevilla (2006), and the survey articles of von zur Gathen (2002) and Gutierrez & Kozen (2003) with further references. It is not hard to identify the two main contributions to the decomposable polynomials. These correspond to left components of degree ℓ and n/ℓ, where ℓ is the smallest prime divisor of the composite number n. An upper bound on the two contributions is immediate, and on all decomposables it follows with the method of von zur Gathen (2008a).

In the tame case, a lower bound on each of the two contributions is again easy, and Ritt's Second Theorem provides an upper bound on their intersection. Together this yields a lower bound on the number of decomposables. It differs from the upper bound only by a relative error which is exponentially decreasing.

In the wild case, the methods from the literature do not yield a satisfactory lower bound. We present in Section 3 a decomposition algorithm which fails on some inputs but works on sufficiently many ones. The algorithm is a centerpiece of this paper and yields lower bounds on the size of the two main contributions in the wild case.

The intersection of the two main contributions corresponds to "collisions", where different pairs of components yield the same composition. Ritt's Second Theorem describes these collisions. Section 4 provides a normal form for the quantities in this Theorem, yielding the exact number of such collisions in the tame case, assuming that $\ell^2 \nmid n$. Furthermore, we give (less precise) substitutes in those cases where the Theorem is not applicable.

Section 5 presents the resulting estimates in the tame case. Section 6 puts together all our bounds in the general case, resulting in a veritable jungle of case distinctions. It is not clear whether this is the nature of the problem or an artifact of our approach. Theorem 26 provides a précis of our results.

The upper and lower bounds in the tame case differ by a factor of $1 + \epsilon$, with ϵ exponentially decreasing in the input size $n \log q$, in the tame case and for growing $n/3\ell^2$. When the field characteristic is the smallest prime divisor of n and divides n exactly twice, then we have a factor of at most 2. In all other cases, the factor is $1 + O(q^{-1})$ over $\mathbb{F}_q$. It remains a challenge whether these gaps can be reduced.

Giesbrecht (1988) was the first to consider our counting problem. He showed that the decomposable polynomials form an exponentially small fraction of all univariate polynomials. My interest, dating back to the supervision of this thesis, was rekindled by a study of similar (but multivariate) counting problems (von zur Gathen 2008a) and during a visit to Pierre Dèbes' group at Lille, where I received a preliminary version of Bodin, Dèbes & Najib (2009). Multivariate decomposable polynomials are counted in von zur Gathen (2008b).

We use the methods from von zur Gathen (2008a), where the corresponding counting task was solved for reducible, squareful, relatively irreducible, and singular bivariate polynomials. Von zur Gathen, Viola & Ziegler (2009) extend those results to multivariate polynomials, and also provide (impractical) exact formulas, and (practical) generating functions. Further work on collisions is reported in von zur Gathen *et al.* (2009a).

2. DECOMPOSITIONS

A nonzero polynomial $f \in F[x]$ over a field F is *monic* if its leading coefficient $\mathrm{lc}(f)$ equals 1. We call f *original* if its graph contains the origin, that is, $f(0) = 0$.

Definition 1. *For $g, h \in F[x]$,*

$$f = g \circ h = g(h) \in F[x]$$

is their composition. *If $\deg g, \deg h \geq 2$, then (g, h) is a* decomposition *of f. A polynomial $f \in F[x]$ is* decomposable *if there exist such g and h, otherwise f is* indecomposable. *The decomposition (g, h) is* normal *if h is monic and original.*

Remark 2. *Multiplication by a unit or addition of a constant does not change decomposability, since*

$$f = g \circ h \Longleftrightarrow af + b = (ag + b) \circ h$$

for all f, g, h as above and $a, b \in F$ with $a \neq 0$. Any decomposition (g, h) can be normalized by this action.

We fix some notation for the remainder of this paper. For $n \geq 0$, we write

$$P_n = \{f \in F[x] \colon \deg f \leq n\}$$

for the vector space of polynomials of degree at most n, of dimension $n + 1$. Furthermore, we consider the subsets

$$P_n^{=} = \{f \in P_n \colon \deg f = n\},$$
$$P_n^{0} = \{f \in P_n^{=} \colon f \text{ monic and original}\}.$$

For any divisor e of n, we have the normal composition map

$$\gamma_{n,e} \colon \begin{array}{ccc} P_e^{=} \times P_{n/e}^{0} & \longrightarrow & P_n^{=}, \\ (g, h) & \longmapsto & g \circ h, \end{array}$$

corresponding to Definition 1, and set

$$D_{n,e} = \operatorname{im} \gamma_{n,e}.$$

The set D_n of all decomposable polynomials in $P_n^{=}$ is

$$D_n = \bigcup_{\substack{e \mid n \\ 1 < e < n}} D_{n,e}.$$

In particular, $D_n = \varnothing$ if n is prime. We also let $I_n = P_n^{=} \setminus D_n$ be the set of indecomposable polynomials. Over a finite field $\mathbb{F}_q$ with q elements, we have

$$\#P_n^{=} = q^{n+1}(1 - q^{-1}),$$
$$\#P_n^{0} = q^{n-1},$$
$$\#D_{n,e} \leq q^{e+n/e}(1 - q^{-1}).$$

3. EQUAL-DEGREE COLLISIONS

For decompositions $f = g \circ h$ over a field of characteristic p, one has to distinguish between the cases where p does not divide $\deg g$ and where it does. There are linearized polynomials with superpolynomially many "inequivalent" decompositions (Giesbrecht 1988).

Fact 3. *Let F be a field of characteristic p, and e a divisor of $n \geq 2$. If p does not divide e, then $\gamma_{n,e}$ is injective, and*

$$\#D_{n,e} = q^{e+n/e}(1 - q^{-1}).$$

In Section 5, we find an upper bound α_n on $\#D_n$, up to some small relative error. When the exact size of the error term is not a concern, then this is quite easy. Furthermore, Fact 3 immediately yields a lower bound of $\alpha_n/2$ if p is not the smallest prime divisor ℓ of n. A result of von zur Gathen (1990b) implies a lower bound of about $\alpha_n/4n$ in general.

Our goal in this paper is to improve these estimates. For this purpose, we have to address the uniqueness (or lack thereof) of normal compositions

$$g \circ h = g^* \circ h^* \tag{4}$$

in two situations. We call $\{(g, h), (g^*, h^*)\}$ satisfying (4) with $h \neq h^*$ an *equal-degree collision* if $\deg g = \deg g^*$ (and hence $\deg h = \deg h^*$), and a *distinct-degree collision* if $\deg g = \deg h^* \neq \deg h$ (and hence $\deg h = \deg g^*$). The present section deals with equal-degree collisions, and Section 4 with distinct-degree collisions.

By Fact 3, there are no equal-degree collisions when $p \nmid \deg g$. In the more interesting case $p \mid \deg g$, collisions are well-known to exist. Our goal, then, is to show that there are few of them, so that the decomposable polynomials are still numerous. Algorithm 7 provides a constructive proof of this. For many, but not all, (g, h) it reconstructs (g, h) from $g \circ h$. To quantify the benefit provided by the algorithm, we rely on a result by Antonia Bluher (2004).

Distinct-degree collisions are classically taken care of by Ritt's Second Theorem. This is the topic of Section 4.

Von zur Gathen (1990b) presents an algorithm for a "wild" decomposition $f = g \circ h$ with

$$\deg f = n = k \cdot m = \deg g \cdot \deg h$$

and $p \mid k$, under some restrictions. It first makes coefficient comparisons to compute h, and then a Taylor expansion to find g. We now take a simplified version of that method. It does not work for all inputs, but for sufficiently many for our counting purpose. In the literal sense, it is not an algorithm; it can be made into one by solving the corresponding system of polynomial equations in the unknown coefficients in cases of "failure", but this is not relevant for the present study.

For any $f \in F[x^p]$ there exist $g, h \in F[x]$ with $f = x^p \circ h = g \circ x^p$. We call such an f a *Frobenius composition* and let $D_n^{+} = D_n \setminus F[x^p]$ be the set of non-Frobenius compositions.

To fix some notation, we have integers

$$d \geq 1,\ r = p^d,\ k = ar,\ m \geq 2,\ n = km,$$
$$\kappa \text{ with } 0 \leq \kappa < k \text{ and } p \nmid a\kappa,$$

and polynomials

$$g = x^k + \sum_{1 \le i \le \kappa} g_i x^i,$$
$$h = \sum_{1 \le i \le m} h_i x^i, \qquad (5)$$
$$f = g \circ h = h^k + \sum_{1 \le i \le \kappa} g_i h^i,$$

with $h_m = 1$, $h_{m-1} \neq 0$, and either $g_\kappa \neq 0$ or $g = x^k$; the latter case corresponds to $\kappa = 0$. The idea is to compute h_i for $i = m-1, m-2, \ldots, 1$ by comparing the known coefficients of f to the unknown ones of h^k and $g_\kappa h^\kappa$. Special situations arise when the latter two polynomials both contribute to a coefficient. We denote by

$$h^{(i)} = \sum_{i<b<m} h_b x^b$$

the top part of h, so that $h^{(m-1)} = 0$. Furthermore, we write $\mathrm{coeff}(v, j)$ for the coefficient of x^j in a polynomial v, and

$$c_{i,j}(v) = \mathrm{coeff}(v \circ (h - h^{(i)}), j).$$

Thus $c_{m-1,j}(x^k) = \mathrm{coeff}(h^k, j)$, and in particular, we have $c_{m-1,j}(g) = f_j$ for all j. To illustrate the usage of these c_{ij}, we consider E_1 below. At some point in the algorithm, we have determined $g_\kappa, h_m, \ldots, h_{i+1}$. The appropriate c_{ij} exhibits h_i in a simple fashion, meaning that we can compute it from f_j and $h^{(i)}$. Lastly we define the rational number

$$i_0 = m\left(\frac{\kappa - a}{r-1} - a + 1\right) = \frac{\kappa m - n}{r-1} + m;$$

thus $i_0 < m$, and i_0 is an integer if and only if

$$r - 1 \mid (\kappa - a)m.$$

Lemma 6. *For $1 \le i \le m$ and $0 \le j \le n$, we have the following.*

E_1: *If $i < m$, then*

$$c_{i,(\kappa-1)m+i}(g_\kappa x^\kappa) = \kappa g_\kappa h_i,$$

and $c_{m-1,\kappa m}(g_\kappa x^\kappa) = g_\kappa$.

E_2: *If $i < m$, then*

$$c_{i,n-r(m-i)}(x^k) = a h_i^r.$$

If $r \nmid j$, then $\mathrm{coeff}(h^k, j) = 0$.

E_3: *If $i_0 \in \mathbb{N}$, then*

$$c_{i_0,(\kappa-1)m+i_0}(x^k + g_\kappa x^\kappa) = a h_{i_0}^r + \kappa g_\kappa h_{i_0}.$$

E_4: *If $m = r$ and $\kappa = k - 1$, then*

$$c_{m-1,\kappa m}(x^k + g_\kappa x^\kappa) = a h_{m-1}^r + g_\kappa,$$
$$c_{m-1,\kappa m-1}(x^k + g_\kappa x^\kappa) = -g_\kappa h_{m-1}.$$

In the following algorithm, the instruction "determine h_i (or g_κ) by E_μ (at x^j)", for $1 \le \mu \le 4$, means that the property E_μ involves some quantity $c_{ij}(\cdot)$ which is a summand in $\mathrm{coeff}(g \circ h, j) = f_j$, the other summands are already known, and we can solve for h_i (or g_κ). The main effort in the correctness proof is to show that all data required are available at that point in the algorithm, and that the equation can indeed be solved. The algorithm's basic structure is driven by the relationship between the degrees κm of $g_\kappa h^\kappa$ and $n - r$ of $h^k - x^n$. We note that since r is a power of p, any $b \in \mathbb{F}_q$ is determined by b^r.

Algorithm 7. Wild decomposition.

Input: $f \in \mathbb{F}_q[x]$ monic and original of degree $n = km$, where $p = \mathrm{char}\,\mathbb{F}_q$, $d \ge 1$, $r = p^d$, and $k = ar$ with $p \nmid a$.

Output: Either a set of at most $r + 1$ pairs (g, h) with $g, h \in \mathbb{F}_q[x]$ monic and original of degrees k, m, respectively, and $f = g \circ h$, or "failure".

1. Let j be the largest integer for which $f_j \neq 0$ and $p \nmid j$. If no such j exists then if $d \ge 2$ call Algorithm 7 recursively and else call a tame decomposition algorithm, in either case with input $f^* = f^{1/p}$ and $k^* = k/p$. If a set of (g^*, h^*) is output by the call, then return the set of all Frobenius compositions $(x^p \circ g^*, h^*)$.
2. If $p \nmid m$ then if $m \nmid j$ then return "failure" else set $\kappa = j/m$. If $p \mid m$ then if $m \nmid j+1$ then return "failure" else set $\kappa = (j+1)/m$. If $p \mid \kappa$, then return "failure". Calculate $i_0 = (\kappa m - n)/(r-1) + m$.
3. If $\kappa m \ge n - r + 2$ then do the following.
   - a. Set $g_\kappa = f_{\kappa m}$.
   - b. Determine h_i for $i = m-1, \ldots, 1$ by E_1.
4. If $\kappa m = n - r + 1$ then do the following.
   - a. Set $g_\kappa = f_{\kappa m}$.
   - b. Determine h_{m-1} by E_3. If E_3 does not have a unique solution, then return "failure".
   - c. Determine h_i for $i = m-2, \ldots, 1$ by E_1.
5. If $\kappa m = n - r$ then do the following.
   - a. Determine h_{m-1} by E_4, in the following way. Compute the set S of all nonzero $s \in \mathbb{F}_q$ with
     $$a s^{r+1} - f_{\kappa m} s - f_{\kappa m - 1} = 0. \qquad (8)$$
     If $S = \varnothing$ then return the empty set, else do steps 5.b and 5.c for all $s \in S$, setting $h_{m-1} = s$.
   - b. Determine g_κ by E_1 and E_2 at $x^{\kappa m}$, from $f_{\kappa m} = a h_{m-1}^r + g_\kappa$.
   - c. For $i = m-2, \ldots, 1$ determine h_i by E_1.
6. If $\kappa m < n - r$ then do the following.
   - a. Determine h_{m-1} by E_2.
   - b. If $r \nmid m$ then determine g_κ by E_1 at $x^{\kappa m}$ (as $g_\kappa = f_{\kappa m}$), else by E_1 at $x^{\kappa m - 1}$ (via $\kappa g_\kappa h_{m-1} = f_{\kappa m - 1}$).
   - c. Determine h_i for decreasing i with $m - 2 \ge i > i_0$ by E_2.
   - d. If i_0 is a positive integer, then determine h_{i_0} by E_3. If E_3 does not yield a unique solution, then return "failure".
   - e. Determine h_i for decreasing i with $i_0 > i \ge 1$ by E_1.

[We now know h.]

7. Compute the remaining coefficients $g_1, \ldots, g_{\kappa-1}$ as the "Taylor coefficients" of f in base h.

8. Return the set of all (g, h) for which $g \circ h = f$. If there are none, then return the empty set.

The Taylor expansion method determines for given f and h the unique g (if one exists) so that $f = g \circ h$; see von zur Gathen (1990a).

We first illustrate the algorithm in some examples.

Example 9. We let $p = 5$, $n = 50$, and $k = r = 5$, so that $a = d = 1$ and $m = 10$, and start with $\kappa = 4 = r - 1$. We assume $f_{39} = g_4 h_9 \neq 0$. Then

$$\begin{aligned} h^5 + g_4 h^4 &= x^{50} + h_9^5 x^{45} + (h_8^5 + g_4) x^{40} + 4 g_4 h_9 x^{39} \\ &+ g_4 (4h_8 + h_9^2) x^{38} + x^{36} \cdot O(x) + (h_7^5 + g_4 (4h_5 + h_9 h_6 \\ &+ h_8 h_7 + h_9^2 h_7 + h_9 h_8^2 + h_9^3 h_8)) x^{35} + O(x^{34}). \end{aligned}$$

Step 1 determines $j = 39$, and step 2 finds $\kappa = (39+1)/10$ and $i_0 = 15/2 \notin \mathbb{N}$. Since $\kappa m = 40 < 45 = n - r$, we go to step 6. Step 6.a computes h_9 at x^{45}, step 6.b yields g_4 at x^{39}, step 6.c determines h_8 at x^{40} by E_2, step 6.d is skipped, and then step 6.e yields $h_7, \ldots, h_1$ at $x^{37}, \ldots, x^{31}$, respectively, all using E_1. Step 7 determines g_1, g_2, g_3, and step 8 checks whether indeed $f = g \circ h$, and if so, returns (g, h).

With the same values, except that $\kappa = 3$, we have

$$\begin{aligned} h^5 + g_3 h^3 = x^{50} &+ h_9^5 x^{45} + h_8^5 x^{40} + h_7^5 x^{35} \\ &+ (h_6^5 + g_3) x^{30} + 3 g_3 h_9 x^{29} + g_3 (3h_9^2 + 3h_8) x^{28} \\ &+ x^{26} \cdot O(x) + (h_5^5 + g_3 (3h_5 + 3h_9 h_6 + 3h_8 h_7 \\ &+ 3h_9^2 h_7 + 3h_9 h_8^2)) x^{25} + O(x^{24}). \end{aligned}$$

Assuming that $f_{29} = 3 g_3 h_9 \neq 0$, the algorithm computes $j = 29$, $\kappa = (29 + 1)/10$, $i_0 = 5 \in \mathbb{N}$, goes to step 6, determines h_9 at x^{45}, g_3 at x^{29}, h_8, h_7, h_6 according to E_2, then h_5 at x^{25} via the known value for $h_5^5 + 3 g_3 h_5$ in step 6.d with E_3. Condition (11) below requires that $(-3g_3)^{(q-1)/4} \neq 1$ and guarantees that h_5 is uniquely determined, as shown in the proof of Theorem 10 below. Finally $h_4, \ldots, h_1$ and g_1, g_2 are computed.

As a last example, we take $p = 5$, $n = 25$, $k = r = m = 5$ and $\kappa = 4$, so that $a = 1$ and

$$h^5 + g_4 h^4 = x^{25} + (h_4^5 + g_4) x^{20} + 4 g_4 h_4 x^{19} + O(x^{18}).$$

Again we assume $f_{19} = 4 g_4 h_4 \neq 0$. Then steps 1 and 2 determine $j = 19$, $\kappa = 4$, and $i_0 = 15/4 \notin \mathbb{N}$. We have $\kappa m = 20 = n - r$, so that we go to step 5. In step 5.a, we have to solve (8). The number of solutions depends on the field. Over $\mathbb{F}_{125}$, we have the following numbers of nonzero solutions s when $f_{20} \neq 0$:

$$\begin{cases} 6 & \text{for } 1 \cdot 124 \text{ values } (f_{20}, f_{19}), \\ 2 & \text{for } 47 \cdot 124 \text{ values } (f_{20}, f_{19}), \\ 1 & \text{for } 25 \cdot 124 \text{ values } (f_{20}, f_{19}), \\ 0 & \text{for } 52 \cdot 124 \text{ values } (f_{20}, f_{19}), \end{cases}$$

and when $f_{20} = 0$:

$$\begin{cases} 2 & \text{for } 62 \text{ values of } f_{19}, \text{ namely the squares}, \\ 0 & \text{for } 62 \text{ values of } f_{19}. \end{cases}$$

We run the remaining steps in parallel for each value $h_4 = s$ with $s \in S$. This yields g_4 in step 5.b, h_3, h_2, h_1 in step 5.c, and g_1, g_2, g_3 in step 7. $\diamondsuit$

We denote by $\mathsf{M}(n)$ a multiplication time, so that polynomials of degree at most n can be multiplied with $\mathsf{M}(n)$ operations in $\mathbb{F}_q$. Then $\mathsf{M}(n)$ is in $O(n \log n \operatorname{loglog} n)$; see von zur Gathen & Gerhard (2003), Chapter 8, and Fürer (2007) for an improvement.

For an input f, we set $\sigma(f) = \#S$ if the precondition of step 5 is satisfied and S computed there, and otherwise $\sigma(f) = 1$.

Theorem 10. *Let f be an input polynomial with parameters n, p, $q = p^e$, d, r, a, k, m as specified, g, h, κ, i_0 as in 5 and 3, so that $f = g \circ h$, set $c = \gcd(d, e)$ and suppose further that*

$$\text{if } i_0 \in \mathbb{N} \text{ and } 1 \leq i_0 < m, \text{ then } (-\kappa g_\kappa / a)^{(q-1)/(p^c - 1)} \neq 1. \tag{11}$$

On input f, Algorithm 7 returns either "failure" or a set of at most $\sigma(f)$ normal decompositions (g^*, h^*) of f, and (g, h) is one of them. Except if returned in step 1, none of them is a Frobenius decomposition. The algorithm uses

$$O\big(\mathsf{M}(n) \log k \, (m + \log(kq))\big)$$

or $O^\sim(n(m + \log q))$ operations in $\mathbb{F}_q$.

Proof. Since $r = p^d \mid k$, we have $\operatorname{coeff}(h^k, j) = 0$ unless $r \mid j$. Furthermore $g_\kappa h^\kappa = g_\kappa x^{\kappa m} + \kappa g_\kappa h_{m-1} x^{\kappa m - 1} + O(x^{\kappa m - 2})$ and $\kappa g_\kappa h_{m-1} \neq 0$, so that j from step 1 equals κm (if $p \nmid m$) or $\kappa m - 1$ (if $p \mid m$). Thus κ is correctly determined in step 2. In particular, f is not a Frobenius composition.

We denote by G the set of (g, h) allowed in the theorem. We claim that the equations used in the algorithm involve only coefficients of f and previously computed values, and usually have a unique solution. It follows that most $f \in \gamma_{n,k}(G)$ are correctly and uniquely decomposed by the algorithm. The only exception to the uniqueness occurs in (8).

In the remaining steps, we use various coefficients f_j for $j = (\kappa - 1)m + i$ with $1 \leq i \leq m$ or $j = n - r(m - i)$ with $i_0 \leq i < m$. The value i_0 is defined so that $n - r(m - i_0) = (\kappa - 1)m + i_0$, and thus

$$n - r(m - i) \geq (\kappa - 1)m + i \text{ if and only if } i \geq i_0,$$

since the first linear function in i has the slope $r > 1$, greater than for the second one. Since $i \geq 1$, it follows that $j > (\kappa - 1)m$ for all j under consideration. For the low-degree part of g we have

$$\deg((g - (x^k + g_\kappa x^\kappa)) \circ h) \leq (\kappa - 1)m < j,$$

so that

$$f_j = \operatorname{coeff}(g \circ h, j) = \operatorname{coeff}(h^k + g_\kappa h^\kappa, j)$$

for all j in the algorithm.

We have to see that the application of E_3 in steps 4.b (where $i_0 = m-1$) and 6.d (where $m-2 \geq i_0 \geq 1$) always has a unique solution. The right hand side of E_3, say $as^r + \kappa g_\kappa s$, is an $\mathbb{F}_p$-linear function of s. The equation has a unique solution if and only if its kernel is $\{0\}$. (Segre 1964, Teil 1, § 3, and Wan 1990 provide an explicit solution in this case.) But when $s \in \mathbb{F}_q$ is nonzero with $as^r + \kappa g_\kappa s = 0$, then $-\kappa g_\kappa / a = s^{r-1}$. Writing $z = p^c$, so that $z - 1 = \gcd(q - 1, r - 1)$, we have

$$(-\kappa g_\kappa / a)^{(q-1)/(z-1)} = (s^{r-1})^{(q-1)/(z-1)} = 1,$$

contradicting the condition (11).

For the correctness it is sufficient to show that all required quantities are known, in particular $c_{i,j}(g_\kappa x^\kappa)$ in E_1 and $c_{i,j}(x^k)$ in E_2, and that the equations determine the coefficient to be computed. We have

$$\deg(h^k - x^n) = \deg((h^a - x^{am})^r) \le (am-1)r = n - r,$$

so that $g_\kappa = f_{\kappa m}$ in steps 3.a and 4.a. The precondition of step 3 implies that for all $i < m$ we have

$$(\kappa - 1)m \ge n - r - m + 2 > n - rm + (r-1)i,$$

$$n - r(m-i) < (\kappa - 1)m + i.$$

Thus from E_1 we have with $j = (\kappa-1)m - i$

$$\begin{aligned} f_{(\kappa-1)m+i} &= \mathrm{coeff}(h^k, j) + \mathrm{coeff}(g_\kappa h^\kappa, j) \\ &= \mathrm{coeff}((h^{(i)})^k, j) + \kappa g_\kappa h_i \end{aligned}$$

with $\kappa g_\kappa \ne 0$, so that h_i can be computed in step 3.b.

The precondition in step 4 implies that $i_0 = m-1$, and hence $(r-1) \mid (a-\kappa)m$. E_3 says that $f_{\kappa m-1} = c_{m-1,\kappa m-1}(x^k + g_\kappa x^\kappa) = a h_{m-1}^r + \kappa g_\kappa h_{m-1}$. We have seen above that under our assumptions the equation $f_{\kappa m-1} = as^r + \kappa g_\kappa s$ has exactly one solution s. By an argument as for step 3.b, also step 4.c works correctly.

The only usage of E_4 occurs in step 5.a, where $\kappa = (n-r)/m = k - r/m$. Since $p \mid k$, r is a power of p, and $p \nmid \kappa$, this implies that $r = m$ and $\kappa = k-1$. We have from E_4

$$\begin{aligned} f_{\kappa m} &= a h_{m-1}^r + g_\kappa, \\ f_{\kappa m-1} &= g_\kappa h_{m-1} = a h_{m-1}^{r+1} - f_{\kappa m} h_{m-1}. \end{aligned}$$

Thus $h_{m-1} \in S$ as computed in step 5.a and g_κ is correctly determined in step 5.b. The precondition of step 5 implies that $i_0 = m - 1 - 1/(r-1)$, which is an integer only for $r = 2$. In that case, $i_0 = m-2 = 0$ and no further h_i is needed. Otherwise, $m-2 < i_0 < m-1$ and step 5.c works correctly since $i < i_0$.

The precondition of step 6 implies that $i_0 < m-1$. If $r \nmid m$, then $\mathrm{coeff}(h^k, \kappa m) = 0$ by E_2, and otherwise $\mathrm{coeff}(h^k, \kappa m - 1) = 0$. Thus g_κ is correctly computed in step 6.b. Correctness of the remaining steps follows as above.

For the cost of the algorithm, two contributions are from calculating $(h^{(j)})^\kappa$ for some $j < m$ and the various rth roots. The first comes to $O(m \cdot \log \kappa \cdot \mathsf{M}(n))$ and the second one to $O(m \cdot \log_p q)$ operations in $\mathbb{F}_q$. E_3 and E_4 are applied at most once. We then have to find all roots of a univariate polynomial of degree at most $r+1$. This can be done with $O(\mathsf{M}(r) \log r \log rq)$ operations (see von zur Gathen & Gerhard (2003), Corollary 14.16). The Taylor coefficients in step 7 can be calculated with $O(\mathsf{M}(n) \log k)$ operations (see von zur Gathen & Gerhard (2003), Theorem 9.15). All other costs are dominated by these contributions, and we find the total cost as

$$O\big(\mathsf{M}(n) \log k \cdot (m + \log(kq))\big). \qquad \square$$

Our next task is to determine the number N of decomposable f obtained as $g \circ h$ in Theorem 10. Since (8) is an equation of degree $r+1$, it has at most $r+1$ solutions, and $\sigma(f) \le r+1$. N is at least the number of (g,h) permitted by Theorem 10, divided by $r+1$.

Fortunately, Bluher (2004) has studied the equation (8) and determined exactly its solution statistics. Her results can be used to derive the following lower bounds.

Corollary 12. *Let $\mathbb{F}_q$ have characteristic p with $q = p^e$, and take integers $d \ge 1$, $r = p^d$, $\ell = ar$ with $p \nmid a$, $m \ge 2$, $n = \ell m$, $c = \gcd(d,e)$, $z = p^c$, $\mu = \gcd(r-1, m)$, $r^* = (r-1)/\mu$, and let G consist of the (g,h) as in Theorem 10. Then we have the following lower bounds on the cardinality of $\gamma_{n,\ell}(G)$.*

(i) If $r \ne m$ and $\mu = 1$:

$$q^{\ell+m}(1-q^{-1})(1-q^{-\ell})(1-q^{-1}(1+q^{-p+2}\frac{(1-q^{-1})^2}{1-q^{-p}})).$$

(ii) If $r \ne m$:

$$\begin{aligned} &q^{\ell+m}(1-q^{-1}) \\ &\big((1-q^{-1}(1+q^{-p+2}\frac{(1-q^{-1})^2}{1-q^{-p}}))(1-q^{-\ell}) \\ &\quad - q^{-\ell-r^*-c/e+2}\frac{(1-q^{-1})^2(1-q^{-r^*(\mu-1)})}{(1-q^{-c/e})(1-q^{-r^*})} \\ &\quad (1+q^{-r^*(p-2)})\big). \end{aligned}$$

(iii) If $r = m$:

$$\begin{aligned} &q^{\ell+m}(1-q^{-1})^2(\frac{1}{2} + \frac{1+q^{-1}}{2z+2} + \frac{q^{-1}}{2} - q^{-\ell}\frac{1-q^{-p+1}}{1-q^{-p}} \\ &\quad - q^{-p+1}\frac{1-q^{-1}}{1-q^{-p}}). \end{aligned}$$

The algorithm works over any field of characteristic p where each element has a pth root; in $\mathbb{F}_q$, this is just the (q/p)th power.

Example 13. When $n = p^2$, then we have $\ell = r = m = p$ in Corollary 12(iii), and including the Frobenius compositions $x^p \circ h$, we obtain

$$\#D_n \ge \alpha_n \cdot \big(\frac{1}{2}(1 + \frac{1}{p+1})(1-q^{-2}) + q^{-p}\big).$$

In characteristic 2, the estimate is exact, since we have accounted for all compositions and a monic original polynomial of degree 2 is determined by its linear coefficient. Thus

$$\begin{aligned} \#D_4 &= \alpha_4 \cdot (\frac{2}{3} \cdot (1-q^{-2}) + q^{-2}) = \alpha_4 \cdot \frac{2+q^{-2}}{3}, \\ \#D_4 &= \frac{3}{4}\alpha_4 \text{ over } \mathbb{F}_2, \\ \#D_4 &= \frac{11}{16}\alpha_4 \text{ over } \mathbb{F}_4. \qquad \diamondsuit \end{aligned}$$

Bodin *et al.* (2009) state without proof that $D_n \approx \frac{3}{4}\alpha_n$ over $\mathbb{F}_2$ for even $n \ge 6$.

4. DISTINCT-DEGREE COLLISIONS

The following are examples of collisions:

$$x^k w^n \circ x^n = x^{kn} w^n(x^n) = x^n \circ x^k w(x^n),$$

for any polynomial $w \in F[x]$, where F is a field (or even a ring), and

$$T_m(x, y^n) \circ T_n(x,y) = T_{mn}(x,y) = T_n(x, y^m) \circ T_m(x,y),$$

where T_n is a *Dickson polynomial*.

Ritt's Second Theorem is the central tool for understanding distinct-degree collisions. It says that under certain conditions the above examples are, up to composition with linear functions, the only distinct-degree collisions. They are called the First Case and Second case, respectively. We use the precise version of Zannier (1993), and the following notation:

$$\deg g = \deg h^* = m, \deg h = \deg g^* = \ell, \tag{14}$$

$$\gcd(m, \ell) = 1, g'(g^*)' \neq 0, \tag{15}$$

$$f = g \circ h = g^* \circ h^*, \text{ all monic original}, \tag{16}$$

where $g' = \partial g / \partial x$ is the derivative of g. We have the following normal form for these collisions.

Theorem 17. *Let F be a field of characteristic p, let $m > \ell \geq 2$ be integers and $n = \ell m$. Furthermore, we have monic original $f, g, h, g^*, h^* \in F[x]$ satisfying (14) through (16). Thus either the First or the Second Case of Ritt's Second Theorem applies.*

(i) In the First Case, there exists a monic polynomial $w \in F[x]$ of degree $s = \lfloor m/\ell \rfloor$ and $c \in F$ so that

$$f = (x - c^{k\ell} w^\ell(c^\ell)) \circ x^{k\ell} w^\ell(x^\ell) \circ (x + c),$$

with $k = m - \ell s$. If $p \nmid n$, then both w and c are uniquely determined by f and ℓ. Furthermore we have

$$\begin{aligned} kw + \ell x w' &\neq 0 \text{ and } p \nmid \ell, & (18)\\ g &= (x - c^{k\ell} w^\ell(c^\ell)) \circ x^k w^\ell \circ (x + c^\ell), \\ h &= (x - c^\ell) \circ x^\ell \circ (x + c), \\ g^* &= (x - c^{k\ell} w^\ell(c^\ell)) \circ x^\ell \circ (x + c^k w(c^\ell)), \\ h^* &= (x - c^k w(c^\ell)) \circ x^k w(x^\ell) \circ (x + c). \end{aligned}$$

Conversely, any (w, c) for which (18) holds yields a collision satisfying (14) through (16) via the above formulas.

(ii) In the Second Case, there exist $b, z \in F$ with $z \neq 0$ so that

$$f = (x - T_n(b, z)) \circ T_n(x, z) \circ (x + b).$$

Now (b, z) is uniquely determined by f. Furthermore we have

$$\begin{aligned} &p \nmid n, & (19)\\ g &= (x - T_n(b, z)) \circ T_m(x, z^\ell) \circ (x + T_\ell(b, z)), \\ h &= (x - T_\ell(b, z)) \circ T_\ell(x, z) \circ (x + b), \\ g^* &= (x - T_n(b, z)) \circ T_\ell(x, z^m) \circ (x + T_m(b, z)), \\ h^* &= (x - T_m(b, z)) \circ T_m(x, z) \circ (x + b). \end{aligned}$$

Conversely, if (19) holds, then any (b, z) as above yields a collision satisfying (14) through (16) via the above formulas.

(iii) When $\ell \geq 3$, the First and Second Cases are mutually exclusive. For $\ell = 2$, the Second Case is included in the First Case.

This normal form can be generalized to the case where $g'(g^*)' = 0$.

Corollary 20. *Let $\mathbb{F}_q$ be a finite field of characteristic p, let ℓ and m be integers with $m > \ell \geq 2$ and $\gcd(\ell, m) = 1$, $n = \ell m$, $s = \lfloor m/\ell \rfloor$, and $t = \#(D_{n,\ell} \cap D_{n,m} \cap D_n^+)$. Using Kronecker's δ, the following hold.*

(i) If $p \nmid n$, then

$$t = (q^{s+3} + (1 - \delta_{\ell,2})(q^4 - q^3))(1 - q^{-1}).$$

(ii) If $p \mid \ell$, then $t = 0$.

In the case disallowed in the above, namely when $\gcd(\ell, m) \neq 1$, we find the following bounds.

Theorem 21. *Let $\mathbb{F}_q$ be a finite field of characteristic p, let ℓ be a prime number, $m \neq \ell$ a multiple of ℓ with $p \nmid m$ and without a prime divisor less than ℓ, and set $n = \ell m$ and $t = \#(D_{n,\ell} \cap D_{n,m})$. Then the following hold.*

(i) If $n \neq \ell^3$, then

$$\begin{aligned} q^{2\ell + n/\ell^2 - 1}(1 - q^{-1}) &\leq t \\ &\leq 2q^{2\ell + n/\ell^2 - 1}(1 - q^{-1})(1 + q^{-n/3\ell^3}). \end{aligned}$$

(ii) If $n = \ell^3$, then $t = q^{3\ell - 1}(1 - q^{-1})$.

Theorem 22. *Let $\mathbb{F}_q$ be a finite field of characteristic p, ℓ a prime number dividing $m > \ell$, assume that $p \mid n = \ell m$, and set $t = \#(D_{n,\ell} \cap D_{n,m} \cap D_n^+)$. Then the following hold.*

(i) If $p \neq \ell$, then

$$t \leq q^{m + \lfloor \ell/p \rfloor + 1}(1 - q^{-1}).$$

(ii) If $p = \ell$, then

$$t \leq q^{m + p - m/p + \lfloor m/p^2 \rfloor + 1}(1 - q^{-1}).$$

Giesbrecht (1988), Theorem 3.8, shows that there exist polynomials of degree n over a field of characteristic p with superpolynomially many decompositions, namely at least $n^{\lambda \log n}$ many, where $\lambda = (6 \log p)^{-1}$.

5. COUNTING TAME DECOMPOSABLE POLYNOMIALS

Giesbrecht (1988) was the first work on our counting problem. He proves an upper bound of $d(n) q^{2+n/2}\ (1 - q^{-1})$ on the number of decomposable polynomials, where $d(n)$ is the number of divisors of n. This is mildly larger than our bound of about $2q^{\ell + n/\ell}(1 - q^{-1})$, with its dependence on ℓ replaced by the "worst case" $\ell = 2$.

Theorem 23. *Let $\mathbb{F}_q$ be a field of characteristic p and with q elements, $n \geq 2$ with $p \nmid n$, ℓ and ℓ_2 the smallest and second smallest nontrivial divisor of n, respectively (with $\ell_2 = 1$ if $n = \ell$ or $n = \ell^2$), $s = \lfloor n/\ell^2 \rfloor$, and*

$$\alpha_n = \begin{cases} 0 & \text{if } n = \ell, \\ q^{2\ell}(1 - q^{-1}) & \text{if } n = \ell^2, \\ 2q^{\ell+n/\ell}(1 - q^{-1}) & \text{otherwise}, \end{cases} \tag{24}$$

$$c = \frac{(n - \ell\ell_2)(\ell_2 - \ell)}{\ell\ell_2},$$

$$\beta_n = \begin{cases} 0 & \text{if } n \in \{\ell, \ell^2, \ell^3, \ell\ell_2\}, \\ \dfrac{q^{-c}}{1 - q^{-1}} & \text{otherwise}, \end{cases}$$

$$\beta_n^* = \frac{q^{-\ell-n/\ell}(q^{s+3} + q^4)}{2}.$$

Then the following hold.

(i) $\#D_n \leq \alpha_n(1 + \beta_n)$.

(ii) $\#I_n \geq \#P_n^= - 2\alpha_n$.

(iii) If $p \neq \ell$, *then* $\#D_{\ell^2} = \alpha_{\ell^2}$.

(iv) If $p \nmid n$ *and* $\ell^2 \nmid n$, *then*

$$\alpha_n(1 - \beta_n^*) \leq \#D_n \leq \alpha_n(1 - q^{-1}\beta_n^* + \beta_n).$$

(v) If $p \nmid n$, *then*

$$\alpha_n(1 - q^{-n/\ell+\ell+n/\ell^2-1}(1 + q^{-n/3\ell^3})) \\ \leq \#D_n \leq \alpha_n(1 - q^{-1}\beta_n^* + \beta_n).$$

6. COUNTING GENERAL DECOMPOSABLE POLYNOMIALS

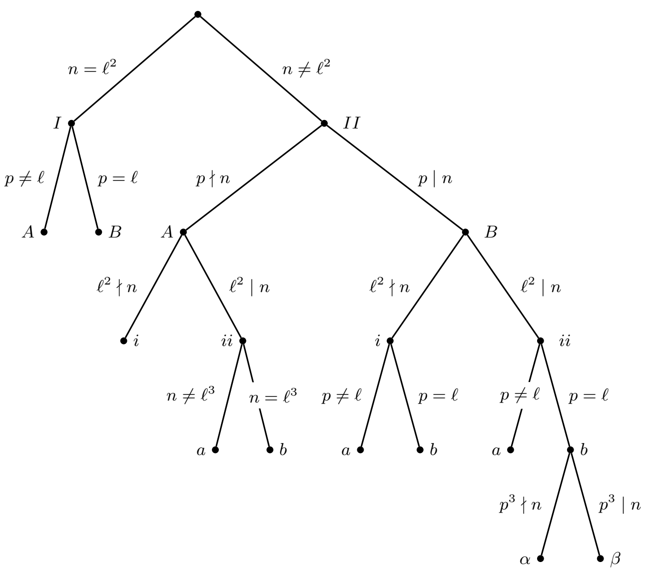

Figure 1: The tree of case distinctions for estimating $\#D_n$.

In the wild case $p \mid n$, we have to deal with an annoyingly large jungle of case distinctions. To keep an overview, we reduce it to the single tree of Figure 1. Its branches correspond to the various bounds on equal-degree collisions (Corollary 12) and on distinct-degree collisions (Section 4). Since at each vertex, the union of all branches includes all cases, the leaves cover all possibilities.

leaf in Figure 1	lower bound on $\#D_n/\alpha_n$	upper
I.A	1	1
I.B	$\frac{1}{2}(1 + \frac{1}{p+1})(1 - q^{-2}) + q^{-p} > 1/2$	1
II.A.i	$1 - \beta_n^* \geq 1 - q^{-n/\ell-\ell+n/\ell^2+3}$	
II.A.ii.a	$1 - 2q^{-n/\ell+\ell+n/\ell^2-1}$	
II.A.ii.b	$1 - q^{-n/\ell+\ell+n/\ell^2-1}$	1
II.B.i.a	$1 - (q^{-1} + q^{-p+1} + q^{-n/\ell-\ell+n/\ell^2+3})/2$	
II.B.i.b	$1 - (q^{-1} - q^{-p})/2$	
II.B.ii.a	$1 - (q^{-1} + q^{-p+1} - q^{-p} + q^{-\ell+1})/2$	1
II.B.ii.b.α	$\frac{1}{2}(\frac{3}{2} + \frac{1}{2p+2} - q^{-1} - \frac{q^{-2}}{2}(1 + \frac{1}{p+1})$ $- \frac{q^{-p+1}}{1-q^{-p}} - \delta_{n,12} \cdot q^{-1})$	
II.B.ii.b.β	$1 - q^{-1} - q^{-p+1}$	1

Table 1: The bounds at the leaves of Figure 1.

Theorem 25. *Let $\mathbb{F}_q$ be a finite field of characteristic p, and ℓ the smallest prime divisor of the composite integer $n \geq 2$. Then we have the following bounds in Table 1 on $\#D_n$ over $\mathbb{F}_q$.*

(i) If the "upper" column in Table 1 contains a 1, then $\#D_n \leq \alpha_n$.

(ii) The lower bounds in Table 1 hold.

The multitude of bounds in Table 1 is quite confusing. Theorem 26 provides simple and universally applicable estimates.

Theorem 26. *Let $\mathbb{F}_q$ be a finite field with q elements and characteristic p, let ℓ be the smallest prime divisor of the composite integer $n \geq 2$, and α_n as in (24). Then the following hold.*

(i) $q^{2\sqrt{n}}/2 \leq \alpha_n < 2q^{n/2+2}$.

(ii) $\alpha_n/2 \leq \#D_n \leq \alpha_n(1 + q^{-n/3\ell^2}) < 2\alpha_n < 4q^{n/2+2}$.

(iii) If $q \geq 5$, *then* $\#D_n \geq (3 - 2q^{-1})\alpha_n/4 \geq q^{2\sqrt{n}}/4$.

(iv) If $\ell \neq p$ *or* $p^2 \nmid n$ *or* $p^3 \mid n$, *then* $\#D_n \geq \alpha_n(1 - 2q^{-1})$.

(v) If $p \nmid n$, *then* $|\#D_n - \alpha_n| \leq \alpha_n \cdot q^{-n/3\ell^2}$.

Open Question 27.

- *In the case where $p = \ell$ and p^2 divides n, can one tighten the gap between upper and lower bounds in Theorem 26(ii), maybe to within a factor $1 + O(q^{-1})$?*
- *Can one simplify the arguments and reduce the number of cases, yet obtain results of a quality as in Theorem 26? The bounds in Corollary 12 are based on "low level" coefficient comparisons. Can these results be proved (or improved) by "higher level" methods?*

7. ACKNOWLEDGMENTS

Many thanks go to Jaime Gutiérrez for alerting me to Umberto Zannier's paper, to Henning Stichtenoth for discussions and for pointing out Antonia Bluher's work, to Laila El Aimani for some computations, and to Konstantin Ziegler for drawing the tree and many more computations. I appreciate the discussions with Arnaud Bodin, Pierre Dèbes, and Salah Najib about the topic, and in particular the challenges that their work Bodin *et al.* (2009) posed.

This work was supported by the B-IT Foundation and the Land Nordrhein-Westfalen. A full version of this Extended Abstract is available as von zur Gathen (2008c).

References

ANTONIA W. BLUHER (2004). On $x^{q+1} + ax + b$. *Finite Fields and Their Applications* **10**(3), 285–305. URL http://dx.doi.org/10.1016/j.ffa.2003.08.004.

ARNAUD BODIN, PIERRE DÈBES & SALAH NAJIB (2009). Indecomposable polynomials and their spectrum. *Acta Arithmetica* (2009), to appear.

MARTIN FÜRER (2007). Fast Integer Multiplication. In *Proceedings of the Thirty-ninth Annual ACM Symposium on Theory of Computing, San Diego, California, USA*, 57–66. ACM. URL http://dx.doi.org/10.1145/1250790.1250800. Preprint available at: URL http://www.cse.psu.edu/~furer/Papers/mult.pdf.

JOACHIM VON ZUR GATHEN (1990a). Functional Decomposition of Polynomials: the Tame Case. *Journal of Symbolic Computation* **9**, 281–299.

JOACHIM VON ZUR GATHEN (1990b). Functional Decomposition of Polynomials: the Wild Case. *Journal of Symbolic Computation* **10**, 437–452.

JOACHIM VON ZUR GATHEN (2002). Factorization and Decomposition of Polynomials. In *The Concise Handbook of Algebra*, ALEXANDER V. MIKHALEV & GÜNTER F. PILZ, editors, 159–161. Kluwer Academic Publishers. ISBN 0-7923-7072-4.

JOACHIM VON ZUR GATHEN (2008a). Counting reducible and singular bivariate polynomials. *Finite Fields and Their Applications* **18**(4), 944–978. Extended abstract in *Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation ISSAC2007, Waterloo, Ontario, Canada* (2007), 369-376.

JOACHIM VON ZUR GATHEN (2008b). Counting decomposable multivariate polynomials. *Preprint,* 21 pages. URL http://arxiv.org/abs/0811.4726.

JOACHIM VON ZUR GATHEN (2008c). Counting decomposable univariate polynomials. *Preprint,* 84 pages. URL http://arxiv.org/abs/0901.0054.

JOACHIM VON ZUR GATHEN & JÜRGEN GERHARD (2003). *Modern Computer Algebra*. Cambridge University Press, Cambridge, UK, 2nd edition. ISBN 0-521-82646-2, 800 pages. URL http://cosec.bit.uni-bonn.de/science/mca.html. First edition 1999.

JOACHIM VON ZUR GATHEN, MARK GIESBRECHT & KONSTANTIN ZIEGLER (2009a). Collisions of polynomial compositions. *In preparation.*

JOACHIM VON ZUR GATHEN, DEXTER KOZEN & SUSAN LANDAU (1987). Functional Decomposition of Polynomials. In *Proceedings of the 28th Annual IEEE Symposium on Foundations of Computer Science, Los Angeles CA*, 127–131. IEEE Computer Society Press, Washington DC.

JOACHIM VON ZUR GATHEN, ALFREDO VIOLA & KONSTANTIN ZIEGLER (2009). Exact counting of reducible multivariate polynomials. *In preparation.*

MARK WILLIAM GIESBRECHT (1988). Complexity Results on the Functional Decomposition of Polynomials. Technical Report 209/88, University of Toronto, Department of Computer Science, Toronto, Ontario, Canada.

JOHANNES GRABMEIER, ERICH KALTOFEN & VOLKER WEISPFENNING (editors) (2003). *Computer Algebra Handbook*. Springer-Verlag, Berlin. ISBN 3-540-65466-6.

JAIME GUTIERREZ & DEXTER KOZEN (2003). *Polynomial Decomposition*, section 2.2.4 (pages 26–28) in Grabmeier *et al.* (2003). Springer.

JAIME GUTIERREZ & DAVID SEVILLA (2006). On Ritt's decomposition theorem in the case of finite fields. *Finite Fields and Their Applications* **12**(3), 403–412. URL http://dx.doi.org/10.1016/j.ffa.2005.08.004.

D. KOZEN & S. LANDAU (1986). Polynomial Decomposition Algorithms. Technical Report 86-773, Department of Computer Science, Cornell University, Ithaca NY.

DEXTER KOZEN & SUSAN LANDAU (1989). Polynomial Decomposition Algorithms. *Journal of Symbolic Computation* **7**, 445–456.

DEXTER KOZEN, SUSAN LANDAU & RICHARD ZIPPEL (1996). Decomposition of Algebraic Functions. *Journal of Symbolic Computation* **22**, 235–246.

BENIAMINO SEGRE (1964). Arithmetische Eigenschaften von Galois-Räumen, I. *Mathematische Annalen* **154**, 195–256. URL http://dx.doi.org/10.1007/BF01362097.

DAQING WAN (1990). Permutation Polynomials and Resolution of Singularities over Finite Fields. *Proceedings of the American Mathematical Society* **110**(2), 303–309. ISSN 0002-9939. URL http://www.jstor.org/journals/00029939.html.

U. ZANNIER (1993). Ritt's Second Theorem in arbitrary characteristic. *Journal für die reine und angewandte Mathematik* **445**, 175–203.