Joachim von zur Gathen (2013). Lower bounds for decomposable univariate wild polynomials. *Journal of Symbolic Computation* **50**, 409–430. URL http://dx.doi.org/10.1016/j.jsc.2011.01.008. Extended abstract in *Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation ISSAC '09, Seoul, Korea* (2009).

Lower bounds for decomposable univariate wild polynomials

Joachim von zur Gathen

B-IT, Universität Bonn
D-53113 Bonn, Germany

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. The tame case, where the field characteristic p does not divide the degree n of f, is reasonably well understood. The wild case, where p divides n, is more challenging. We present an efficient algorithm for this case that computes a decomposition, if one exists. It works for most but not all inputs, and provides a reasonable lower bound on the number of decomposable polynomials over a finite field. This is a central ingredient in finding a good approximation to this number.

Key words: computer algebra, wild 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 F). The present paper is part of a project that aims at a quantitative version of this intuition, namely an approximation to the number of decomposables over a finite field, together with a good relative error bound.

One readily obtains an upper bound. The challenge then is to find an essentially matching lower bound. The *tame case*, where the field characteristic p does not divide the degree of the left component, is well understood, both theoretically and algorithmically, since the breakthrough result of Kozen & Landau (1986); see also von zur Gathen, Kozen & Landau (1987); Kozen &

Email addresses: gathen@bit.uni-bonn.de (Joachim von zur Gathen)

Landau (1989); von zur Gathen (1990a); Kozen, Landau & Zippel (1996); Gutierrez & Sevilla (2006), and the survey articles of von zur Gathen (2002) and Gutierrez & Kozen (2003) with further references. The present paper deals with the complementary *wild case*, which is also addressed in Barton & Zippel (1985) and Zippel (1991).

Let $k, m \geq 2$ be integers, and S a set of pairs (g, h) of polynomials from $F[x]$ of degrees k, m, respectively, and h monic with $h(0) = 0$. Then we want to bound the number s of all $g \circ h$ with $(g, h) \in S$. Clearly $s \leq \#S$. It is well-known that in the tame case the composition map is injective, so that $s = \#S$. In the wild case, this is not true in general. The goal, then, in this paper is to prove a lower bound $\#S \cdot (1 - \varepsilon) \leq s$, with a small ε. This is achieved for a particular S described in Theorem 4.15(ii) by an algorithm that takes some $f \in F[x]$ and a factorization $n = \deg f = k \cdot m$ as input, and outputs all decompositions $(g, h) \in S$ with $f = g \circ h$. Using a result of Bluher (2004), one can show that "usually" there are only few decompositions. The desired lower bound then follows.

The algorithm presented here is similar in spirit to the one in von zur Gathen (1990b), and also works for most, but not all, inputs. It is somewhat simpler and faster, but its raison d'être is the lower bound just mentioned. The older method yields an estimate which is weaker by a factor of about $1/2n$ (see Fact 3.1(ii)) and insufficient for our goal. The new lower bound in Theorem 6.1 is of the form $\#S \cdot (1 - O(q^{-1}))$ over $\mathbb{F}_q$, where S is the set of all (g, h) of the degrees under consideration.

Throughout this paper, we provide explicit estimates without unspecified constants. In particular, the $O(q^{-1})$ above represents an explicit expression which depends on various parameters and divisibility conditions among them. It remains an open problem to replace q^{-1} by some smaller quantity, maybe q^{-p+1} (for $p \geq 3$).

In order to approximate the number of decomposable polynomials, one has to address the uniqueness (or lack thereof) of compositions

$$g \circ h = g^* \circ h^* \tag{1.1}$$

with $h \neq h^*$ and both monic with constant coefficient 0, in two situations. We have an *equal-degree collision* $\{(g, h), (g^*, h^*)\}$ 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 paper only deals with equal-degree collisions and we drop the qualifier "equal-degree" throughout. Concerning distinct-degree collisions, Ritt's Second Theorem is the central tool, describing all possibilities for such collisions. A normal form for the quantities in this Theorem and an estimate for the number of such collisions are in von zur Gathen (2010a), and von zur Gathen (2010b) describes the final approximation result. Some of these results are reported in von zur Gathen (2009). Certain wild cases, in particular decompositions at degree p^2, are studied in von zur Gathen, Giesbrecht & Ziegler (2010). Multivariate decomposable polynomials are counted in von zur Gathen (2010c).

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 2.1. *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.

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 $a \neq 0$. In other words, the set of decomposable polynomials is invariant under this action of $F^\times \times F$ on $F[x]$. In particular, if we have a set M of monic original decomposable polynomials and let M^* be the set of all their compositions with a linear polynomial on the left, then

$$\#M^* = q^2(1 - q^{-1}) \cdot \#M. \tag{2.2}$$

Furthermore, any decomposition (g, h) can be normalized by this action, by taking $a = \mathrm{lc}(h)^{-1} \in F^\times$, $b = -a \cdot h(0) \in F$, $g^* = g((x - b)a^{-1}) \in F[x]$, and $h^* = ah + b$. Then $g \circ h = g^* \circ h^*$ and h^* is monic original.

It is therefore sufficient to consider compositions $f = g \circ h$ where all three polynomials are monic and original. If D_n is the set of such f of degree n, then the number of all decomposable polynomials of degree n, not restricted to monic original, is

$$q^2(1 - q^{-1}) \cdot \#D_n. \tag{2.3}$$

We fix some notation for the remainder of this paper. For $n \geq 1$, we write

$$P_n = \{f \in F[x]\colon \deg f = n, f \text{ monic and original}\},$$

and use $n = \deg f \geq 1$ throughout. For any divisor e of n, we have the composition map

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

corresponding to Definition 2.1, and set

$$D_{n,e} = \operatorname{im} \gamma_{n,e}. \tag{2.4}$$

The set D_n of all decomposable polynomials in P_n satisfies

$$D_n = \bigcup_{\substack{e \mid n \\ 1<e<n}} D_{n,e}. \tag{2.5}$$

In particular, $D_n = \varnothing$ if n is prime. Over a finite field $\mathbb{F}_q$ with q elements, we have

$$\begin{aligned} \#P_n &= q^{n-1}, \\ \#D_{n,e} &\leq q^{e+n/e-2}. \end{aligned}$$

Example 2.6. We look at monic original decompositions (g, h) of univariate monic original quartic polynomials f, so that $n = 4$. The general case is

$$(x^2 + ax) \circ (x^2 + bx) = x^4 + ux^3 + vx^2 + wx \in F[x],$$

with $a, b, u, v, w \in F$. We find that with $a = 2w/u$ and $b = u/2$ (assuming $2u \neq 0$), the cubic and linear coefficients match, and the whole decomposition does if and only if

$$u^3 - 4uv + 8w = 0.$$

If F is infinite of characteristic $\neq 2$, then this is a defining equation for the hypersurface of decomposable polynomials in P_4. This example is also in Barton & Zippel (1976, 1985). In characteristic 2, we find the conditions $u = 0$, $a = b^2 + v$, and $b^3 + bv + w = 0$. The latter is related to the projective polynomials of Section 5. ◊

3. Equal-degree collisions

A decomposition (g, h) of $f = g \circ h$ over a field F of characteristic $p \geq 0$ is called *tame* if $p \nmid \deg g$, and *wild* otherwise, in analogy with ramification indices. The polynomial f itself is *tame* if $p \nmid \deg f = n$, and *wild* otherwise. The tame case is well understood, both theoretically and algorithmically. The wild case is more difficult and less well understood; there are polynomials with superpolynomially many "inequivalent" decompositions (Giesbrecht, 1988).

For $u, v \in F[x]$ and $j \in \mathbb{N}$, we write

$$u = v + O(x^j)$$

if $\deg(u - v) \leq j$. We start with two facts from the literature concerning the injectivity of the composition map. When $p \mid n$, a polynomial $f = x^n + f_i x^i + O(x^{i-1})$ with $i < n$ and $f_i \neq 0$ is called *simple* if $i \neq n - p$.

FACT 3.1. *Let F be a field of characteristic p, and e a divisor of $n \geq 2$.*

(i) *If p does not divide e, then $\gamma_{n,e}$ is injective, and for $F = \mathbb{F}_q$ we have*

$$\#D_{n,e} = q^{e+n/e-2}.$$

(ii) *If p divides n exactly d times and $f \in F[x]$ is simple, then f has at most $s < 2p^d \leq 2n$ monic normal decompositions, where $s = (p^{d+1} - 1)/(p - 1) = 1 + p + \cdots + p^d$.*

PROOF. The uniqueness in (i) is well-known, see e.g., von zur Gathen (1990a) and the references therein. (ii) follows from von zur Gathen (1990b), where the above notion of a simple polynomial is defined, and (the proof of) Corollary 3.6 of that paper shows that there are at most s such decompositions of f. □

Von zur Gathen (1990b) also gives an algorithm to decide decomposability and, in that case, to compute all such decompositions. This only applies to "simple" polynomials, and no nontrivial general upper bound on the number of decompositions seems to be known.

Algorithm 4.10 below uses a similar approach. On the one hand, it applies to more restricted inputs. On the other hand, it is faster (roughly, n^2 vs. n^4), more transparent and hence easier to analyze, and yields a lower bound on the number of decomposables at fixed component degrees.

Von zur Gathen (2009) provides an approximate upper bound α_n on $\#D_n$, with a small relative error. Furthermore, Fact 3.1 immediately yields a lower bound of $\alpha_n/2$ if p is not the smallest prime divisor ℓ of n, and of about $\alpha_n/4n$ in general, since "most" polynomials are simple. The task now is to improve these estimates.

By Fact 3.1(i), 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; Example 6.16 exhibits all four collisions over $\mathbb{F}_3$ at degree 9. Our goal, then, is to show that there are few of them, so that the decomposable polynomials are still numerous. Algorithm 4.10 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).

It is useful to single out a special case of wild compositions. If $f \in F[x^p] \cap P_n$, then $f = h \circ x^p$ for some $h \in P_{n/p}$, and f is decomposable if $n > p$.

DEFINITION 3.2. *An $f \in F[x^p]$ of degree larger than p is called a* Frobenius composition, *and any decomposition (g, h) of $f = g \circ h$ is a* Frobenius decomposition. *For a positive integer j, we denote by $\varphi_j \colon F \longrightarrow F$ the jth power of the Frobenius map over F, with $\varphi_j(a) = a^{p^j}$ for all $a \in F$, and extend it coefficientwise to an $\mathbb{F}_p$-linear map $\varphi_j \colon F[x] \longrightarrow F[x]$.*

For any monic original $h \in F[x]$ of degree at least 2 and distinct from x^{p^j}, we have the collision

$$x^{p^j} \circ h = \varphi_j(h) \circ x^{p^j}. \tag{3.3}$$

Over $F = \mathbb{F}_q$, there are $q^{p^j-1} - 1$ many $h \in P_{p^j}$ with $h \neq x^{p^j}$ and for $m \neq p^j$, this produces q^{m-1} collisions with $h \in P_m$. This example is noted in Schinzel (1982), Section I.5, page 39.

The Frobenius compositions from Definition 3.2 are easily described and counted. It is useful to separate them from the others. If $p \mid n$ and ℓ is a proper divisor of $n > p$, we set

$$\begin{aligned} D_n^{\varphi} &= D_n \cap F[x^p], \\ D_n^{+} &= D_n \smallsetminus D_n^{\varphi}, \\ D_{n,\ell}^{+} &= D_{n,\ell} \cap D_n^{+}, \end{aligned} \tag{3.4}$$

so that D_n^{φ} comprises exactly the Frobenius compositions of degree n.

4. A decomposition algorithm

We now describe an algorithm for certain "wild" decompositions $f = g \circ h$ with

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

and $p \mid k$. It first makes coefficient comparisons to compute h, and then a Taylor expansion to find g. It does not work for all inputs, but for sufficiently many for our counting purpose. In general, decomposing a polynomial can be attempted by solving the corresponding system of equations in the coefficients of the unknown components, say, using Gröbner bases. However, over sufficiently bizarre fields (certain infinite but "computable" fields of positive characteristic), decomposability is undecidable (von zur Gathen (1990b)).

To fix some notation, we have positive integers

$$d, \; r = p^d, \; a, k = ar, \; m \geq 2, \; n = km, \; \kappa < k \text{ with } p \nmid a\kappa, \tag{4.1}$$

and polynomials

$$\begin{aligned} g &= x^k + \sum_{1 \leq i \leq \kappa} g_i x^i, \\ h &= \sum_{1 \leq i \leq m} h_i x^i, \\ f &= \sum_{1 \leq i \leq n} f_i x^i = g \circ h = h^k + \sum_{1 \leq i \leq \kappa} g_i h^i, \end{aligned} \tag{4.2}$$

with $h_m = 1$, $h_{m-1} \neq 0$, and $g_\kappa \neq 0$. 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

$$h^{(i)} = \sum_{i<j<m} h_j x^j$$

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

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

Thus $c_{m-1,j}(x^k) = \operatorname{coeff}(h^k, j)$, 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} in (4.6) exhibits h_i in a simple fashion, meaning that we can compute it from the known data f_j and $h^{(i)}$.

Lastly we define the rational number

$$i_0 = m(\frac{\kappa - a}{r-1} - a + 1) = \frac{\kappa m - n}{r-1} + m. \tag{4.3}$$

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

$$r - 1 \mid (\kappa - a)m. \tag{4.4}$$

The following lemma describes, in the language introduced above, the coefficients that we will use.

LEMMA 4.5. *For $1 \le i \le m$ and $0 \le j \le n$, we have the following*

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

$$c_{i,(\kappa-1)m+i}(g_\kappa x^\kappa) = \kappa g_\kappa h_i, \tag{4.6}$$

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

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

$$c_{i,n-r(m-i)}(x^k) = a h_i^r. \tag{4.7}$$

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

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

$$c_{i_0,(\kappa-1)m+i_0}(x^k + g_\kappa x^\kappa) = a h_{i_0}^r + \kappa g_\kappa h_{i_0}. \tag{4.8}$$

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

$$\begin{aligned} c_{m-1,\kappa m}(x^k + g_\kappa x^\kappa) &= a h_{m-1}^r + g_\kappa, \\ c_{m-1,\kappa m-1}(x^k + g_\kappa x^\kappa) &= -g_\kappa h_{m-1}. \end{aligned} \tag{4.9}$$

PROOF. For E_1, we have to consider

$$g_\kappa(x^m + h_i x^i + O(x^{i-1}))^\kappa = g_\kappa x^{\kappa m} + g_\kappa \cdot \kappa h_i x^{(\kappa-1)m+i} + O(x^{(\kappa-1)m+i-1}).$$

We observe that

$$\begin{aligned} c_{i,(\kappa-1)m+i}(g_\kappa x^\kappa) &= g_\kappa \cdot \kappa h_i, \\ c_{m-1,\kappa m}(g_\kappa x^\kappa) &= \operatorname{coeff}(g_\kappa h^\kappa, \kappa m) = g_\kappa, \end{aligned}$$

and E_1 follows. For E_2, we start with

$$h^a = x^{am} + ah_{m-1}x^{am-1} + O(x^{am-2}).$$

When $i < m$, then in the coefficient of $x^{(a-1)m+i}$ in h^a, we have the contribution ah_i, which comes from taking in the expansion of h^a the factor x^m exactly $a-1$ times and the factor $h_i x^i$ exactly once; there are a ways to make these choices. The largest degree to which a summand $h_j x^j$ contributes in h^a is $(a-1)m + j$, so that those with $j < i$ do not appear in the coefficient under consideration, and $c_{i,(a-1)m+i}(x^a) = ah_i$. Raising h^a to the rth power yields

$$c_{i,((a-1)m+i)r}(x^k) = c_{i,((a-1)m+i)r}((x^a)^r) = a^r h_i^r = ah_i^r$$

and proves E_2, since $((a-1)m+i)r = n - r(m-i)$.

For E_3, we use E_2 and E_1 to find

$$\begin{aligned}(\kappa-1)m + i_0 &= n - r(m - i_0),\\ c_{i_0,(\kappa-1)m+i_0}(x^k + g_\kappa x^\kappa) &= c_{i_0,n-r(m-i_0)}(x^k) + c_{i_0,(\kappa-1)m+i_0}(g_\kappa x^\kappa)\\ &= ah_{i_0}^r + \kappa g_\kappa h_{i_0}.\end{aligned}$$

For E_4, we have $\kappa m = n - r$ and from E_2 and E_1

$$\begin{aligned}c_{m-1,\kappa m}(x^k + g_\kappa x^\kappa) &= c_{m-1,n-r}(x^k) + c_{m-1,\kappa m}(g_\kappa x^\kappa) = ah_{m-1}^r + g_\kappa,\\ c_{m-1,\kappa m-1}(x^k + g_\kappa x^\kappa) &= \mathrm{coeff}(h^k, \kappa m - 1) + c_{m-1,\kappa m-1}(g_\kappa x^\kappa)\\ &= 0 + \kappa g_\kappa h_{m-1} = -g_\kappa h_{m-1}.\end{aligned}$$ □

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). When we use E_2, we first compute $y = h_i^r$ and then h_i by extracting the rth root of y. Over a finite field, this always yields a unique answer, since r is a power of p. But in general, y might not have an rth root. We say "compute h_i^r by E_2, then h_i if possible" to mean that first y is determined, then h_i as its rth root; if y does not have an rth root, then the empty set is returned. In step 1, $f^{1/p}$ is to be interpreted in the same sense.

The main effort in the correctness proof is to show that all data required are available at any 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 $h^k - x^n$.

Algorithm 4.10. Wild decomposition.

Input: $f \in F[x]$ monic and original of degree $n = km$, where F is a field of characteristic $p \geq 2$, $d \geq 1$, $r = p^d$, $k = ar$ with $p \nmid a$, and $m \geq 2$.

Output: Either a set of at most $r+1$ pairs (g, h) with $g, h \in F[x]$ monic and original of degrees k and 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 $d \geq 2$ call Algorithm 4.10 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 $\kappa m \geq n - r + 2$ 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. [We have $i_0 = m - 1 \in \mathbb{N}$.] If (4.8) 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 A of all nonzero $s \in \mathbb{F}_q$ with
   $$as^{r+1} - f_{\kappa m} s - f_{\kappa m - 1} = 0. \tag{4.11}$$
   [We will see that the conditions in E_4 are satisfied.] If $A = \varnothing$ then return the empty set, else do steps 5.b and 5.c for all $s \in A$, setting $h_{m-1} = s$.
   b. Determine g_κ by E_4 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}^r by E_2, then h_{m-1} if possible.

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^r by E_2, then h_i if possible, for decreasing i with $m-2 \geq i > i_0$.

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 $i_0 > i \geq 1$ by E_1.

7. [We now know h.] 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 in step 7 method determines, for given f and h, the unique g (if one exists) so that $f = g \circ h = \sum_{1 \leq i \leq k} g_i h^i$. Such Taylor coefficients of f in base h always exist uniquely with $\deg g_i < \deg h$ for all i; see von zur Gathen & Gerhard (2003), Section 5.11. We have a decomposition of f if and only if all g_i are constant. This view was presented in von zur Gathen (1990a).

We first illustrate the algorithm in three examples.

EXAMPLE 4.12. 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

$$h^5 + g_4 h^4 = x^{50} + h_9^5 x^{45} + (h_8^5 + g_4)x^{40} + 4g_4 h_9 x^{39} + g_4(4h_8 + h_9^2)x^{38}$$

$$+x^{36} \cdot O(x) + (h_7^5 + g_4(4h_5 + h_9 h_6 + h_8 h_7 + h_9^2 h_7 + h_9 h_8^2 + h_9^3 h_8))x^{35} + O(x^{34}).$$

Step 1 determines $j = 39$, and step 2 finds $\kappa = (39 + 1)/10 = 4$ and $i_0 = 15/2 \notin \mathbb{N}$. Since $\kappa m = 40 < 45 = n - r$, we go to step 6. Step 6.a computes $h_9 = f_{45}^{1/5}$ at x^{45}, step 6.b yields $g_4 = f_{39}/4h_9$ at x^{39}, step 6.c determines $h_8 = (f_{40} - g_4)^{1/5}$ 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). $\diamondsuit$

Example 4.13. With the same values as above, except that $\kappa = 3$, we have

$$\begin{aligned} h^5 + g_3h^3 = x^{50} &+ h_9^5x^{45} + h_8^5x^{40} + h_7^5x^{35} \\ &+ (h_6^5 + g_3)x^{30} + 3g_3h_9x^{29} + g_3(3h_9^2 + 3h_8)x^{28} + x^{26} \cdot O(x) \\ &+ (h_5^5 + g_3(3h_5 + 3h_9h_6 + 3h_8h_7 + 3h_9^2h_7 + 3h_9h_8^2))x^{25} + O(x^{24}). \end{aligned}$$

Assuming that $f_{29} = 3g_3h_9 \neq 0$, 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 $h_5^5 + 3g_3h_5$ in step 6.d with E_3. Condition (4.16) 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 4.15 below. Finally $h_4, ..., h_1$ and g_1, g_2 are computed. $\diamondsuit$

Example 4.14. Finally, we take $p = 5$, $n = 25$, $k = r = m = 5$ and $\kappa = 4$, so that $a = 1$ and

$$h^5 + g_4h^4 = x^{25} + (h_4^5 + g_4)x^{20} + 4g_4h_4x^{19} + O(x^{18}).$$

Again we assume $f_{19} = 4g_4h_4 \neq 0$. 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 (4.11). The number of solutions is discussed starting with Fact 5.5 below. We consider two special cases, namely $q = 5$ and $q = 125$. For $q = 5$, we have 20 pairs $(v, w) = (f_{20}, f_{19}) \in \mathbb{F}_5^2$ to consider, with $w \neq 0$. When $v \neq 0$, then the number of solutions of (4.11) is

$$\begin{cases} 2 & \text{if } wv^{-2} \in \{2, 0\}, \\ 1 & \text{if } wv^{-2} = 1, \\ 0 & \text{otherwise,} \end{cases}$$

and when $v = 0$:

$$\begin{cases} 2 & \text{for the squares } w = 1, 4, \\ 0 & \text{otherwise.} \end{cases}$$

Over $\mathbb{F}_{125}$, we have the following numbers of nonzero solutions s when $v \neq 0$:

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

and when $v = 0$:

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

These numbers are explained below. We run the remaining steps in parallel for each value $h_4 = s$ with $s \in A$. 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. ♢

The algorithm works over any perfect field of characteristic p where each element has a pth root; in $\mathbb{F}_q$, this is just the (q/p)th power. It even works over an arbitrary field of characteristic p provided we have a subroutine that tests whether a field element is a pth power, and if so, returns a pth root. Then where a pth root is requested in the algorithm (steps 1, 3a, 6a, 6c, and 6d), we either return "no decomposition" or the root, depending on the outcome of the test.

The older algorithm from von zur Gathen (1990b) keeps track of a certain polynomial v, factors it, and works with the roots of its irreducible factors. Here, this is replaced by the conceptually simpler case distinctions of the mutually exclusive steps 3, 4, 5, and 6. More importantly, the present approach leads to lower bounds of the form $q^{k+m-2}(1 + O(q^{-1}))$ in Theorem 6.1, while the older approach only yields something like $q^{k+m-2}/2n$, as in Fact 3.1(ii).

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 F. 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 $\sigma(f) = \#A$ if the precondition of step 5 is satisfied and A computed there, and otherwise $\sigma(f) = 1$.

THEOREM 4.15. *Let f be an input polynomial with parameters n, p, $q = p^e$, d, r, a, k, m as specified by the input conditions, and assume F to be perfect.*

(i) *Algorithm 4.10 returns either "failure" or a set of monic original decompositions (g^*, h^*) of f. Except if returned in step 1, none of them is a Frobenius decomposition. If $F = \mathbb{F}_q$ is finite, then the algorithm uses*

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

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

(ii) *Suppose furthermore that* g, h, κ, i_0 *are as in (4.2) and (4.3), so that* $f = g \circ h$, $F = \mathbb{F}_q = \mathbb{F}_{p^e}$, *set* $c = \gcd(d, e)$ *and assume that*

$$\text{if } i_0 \in \mathbb{N} \text{ and } 1 \leq i_0 < m, \text{ then } (-\kappa g_\kappa / a)^{(q-1)/(p^c-1)} \neq 1. \tag{4.16}$$

Then "failure" does not happen, at most $\sigma(f)$ *decompositions are returned, and* (g, h) *is one of them.*

PROOF. Since $r = p^d \mid k$, we have $\mathrm{coeff}(h^k, j) = 0$ 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.

For the cost of the algorithm over $F = \mathbb{F}_q$, 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

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

This proves (i). For (ii), we claim that the equations used in the algorithm involve only coefficients of f and previously computed values. If we denote by G the set of (g, h) allowed in Theorem 4.15(ii), then for $f \in \gamma_{n,k}(G)$, these equations usually have a unique solution. It follows that most such f are correctly and uniquely decomposed by the algorithm. The only exception to the uniqueness occurs in (4.11).

In steps 3 through 6, 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

$$n - r(m - i) \geq (\kappa - 1)m + i \text{ if and only if } i \geq i_0, \tag{4.17}$$

since the first linear function of 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 as above. 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

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

for all j in the algorithm. Thus the coefficients of g, except g_κ, are not needed up to step 6.

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 (4.8), 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

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

violating the condition (4.16).

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

$$\deg(h^k - x^n) = \deg((h^a - x^{am})^r) \leq (am-1)r = n - r, \tag{4.18}$$

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

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

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

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 $\kappa g_\kappa \neq 0$, 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 $f_{\kappa m - 1} = c_{m-1,\kappa m-1}(x^k + g_\kappa x^\kappa) = ah_{m-1}^r + \kappa g_\kappa h_{m-1}$. 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. Step 4.c works correctly, by an argument as for step 3.b.

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

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

Thus $h_{m-1} \in A$ 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 $\operatorname{coeff}(h^k, \kappa m) = 0$ by E_2, and otherwise $\operatorname{coeff}(h^k, \kappa m - 1) = 0$. Thus g_κ is correctly computed in step 6.b. Correctness of the remaining steps follows as above. $\square$

A more direct way to compute h (say, in step 3) is to consider its reversal as the κth root of the reversal of $(f - h^k)/g_\kappa$, feeding the contribution of h^k into the Newton iteration as in von zur Gathen (1990a). This procedure has not been analyzed.

5. Bluher's count

Our next task is to determine the number N of decomposable f obtained as $g \circ h$ in Theorem 4.15. Since (4.11) 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 4.15(ii), divided by $r+1$. The following considerations lead to a much better lower bound on N.

In the following we write, as usually, $p = \operatorname{char} \mathbb{F}_q$, and also

$$q = p^e, r = p^d, c = \gcd(d, e), z = p^c, \tag{5.1}$$

so that $\mathbb{F}_q \cap \mathbb{F}_r = \mathbb{F}_z$ (assuming an embedding of $\mathbb{F}_q$ and $\mathbb{F}_r$ in a common superfield) and $\gcd(q-1, r-1) = z - 1$ (see Lemma 5.9). We have to understand the number of solutions s of (4.11), in other words, the size of

$$S(v, w) = \{s \in \mathbb{F}_q^\times : s^{r+1} - vs - w = 0\}$$

for $v = f_{\kappa m}/a$, $w = f_{\kappa m-1}/a \in \mathbb{F}_q$. Equation (4.11) is only used in step 5, where $m = r$, as noted above. We have $\kappa = (j+1)/m$ in step 2 and hence $f_{\kappa m-1} \neq 0$ and $w \neq 0$. Furthermore, we define for $u \in \mathbb{F}_q$

$$T(u) = \{t \in \mathbb{F}_q^\times : t^{r+1} - ut + u = 0\}. \tag{5.2}$$

In (4.11), we have $w \neq 0$, but v might be zero. In order to apply a result from the literature, we first assume that also v is nonzero, make the invertible substitution $s = -v^{-1}wt$, and set $u = v^{r+1}(-w)^{-r} = -v^{r+1}w^{-r} \in \mathbb{F}_q$. Then $u \neq 0$ and

$$\begin{aligned} s^{r+1} - vs - w &= (-v^{-1}w)^{r+1}(t^{r+1} - ut + u), \\ \#S(v,w) &= \#T(u). \end{aligned} \tag{5.3}$$

This reduces the study of $S(v,w)$, with two parameters, to the one-parameter problem $T(u)$. The polynomial $t^{r+1} - ut + u$ is a special type of the *projective polynomials* introduced by Abhyankar (1997) and has appeared in other contexts such as the inverse Galois problem, difference sets, and Müller-Cohen-Matthews polynomials. Bluher (2004) has determined the combinatorial properties that we need here; see her paper also for further references. Bluher allows an infinite ground field F, but we only use her results for $F = \mathbb{F}_q$. A simplified proof is presented in von zur Gathen *et al.* (2010).

For $i \geq 0$, let

$$\begin{aligned} C_i &= \{u \in \mathbb{F}_q^\times : \#T(u) = i\}, \\ c_i &= \#C_i. \end{aligned} \tag{5.4}$$

Then $C_i = \varnothing$ for $i > r+1$. Bluher (2004) completely determines these c_i, as follows.

FACT 5.5. *With the notations (5.1) and (5.4), let $I = \{0, 1, 2, z+1\}$. Then*

$$\begin{aligned} c_1 &= \frac{q}{z} - \gamma, \\ c_i &= 0 \textit{ unless } i \in I, \\ c_{z+1} &= \left\lfloor \frac{q}{z^3 - z} \right\rfloor, \end{aligned} \tag{5.6}$$

where

$$\gamma = \begin{cases} 1 & \textit{if } q \textit{ is even and } e/c \textit{ is odd}, \\ 0 & \textit{otherwise}, \end{cases} \tag{5.7}$$

and furthermore

$$q = 1 + \sum_{i \in I} c_i = 2 + \sum_{i \in I} i c_i. \tag{5.8}$$

PROOF. The claims are shown in Bluher (2004), Theorem 5.6. Her statement assumes $tu \neq 0$, which is equivalent to our assumption $t \neq 0$. For c_{z+1}, she finds $(qz^{-1} - z)/(z^2 - 1)$ if e/z is even, and otherwise $(qz^{-1} - 1)(z^2 - 1)$. The rounding in (5.6) avoids this case distinction. Equation (5.8) corresponds to the fact that the numbers c_i form the preimage statistics of the map from $\mathbb{F}_q \setminus \{0, 1\}$ to $\mathbb{F}_q \setminus \{0\}$ given by the rational function $x^{r+1}/(x - 1)$. □

Equations (5.6) and (5.8) also determine the remaining two values c_0 and c_2, namely $c_2 = \frac{1}{2}(q - 2 - c_1 - (z + 1)c_{z+1})$ and $c_0 = 1 + c_2 + zc_{z+1}$. For large z, we have

$$c_2 \approx \frac{q}{2}(1 - \frac{1}{z} - \frac{z+1}{z^3 - z}) = \frac{q}{2}(1 - \frac{1}{z-1}) \approx \frac{q}{2}.$$

Thus $x^{r+1}/(x - 1)$ behaves for odd q a bit like squaring: about half the elements have two preimages, and about half have none.

For the case $v = 0$, we have the following facts, which are presumably well-known. For an integer m, we let the integer $\nu(m)$ be the multiplicity of 2 in m, so that $m = 2^{\nu(m)} m^*$ with an odd integer m^*.

LEMMA 5.9. *Let $\mathbb{F}_q$ have characteristic p with $q = p^e$, $r = p^d$ with $d \geq 1$, $b = \gcd(q - 1, r + 1)$ and $w \in \mathbb{F}_q^\times$. Then the following hold.*

(i)
$$\#S(0, w) = \begin{cases} b & \text{if } w^{(q-1)/b} = 1, \\ 0 & \text{otherwise.} \end{cases}$$

(ii) *We let $c = \gcd(d, e)$, $z = p^c$, $\delta = \nu(d)$, $\varepsilon = \nu(e)$, $\alpha = \nu(r^2 - 1)$, $\beta = \nu(q - 1)$,*

$$\lambda = \begin{cases} 2 & \text{if } \delta < \varepsilon, \\ 1 & \text{if } \delta \geq \varepsilon, \end{cases}$$

$$\mu = \begin{cases} 1 & \text{if } \alpha > \beta, \\ 0 & \text{if } \alpha \leq \beta. \end{cases}$$

Then $\gcd(r-1, q-1) = z-1$ *and*

$$b = \frac{(z^\lambda - 1)\cdot 2^\mu}{z-1} = \begin{cases} 2(z+1) & \text{if } \delta < \varepsilon \text{ and } \alpha > \beta, \\ z+1 & \text{if } \delta < \varepsilon \text{ and } \alpha \le \beta, \\ 2 & \text{if } \delta \ge \varepsilon \text{ and } \alpha > \beta, \\ 1 & \text{if } \delta \ge \varepsilon \text{ and } \alpha \le \beta. \end{cases}$$

(iii) *If p is odd, then $\alpha > \beta$ if and only if e/c is odd.*

PROOF. (i) The power function $y \mapsto y^{r+1}$ from $\mathbb{F}_q^\times$ to $\mathbb{F}_q^\times$ maps b elements to one, and its image consists of the $w \in \mathbb{F}_q$ with $w^{(q-1)/b} = 1$.

(ii) For the first claim that

$$\gcd(q-1, r-1) = z-1, \tag{5.10}$$

we may assume, by symmetry, that $d > e$ and let $d = ie + j$ be the division with remainder of d by e, with $0 \le j < e$. Then for

$$a = \frac{x^j(x^{d-j}-1)}{x^e - 1} = x^j \cdot \frac{x^{ie}-1}{x^e-1} \in \mathbb{Z}[x],$$

we have

$$x^d - 1 = a\cdot(x^e - 1) + (x^j - 1).$$

By induction along the Extended Euclidean Algorithm for (d, e) it follows that all quotients in the Euclidean Algorithm for $(x^d - 1, x^e - 1)$ in $\mathbb{Q}[x]$ are, in fact, in $\mathbb{Z}[x]$, hence also the Bézout coefficients, and that all remainders are of the form $x^y - 1$, where y is some remainder for d and e. For $c = \gcd(d, e)$, there exist u, v, s, $t \in \mathbb{Z}[x]$ so that

$$\begin{aligned} u\cdot(x^c - 1) &= x^d - 1, \\ v\cdot(x^c-1) &= x^e - 1, \\ s\cdot(x^d - 1) + t\cdot(x^e - 1) &= x^c - 1. \end{aligned}$$

Substituting any integer q for x into these equations shows the claim (5.10).

We note that $\gcd(2d, e) = \lambda c$ and

$$\gcd(p^d - 1, p^d + 1) = \begin{cases} 2 & \text{if } p \text{ is odd}, \\ 1 & \text{if } p \text{ is even}. \end{cases}$$

When p is even, then $\alpha = \beta = 0$. Applying (5.10) to $q = p^e$ and $r^2 = p^{2d}$, we find

$$\begin{aligned}
p^{\lambda c} - 1 &= \gcd((p^d - 1)(p^d + 1), p^e - 1) \\
&= \gcd(p^d - 1, p^e - 1) \cdot \gcd(p^d + 1, p^e - 1) \\
&= (p^c - 1) \cdot b, \\
b = \frac{p^{\lambda c} - 1}{p^c - 1} &= \begin{cases} z + 1 & \text{if } \delta < \varepsilon, \\ 1 & \text{if } \delta \geq \varepsilon. \end{cases}
\end{aligned}$$

For odd p, the second equation above is still almost correct, except possibly for factors which are powers of 2. We note that exactly one of $\nu(p^d - 1)$ and $\nu(p^d + 1)$ equals 1, and

$$\begin{aligned}
p^{\lambda c} - 1 &= \gcd((p^d - 1)(p^d + 1), p^e - 1) \\
&= \gcd(p^d - 1, p^e - 1) \cdot \gcd(p^d + 1, p^e - 1) \cdot 2^{-\mu} \\
&= (p^c - 1) \cdot b \cdot 2^{-\mu}, \\
b &= \frac{(p^{\lambda c} - 1) \cdot 2^{\mu}}{p^c - 1}.
\end{aligned}$$

(iii) We define the integers k_q and k_r by

$$\begin{aligned}
\frac{q - 1}{z - 1} &= \frac{z^{e/c} - 1}{z - 1} = z^{e/c - 1} + \cdots + 1 = k_q, \\
\frac{r^2 - 1}{z - 1} &= \frac{(r + 1)(z^{d/c} - 1)}{z - 1} = (r + 1)(z^{d/c - 1} + \cdots + 1) = (r + 1)k_r.
\end{aligned}$$

Now $r+1$ is even and z is odd. If e/c is odd, then k_q is odd and hence $\alpha > \beta$. Now assume that e/c is even. Then d/c is odd, and so is k_r, and k_q is even. Hence $\nu(r - 1) = \nu(z - 1) \geq 1$, and we denote this integer by γ. If $\gamma \geq 2$, then $\nu(r + 1) = 1 \leq \nu(k_q)$ and $\alpha = \nu(r + 1) + \gamma \leq \nu(k_q) + \gamma = \beta$.

Now suppose that $\gamma = 1$, and let $\tau = \nu(z + 1)$ and $m = (z + 1) \cdot 2^{-\tau}$. Then $\tau \geq 2$, m is an odd integer, and

$$\begin{aligned}
z^2 &= (m2^{\tau} - 1)^2 \equiv -2 \cdot 2^{\tau} + 1 \equiv 2^{\tau+1} + 1 \bmod 2^{\tau+2}, \\
r^2 &= (z^2)^{d/c} = (2^{\tau+1} + 1)^{d/c} \equiv 2^{\tau+1} + 1 \bmod 2^{\tau+2}, \\
q &= (z^2)^{e/2c} \equiv (2^{\tau+1} + 1)^{e/2c} \bmod 2^{\tau+2}.
\end{aligned}$$

The last value equals $2^{\tau+1} + 1$ or 1 modulo $2^{\tau+2}$ if $e/2c$ is odd or even, respectively. In either case, it follows that $\alpha = \nu(r^2 - 1) = \tau + 1 \leq \nu(q - 1) = \beta$. $\square$

6. The number of decomposable polynomials

We now bound from below the number $\#D^+_{n,k}$ of non-Frobenius compositions in the wild case, where $p \mid k$. The number of all monic original g and h of degrees k and m, respectively, is q^{k+m-2}, and the lower bound is $q^{k+m-2}(1 - O(q^{-1}))$, with explicit (but somewhat complicated) expressions for the $O(q^{-1})$.

THEOREM 6.1. *Let $\mathbb{F}_q$ have characteristic p with $q = p^e$, and take integers $d \geq 1$, $r = p^d$, $k = ar$ with $p \nmid a$, $m \geq 2$, $n = km$, $c = \gcd(d, e)$, $z = p^c$, $\mu = \gcd(r - 1, m)$, $r^* = (r - 1)/\mu$, and let G consist of the (g, h) as in Theorem 4.15(ii). Then we have the following lower bounds on the cardinality of $\gamma_{n,k}(G)$.*

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

$$q^{k+m-2}(1 - q^{-1}(1 + q^{-p+2}\frac{(1 - q^{-1})^2}{1 - q^{-p}}))(1 - q^{-k}),$$

(ii) *If $r \neq m$:*

$$\begin{aligned}
&q^{k+m-2}\big((1 - q^{-1}(1 + q^{-p+2}\frac{(1 - q^{-1})^2}{1 - q^{-p}}))(1 - q^{-k})\\
&\qquad - q^{-r^*-c/e+1}\frac{(1 - q^{-1})^2(1 - q^{-r^*(\mu-1)})}{(1 - q^{-c/e})(1 - q^{-r^*})}\\
&\qquad \cdot (1 - q^{-r^*(p-1)}\frac{(1 - q^{-r^*})(1 - q^{-pr^*\mu^*})}{(1 - q^{-r^*(\mu-1)})(1 - q^{-pr^*})})\big)\\
&\geq q^{k+m-2}\big((1 - q^{-1}(1 + q^{-p+2}\frac{(1 - q^{-1})^2}{1 - q^{-p}}))(1 - q^{-k})\\
&\qquad - q^{-r^*+1}\frac{(1 - q^{-1})^2(1 - q^{-r^*(\mu-1)})}{1 - q^{-r^*}})\big)\\
&\geq q^{k+m-2}\big((1 - q^{-1}(1 + q^{-p+2}\frac{(1 - q^{-1})^2}{1 - q^{-p}}))(1 - q^{-k})\\
&\qquad - 2q^{-r^*+1}(1 - q^{-1})^2\big).
\end{aligned}$$

(iii) *If $r = m$:*

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

PROOF. We have seen at the beginning of the proof of Theorem 4.15 that steps 1 and 2 determine j and κ. We also know that, given g_κ and h_{m-1}, the remaining coefficients of g and h are uniquely determined by those of f.

We count the number of compositions $g \circ h$ according to the four mutually exclusive conditions in steps 3 through 6, for a fixed κ. The admissible κ are those with $1 \leq \kappa < k$ and $p \nmid \kappa$. The expressions E_3 or E_4 are used if and only if either $i_0 \in \mathbb{N}$ or $\kappa m = n - r$, respectively. If neither happens, then the number of (g, h) is

$$q^\kappa(1 - q^{-1}) \cdot q^{m-1}(1 - q^{-1}) = q^{\kappa+m-1}(1 - q^{-1})^2. \tag{6.2}$$

The expression E_3 is used if and only if $\kappa \in K$, where

$$K = \{\kappa \in \mathbb{N} \colon 1 \leq \kappa < k, p \nmid \kappa, i_0 \in \mathbb{N}, 1 \leq i_0 < m\},$$

which corresponds to steps 4.b (where $i_0 = m - 1$) and 6.d (where $i_0 \in \mathbb{N}$ and $1 \leq i_0 \leq m - 2$). For $\kappa \in K$, we have the condition (4.16) that $(-\kappa g_\kappa/a)^{(q-1)/(z-1)} \neq 1$. The exponent is a divisor of $q - 1$, and there are exactly $(q - 1)/(z - 1)$ values of g_κ that violate (4.16). Thus for $\kappa \in K$ the number of (g, h) equals

$$(q - 1 - \frac{q-1}{z-1})q^{\kappa-1} \cdot q^{m-1}(1 - q^{-1}) = q^{\kappa+m-1}(1 - q^{-1})^2(1 - \frac{1}{z-1}). \tag{6.3}$$

The only usage of E_4 occurs in step 5.a, where $\kappa = (n-r)/m = k-r/m$. We have seen in the proof of Theorem 4.15 that this implies $r = m$ and $\kappa = k - 1$. We split G according to whether $\kappa = k - 1$ or $\kappa < k - 1$, setting

$$G^* = \{(g, h) \in G \colon \kappa = k - 1 \text{ in } (4.2)\}.$$

We define three summands N_{12}, N_3, and N_4 according to whether only E_1 and E_2, or also E_3, or E_4 are used, respectively:

$$\begin{aligned}
N_{12} &= \sum_{\substack{1 \leq \kappa < k \\ p \nmid \kappa}} q^{\kappa+m-1}(1 - q^{-1})^2, \\
N_3 &= \sum_{\kappa \in K} \left(q^{\kappa+m-1}(1 - q^{-1})^2 - q^{\kappa+m-1}(1 - q^{-1})^2(1 - \frac{1}{z-1}) \right), \\
N_4 &= q^{k+m-2}(1 - q^{-1})^2 - \#\gamma_{n,k}(G^*).
\end{aligned}$$

We will see below that $K = \varnothing$ if $r = m$. If $r \neq m$ and $K = \varnothing$, then we have for each $\kappa < k$ a number of polynomials as in (6.2) in $\gamma_{n,k}(G)$, and in total N_{12} many. If we only assume $r \neq m$, we have to replace (6.2) by (6.3) for each $\kappa \in K$. This corresponds to subtracting N_3 from N_{12} in the total. Finally, if $r = m$, then $K = \varnothing$ and for $\kappa = k - 1$ we have to replace (6.2) by $\#\gamma_{n,k}(G^*)$. This means deducting N_4 from N_{12} in the total. Together, we have

$$\#\gamma_{n,k}(G) \geq \begin{cases} N_{12} & \text{if } r \neq m \text{ and } K = \varnothing, \\ N_{12} - N_3 & \text{if } r \neq m, \\ N_{12} - N_4 & \text{if } r = m. \end{cases}$$

Since $p \mid k$, the first sum equals

$$\begin{aligned} N_{12} &= q^{m-1}(1-q^{-1})^2 \Big(\sum_{1 \leq \kappa < k} q^\kappa - \sum_{\substack{1 \leq \kappa < k \\ p \mid \kappa}} q^\kappa \Big) \\ &= q^{m-1}(1-q^{-1})^2 \Big(\frac{q^k - 1}{q-1} - 1 - \frac{(q^p)^{k/p} - 1}{q^p - 1} + 1 \Big) \\ &= q^{k+m-2}(1-q^{-1})(1-q^{-k}) \frac{1 - q^{-p+1}}{1 - q^{-p}} \\ &= q^{k+m-2}\Big(1 - q^{-1}\Big(1 + q^{-p+2}\frac{(1-q^{-1})^2}{1-q^{-p}}\Big)\Big)(1-q^{-k}). \end{aligned}$$

For N_3, we describe K more transparently. First we note that

$$\begin{aligned} & 1 \leq i_0 = \frac{\kappa m - n}{r-1} + m \leq m - 1 \\ \Longleftrightarrow\ & k - (r-1) + \frac{r-1}{m} \leq \kappa \leq k - \frac{r-1}{m}. \end{aligned} \tag{6.4}$$

We recall $\mu = \gcd(r-1, m)$ and $r^* = (r-1)/\mu$, and set $m^* = m/\mu$, so that $\gcd(r^*, m^*) = 1$ and

$$(6.4) \Longleftrightarrow k - (r-1) + \frac{r^*}{m^*} \leq \kappa \leq k - \frac{r^*}{m^*}.$$

From (4.3) we find

$$i_0 \in \mathbb{Z} \Longleftrightarrow (r-1) \mid (\kappa - a)m \Longleftrightarrow r^* \mid (\kappa - a)m^* \Longleftrightarrow r^* \mid \kappa - a. \tag{6.5}$$

Since $r^* \mid k - a = a(r-1)$, we have

$$(6.5) \Longleftrightarrow \exists j \in \mathbb{Z} \quad \kappa = k - (r-1) + jr^*. \tag{6.6}$$

If $i_0 \in \mathbb{Z}$, we fix this uniquely determined j. Then

$$(6.4) \Longleftrightarrow \frac{1}{m^*} \leq j \leq \frac{r-1}{r^*} - \frac{1}{m^*} \Longleftrightarrow 1 \leq j \leq \mu - 1. \tag{6.7}$$

Since $\mu \mid (r-1)$ and $r = p^d$, we have $p \nmid \mu$. Thus

$$\begin{aligned} p \mid \kappa &\Longleftrightarrow 1 - \frac{j}{\mu} \equiv 1 + \frac{j(r-1)}{\mu} \equiv k - (r-1) + jr^* = \kappa \equiv 0 \bmod p \qquad (6.8)\\ &\Longleftrightarrow j \equiv \mu \bmod p \Longleftrightarrow \exists i \in \mathbb{Z} \quad j = \mu - ip, \\ (6.4) &\Longleftrightarrow 1 \leq j = \mu - ip \leq \mu - 1 \Longleftrightarrow 1 \leq i \leq \lfloor \frac{\mu - 1}{p} \rfloor. \end{aligned}$$

Abbreviating $\mu^* = \lfloor (\mu - 1)/p \rfloor$, it follows that

$$K = \{k - (r-1) + jr^* \colon 1 \leq j < \mu\} \smallsetminus \{k - ipr^* \colon 1 \leq i \leq \mu^*\}.$$

In particular, we have $K = \varnothing$ if $\mu = 1$. Assuming $\mu \geq 2$ and using $z = p^c = q^{c/e}$, we can evaluate N_3 as follows.

$$\begin{aligned} N_3 &= \sum_{\kappa \in K} \frac{q^{\kappa + m - 1}}{z - 1} (1 - q^{-1})^2 \\ &= \frac{q^{m-1}(1 - q^{-1})^2}{z - 1} \sum_{\kappa \in K} q^\kappa \\ &= \frac{q^{m-1}(1 - q^{-1})^2}{z - 1} \Big(q^{k-(r-1)+r^*} \frac{(q^{r^*})^{\mu - 1} - 1}{q^{r^*} - 1} - q^{k - pr^*} \frac{1 - (q^{-pr^*})^{\mu^*}}{1 - q^{-pr^*}} \Big) \\ &= q^{k+m-1-r^*-c/e} \frac{(1 - q^{-1})^2 (1 - q^{-r^*(\mu - 1)})}{(1 - q^{-c/e})(1 - q^{-r^*})} \\ &\quad \cdot \Big(1 - q^{-r^*(p-1)} \frac{(1 - q^{-r^*})(1 - q^{-pr^* \mu^*})}{(1 - q^{-r^*(\mu-1)})(1 - q^{-pr^*})} \Big). \end{aligned}$$

In order to evaluate N_4, we first recall from the above that we have $\kappa m = n - r$, $\kappa = k - 1$, $m = r$, and any $(g, h) \in G^*$ is uniquely determined by $f = g \circ h$, g_{k-1}, and h_{m-1}. To any $(g,h) \in G^*$, we associate the field elements

$$\begin{aligned} V(g,h) &= h_{m-1}^r + g_{k-1}/a, \\ W(g,h) &= -g_{k-1}h_{m-1}/a, \\ U(g,h) &= -V(g,h)^{r+1}W(g,h)^{-r}. \end{aligned} \tag{6.9}$$

Then if $f = g \circ h$, we have $aV(g,h) = f_{n-r}$ and $aW(g,h) = f_{n-r-1} \neq 0$ by (4.9). If $V(g,h) \neq 0$, then for nonzero $s \in \mathbb{F}_q$ and $t = -V(g,h) \cdot W(g,h)^{-1}s$, (5.3) says that

$$\text{(4.11) holds} \iff s \in S(V(g,h), W(g,h)) \iff t \in T(U(g,h)).$$

We recall the sets C_i from (5.4) and for $i \in \{1, 2, z+1\}$, we set

$$\begin{aligned} G_i &= \{(g,h) \in G^* \colon V(g,h) \neq 0, U(g,h) \in C_i\}, \\ G_0 &= \{(g,h) \in G^* \colon V(g,h) = 0\}. \end{aligned} \tag{6.10}$$

These four sets form a partition of G^*. Now let $v \in \mathbb{F}_q^\times$, $i \in \{1, 2, z+1\}$, $u \in C_i$, and $g_{k-2}, \ldots, g_1, h_{m-2}, \ldots, h_1 \in \mathbb{F}_q$. From these data, we construct $(g,h) \in G_i$ with $g = \sum_{1 \leq i \leq k} g_i x^i$ and $h = \sum_{1 \leq i \leq m} h_i x^i$ and $g_k = h_m = 1$, so that only g_{k-1} and h_{m-1} still need to be determined. Furthermore, if $f = g \circ h$, we claim that different data lead to different f. This will imply that

$$\gamma_{n,k}(G_i) \geq (q-1)c_i \cdot q^{k+m-4}. \tag{6.11}$$

By assumption, we have $\#T(u) = i \geq 1$ and hence $u \neq 0$. We choose some $t \in T(u)$ and define $w, s \in \mathbb{F}_q^\times$ by

$$\begin{aligned} w^r &= -v^{r+1}u^{-1}, \\ s &= -v^{-1}wt. \end{aligned}$$

Then $s \in S(v,w)$ by (5.3). We set $h_{m-1} = s$ and $g_{k-1} = av - as^r$. Now g and h are determined, and (4.9) implies that

$$\begin{aligned} f_{n-r} &= ah_{m-1}^r + g_\kappa = aV(g,h) = av, \\ f_{n-r-1} &= -g_\kappa h_{m-1} = aW(g,h) = -a(v - s^r)s = a(s^{r+1} - vs) = aw, \\ U(g,h) &= -v^{r+1}w^{-r} = -v^{r+1}(-v^{r+1}u^{-1})^{-1} = u. \end{aligned}$$

Suppose that (u,v) and $(\tilde{u}, \tilde{v})$ lead to $(f_{n-r}, f_{n-r-1}) = (av, aw)$ and $(\widetilde{f_{n-r}}, \widetilde{f_{n-r-1}}) = (a\tilde{v}, a\tilde{w})$, and that the latter pairs are equal. Then $v = \tilde{v}$ and $u = -v^{r+1}w^{-r} = -\tilde{v}^{r+1}\tilde{w}^{-r} = \tilde{u}$. This concludes the proof of (6.11).

A similar argument works for G_0. We let $b = \gcd(q-1, r+1)$, take $w \in \mathbb{F}_q$ with $w^{(q-1)/b} = 1$, and some $s \in \mathbb{F}_q$ with $s^{r+1} = w$. There are $(q-1)/b$ such w, and according to Lemma 5.9(i), b such values s for each w. We set $h_{m-1} = s$ and $g_{k-1} = -ah_{m-1}^r$ and, as above, complete them with arbitrary coefficients to $(g, h) \in G_0$. When $f = g \circ h$, then $f_{n-r} = 0$ and $f_{n-r-1} = -g_{k-1}h_{m-1} = ah_{m-1}^{r+1} = aw = aW(g, h)$, and different w lead to different f. It follows that

$$\gamma_{n,k}(G_0) \geq \frac{q-1}{b} \cdot q^{k+m-4}. \tag{6.12}$$

We claim that the images of G_1, G_2, G_{z+1}, and G_0 under $\gamma_{n,k}$ are pairwise disjoint. The map $V : G^* \longrightarrow \mathbb{F}_q$ distinguishes between G_0 and G_i with $i \in \{1, 2, z+1\}$. For the latter three values, U determines i by (6.10). Furthermore, the values of V and W, and hence of U, are determined by the coefficients of $f = g \circ h = \gamma_{n,k}((g, h))$. This proves the claim. It follows that

$$\begin{aligned} \sum_{i=0,1,2,z+1} \#\gamma_{n,k}(G_i) &\geq \sum_{i=1,2,z+1} (q-1)c_i \cdot q^{k+m-4} + \frac{q-1}{b} \cdot q^{k+m-4} \qquad (6.13) \\ &= (q-1)q^{k+m-4}\Big(\sum_{i=1,2,z+1} c_i + \frac{1}{b}\Big). \end{aligned}$$

We write $q = p^e$ and set

$$z^* = \begin{cases} z & \text{if } e/c \text{ is odd,} \\ z^2 & \text{if } e/c \text{ is even.} \end{cases}$$

Fact 5.5 yields

$$c_{z+1} = \left\lfloor \frac{q}{z^3 - z} \right\rfloor = \frac{q - z^*}{z^3 - z},$$

$$\begin{aligned} 2 \sum_{i=1,2,z+1} c_i &= 2c_1 + (q - 2 - c_1 - (z+1)c_{z+1}) + 2c_{z+1} \\ &= q - 2 + \frac{q}{z} - \gamma - (z-1)\frac{q - z^*}{z^3 - z} \\ &= q - 2 + \frac{q}{z} - \gamma - \frac{q - z^*}{z^2 + z}, \end{aligned}$$

$$\#\gamma_{n,k}(G^*) \geq q^{k+m-3}(1-q^{-1})(\frac{1}{2}(q-2+\frac{q}{z}-\gamma-\frac{q-z^*}{z^2+z})+\frac{1}{b}).$$

We call the last factor B. We first consider the case where e/c is odd. In the notation of Lemma 5.9, we have $\delta = \nu(d) \geq \nu(e) = \varepsilon$, so that

$$b = \begin{cases} 2 & \text{if } p \text{ is odd,} \\ 1 & \text{if } p = 2. \end{cases}$$

If p is odd, then $\gamma = 0$ and $2/b - \gamma = 1$. If $p = 2$, then $\gamma = 1$ and again $2/b - \gamma = 2 - 1 = 1$. It follows that

$$2B = q - 2 + \frac{q}{z} - \frac{q-z}{z^2+z} + \frac{2}{b} - \gamma = q(1 + \frac{1}{z+1}(1-\frac{z}{q})).$$

In the second case, e/c is even, so that $\gamma = 0$, $\alpha \leq \beta$ and $\delta < \varepsilon$ in Lemma 5.9, so that $b = z+1$ and

$$2B = q - 2 + \frac{q}{z} - \frac{q-z^2}{z^2+z} + \frac{2}{z+1} = q(1 + \frac{1}{z+1}(1-\frac{z}{q})).$$

It follows that in all cases

$$\begin{aligned}
\#\gamma_{n,k}(G^*) &\geq \frac{1}{2}q^{k+m-2}(1-q^{-1})(1+\frac{1}{z+1}(1-\frac{z}{q})), \\
N_4 &\leq q^{k+m-2}(1-q^{-1})(1-q^{-1}-\frac{1}{2}(1+\frac{1}{z+1}(1-\frac{z}{q}))) \\
&= q^{k+m-2}(1-q^{-1})(\frac{1}{2}-\frac{1+q^{-1}}{2z+2}-\frac{q^{-1}}{2}).
\end{aligned}$$

Together we have found the following lower bounds on $\#\gamma_{n,k}(G)$. If $r \neq m$ and $\mu = 1$, then

$$\begin{aligned}
\#\gamma_{n,k}(G) \geq N_{12} &= q^{k+m-2}(1-q^{-1}(1+q^{-p+2}\frac{(1-q^{-1})^2}{1-q^{-p}}))(1-q^{-k}) \\
&= q^{k+m-2}(1-q^{-1})(1-q^{-k})\frac{1-q^{-p+1}}{1-q^{-p}}.
\end{aligned}$$

If $r \neq m$, then

$$
\begin{aligned}
\#\gamma_{n,k}(G) \geq N_{12} - N_3 \geq q^{k+m-2}&(1 - q^{-1}(1 + q^{-p+2}\frac{(1-q^{-1})^2}{1-q^{-p}}))(1-q^{-k}) \\
&- q^{k+m-1-r^*-c/e}\frac{(1-q^{-1})^2(1-q^{-r^*(\mu-1)})}{(1-q^{-c/e})(1-q^{-r^*})} \\
&\cdot (1 - q^{-r^*(p-1)}\frac{(1-q^{-r^*})(1-q^{-pr^*\mu^*})}{(1-q^{-r^*(\mu-1)})(1-q^{-pr^*})}) \\
= q^{k+m-2}\big(&(1 - q^{-1}(1 + q^{-p+2}\frac{(1-q^{-1})^2}{1-q^{-p}}))(1-q^{-k}) \\
&- q^{-r^*-c/e+1}\frac{(1-q^{-1})^2(1-q^{-r^*(\mu-1)})}{(1-q^{-c/e})(1-q^{-r^*})} \\
&\cdot (1 - q^{-r^*(p-1)}\frac{(1-q^{-r^*})(1-q^{-pr^*\mu^*})}{(1-q^{-r^*(\mu-1)})(1-q^{-pr^*})})\big).
\end{aligned}
$$

For the first inequality in the statement of (ii), we observe that $c \geq 1$ and

$$
\frac{q^{-c/e}}{1-q^{-c/e}} = \frac{p^{-c}}{1-p^{-c}} \leq 1. \tag{6.14}
$$

For the last estimate, we have $q^{-r^*} \leq 1/2$ and

$$
-\frac{1-q^{-r^*(\mu-1)}}{1-q^{-r^*}} \geq -\frac{1}{1-q^{-r^*}} \geq -2.
$$

If $r = m$, then

$$
\begin{aligned}
\#\gamma_{n,k}(G) \geq N_{12} - N_4 &\geq q^{k+m-2}(1-q^{-1})(1-q^{-k})\frac{1-q^{-p+1}}{1-q^{-p}} \\
&\quad - q^{k+m-2}(1-q^{-1})(\frac{1}{2} - \frac{q^{-1}}{2} - \frac{1+q^{-1}}{2z+2}) \\
&= q^{k+m-2}(1-q^{-1})(\frac{1}{2} + \frac{1+q^{-1}}{2z+2} + \frac{q^{-1}}{2}) \\
&\quad - q^{-k}\frac{1-q^{-p+1}}{1-q^{-p}} - q^{-p+1}\frac{1-q^{-1}}{1-q^{-p}}) \\
&= q^{k+m-2}\big(\frac{1}{2}(1 + \frac{1-q^{-2}}{z+1} - q^{-2}) \\
&\quad - (1-q^{-1})(-q^{-k}\frac{1-q^{-p+1}}{1-q^{-p}} - q^{-p+1}\frac{1-q^{-1}}{1-q^{-p}})\big). \qquad \square
\end{aligned}
$$

Example 6.15. When $n = p^2$, then we have $k = r = m = p$ in Theorem 6.1(iii). We write $\alpha_n = q^{2p-2}$, so that $\#D_n \leq \alpha_n$. Including the q^{p-1} Frobenius compositions, we obtain

$$
\begin{aligned}
\#D_n &\geq \frac{1}{2}q^{2p-2}(1-q^{-1})(1 + \frac{1+q^{-1}}{p+1} + q^{-1} - 2q^{-p+1}) + q^{p-1} \\
&= \alpha_n \cdot \big(\frac{1}{2}(1 + \frac{1}{p+1})(1-q^{-2}) + q^{-p}\big).
\end{aligned}
$$

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

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

Over an algebraically closed field of characteristic 2, a quartic polynomial is decomposable if and only if its cubic coefficient vanishes; see Example 2.6.

For $p = 3$, we find

$$\begin{aligned}
\#D_9 &\geq \alpha_9 \cdot (\frac{5}{8}(1 - q^{-2}) + q^{-3}) = \alpha_9 \cdot (\frac{5}{8} - q^{-2}(\frac{5}{8} - q^{-1})),\\
\#D_9 &\geq \frac{16}{27} \cdot \alpha_9 > 0.59259\, \alpha_9 \text{ over } \mathbb{F}_3,\\
\#D_9 &\geq \frac{451}{3^6} \cdot \alpha_9 > 0.61065\, \alpha_9 \text{ over } \mathbb{F}_9.
\end{aligned}$$

The experiments reported in von zur Gathen (2010b) show that these are serious underestimates of the actual ratios ≈ 0.8518 and ≈ 0.9542, respectively. In the same vein we find, when $n = ap^2 > p^2$ with $p \nmid a$ and $k = n/p$, that

$$\#D_{n,n/p} \geq q^{n/p+p-2} \cdot (\frac{1}{2}(1 + \frac{1}{p+1})(1 - q^{-2}) + q^{-p}). \qquad \diamondsuit$$

Example 6.16. In $\mathbb{F}_3[x]$, we have, besides the eight Frobenius collisions according to Definition 3.2, four collisions of degree 9:

$$\begin{gathered}
(x^3 + x) \circ (x^3 - x) = (x^3 - x) \circ (x^3 + x) = x^9 - x,\\
(x^3 + x^2) \circ (x^3 - x^2 - x) = (x^3 - x^2 + x) \circ (x^3 + x^2) = x^9 + x^5 - x^4 + x^3 + x^2,\\
(x^3 + x^2 + x) \circ (x^3 - x^2) = (x^3 - x^2) \circ (x^3 + x^2 - x) = x^9 + x^5 + x^4 + x^3 - x^2,\\
(x^3 + x^2 + x) \circ (x^3 - x^2 + x) = (x^3 - x^2 + x) \circ (x^3 + x^2 + x) = x^9 + x^5 + x.
\end{gathered}$$

The general bounds from Theorem 6.1 and Example 6.15 provide the first two of the following inequalities:

$$39 = 3 \cdot 13 < 48 = 3 \cdot 16 < \#D_9 = 69 = 3 \cdot 23 < 81 = 3 \cdot 27 = \alpha_9. \qquad \diamondsuit$$

Open Question 6.17. *Our approach is based on "low level" coefficient comparisons. Can the present results be (im)proved by "higher level" methods, maybe with more elegant arguments? Ritt (1922) muses in a footnote (on his page 59): "An idea which presents itself naturally is to consider this problem as one in undetermined coefficients [...] A study of the equations for the coefficients convinces me that such a plan would not be easy to carry out, and that the function-theoretic methods used here are not far-fetched."*

7. Acknowledgments

Many thanks go to Henning Stichtenoth for interesting discussions and for pointing out Antonia Bluher's work, to Konstantin Ziegler for some experiments and to the anonymous reviewers for helpful comments. An Extended Abstract of this paper appeared as part of von zur Gathen (2009). This work was supported by the B-IT Foundation and the Land Nordrhein-Westfalen.

References

SHREERAM S. ABHYANKAR (1997). Projective Polynomials. *Proceedings of the American Mathematical Society* **125**(6), 1643–1650. ISSN 00029939. URL `http://www.jstor.org/stable/2162203`.

DAVID R. BARTON & RICHARD ZIPPEL (1985). Polynomial Decomposition Algorithms. *Journal of Symbolic Computation* **1**, 159–168.

DAVID R. BARTON & RICHARD E. ZIPPEL (1976). A Polynomial Decomposition Algorithm. In *Proceedings of the third ACM Symposium on Symbolic and Algebraic Computation*, RICHARD D. JENKS, editor, 356–358. ACM Press, Yorktown Heights, New York, United States. URL `http://dx.doi.org/10.1145/800205.806356`.

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`.

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 `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. URL `http://dx.doi.org/10.1016/S0747-7171(08)80014-4`.

JOACHIM VON ZUR GATHEN (1990b). Functional Decomposition of Polynomials: the Wild Case. *Journal of Symbolic Computation* **10**, 437–452. URL `http://dx.doi.org/10.1016/S0747-7171(08)80054-5`.

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 (2009). The Number of Decomposable Univariate Polynomials — Extended Abstract. In *Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation ISSAC2009,* Seoul, Korea, JOHN P. MAY, editor, 359–366. ISBN 978-1-60558-609-0. Preprint (2008) at `http://arxiv.org/abs/0901.0054`.

JOACHIM VON ZUR GATHEN (2010a). Normal form for Ritt's Second Theorem. *Submitted,* 39 pages.

JOACHIM VON ZUR GATHEN (2010b). Counting decomposable univariate polynomials 42 pages. Preprint.

JOACHIM VON ZUR GATHEN (2010c). Counting decomposable multivariate polynomials. *To appear in Applicable Algebra in Engineering, Communication and Computing*. Abstract in "Abstracts of the Ninth International Conference on Finite Fields and their Applications", pages 21–22, Dublin, July 2009, Claude Shannon Institute, `http://www.shannoninstitute.ie/fq9/AllFq9Abstracts.pdf`.

JOACHIM VON ZUR GATHEN & JÜRGEN GERHARD (2003). *Modern Computer Algebra.* Cambridge University Press, Cambridge, UK, Second edition. ISBN 0-521-82646-2, 800 pages. URL `http://cosec.bit.uni-bonn.de/science/mca/`. Other available editions: first edition 1999, Chinese edition, Japanese translation.

JOACHIM VON ZUR GATHEN, MARK W. GIESBRECHT & KONSTANTIN ZIEGLER (2010). Composition collisions and projective polynomials. *Preprint*. URL `http://arxiv.org/abs/1005.1087`. Extended abstract in Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation ISSAC2010, Munich, Germany.

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. URL http://dx.doi.org/10.1109/SFCS.1987.29. Final version in Journal of Symbolic Computation.

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. Available as http://arxiv.org/abs/1004.5433.

Johannes Grabmeier, Erich Kaltofen & Volker Weispfenning (editors) (2003). *Computer Algebra Handbook – Foundations, Applications, Systems*. Springer-Verlag, Berlin, Heidelberg, New York. ISBN 3-540-65466-6. URL http://www.springer.com/978-3-540-65466-7.

Jaime Gutierrez & Dexter Kozen (2003). Polynomial Decomposition. In Grabmeier *et al.* (2003), section 2.2.4 (pages 26–28). URL http://www.springer.com/978-3-540-65466-7.

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.

Dexter Kozen & Susan 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. An earlier version was published as Kozen & Landau (1986).

Dexter Kozen, Susan Landau & Richard Zippel (1996). Decomposition of Algebraic Functions. *Journal of Symbolic Computation* **22**, 235–246.

J. F. Ritt (1922). Prime and Composite Polynomials. *Transactions of the American Mathematical Society* **23**, 51–66. URL http://www.jstor.org/stable/1988911.

Andrzej Schinzel (1982). *Selected Topics on Polynomials*. Ann Arbor; The University of Michigan Press. ISBN 0-472-08026-1.

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.

Richard Zippel (1991). Rational Function Decomposition. In *Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation ISSAC '91,* Bonn, Germany, Stephen M. Watt, editor, 1–6. ACM Press, Bonn, Germany. ISBN 0-89791-437-6.