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/

ABSTRACT

A univariate polynomial \( f \) over a field is decomposable if it is a composition \( f = gh \) 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 does not divide the degree \( n \) of \( f \), is reasonably well understood, and we obtain exponentially decreasing error bounds.

In 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; F.2.2 [Analysis of Algorithms and Problem Complexity]: Counting problems; I.1.2 [Algorithms]: Algebraic algorithms.

General Terms: Algorithms.

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

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.

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. His interest, dating back to the supervision of this thesis, was rekindled by a study of similar (but multivariate) counting problems (von zur Gathen 2002a) and during a visit to Pierre Dèbes’ group at Lille, where I received a preliminary version of Bodin, Dèbes & Najib (2009). Mul-
tivariate 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, squarefree, 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 \( \text{lc}(f) \) 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 \( g, h \); 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
\[
f = g \circ h \iff a \circ f = (ag + b) \circ h
\]
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
\[
P_n = \{ f \in F[x] : \deg f \leq n \}
\]
for the vector space of polynomials of degree at most \( n \), of dimension \( n + 1 \). Furthermore, we consider the subsets
\[
P^{w}_n = \{ f \in P_n : \deg f = n \},
P^{o}_n = \{ f \in P^{w}_n : f \text{ monic and original} \}.
\]
For any divisor \( e \) of \( n \), we have the normal composition map
\[
\gamma_{n,e} : P^{w}_n \times P^{o}_{n/e} \to P^w_n, \quad (g, h) \mapsto g \circ h,
\]
corresponding to Definition 1, and set
\[
D_{n,e} = \im \gamma_{n,e}.
\]
The set \( D_n \) of all decomposable polynomials in \( P^w_n \) is
\[
D_n = \bigcup_{1 < c < n} D_{n,c}.
\]
In particular, \( D_n = \emptyset \) if \( n \) is prime. We also let \( I_n = P^w_n \setminus D_n \) be the set of indecomposable polynomials. Over a finite field \( F_q \) with \( q \) elements, we have
\[
\#P^w_n = q^{n+1}(1 - q^{-1}),
\]
\[
\#P^{o}_n = q^{n-1},
\]
\[
\#D_{n,e} \leq q^{e+n/e}(1 - q^{-1}).
\]

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 \( \alpha_n \) on \( \#D_{n,e} \), 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 of \( n \). A result of von zur Gathen (1990b) implies a lower bound of about \( \alpha_n/An \) 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
\[
g \circ h = g^* \circ h^*
\]
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 \( p | \deg g \), 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 Bluhler (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 \( p \nmid k \), 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
\[
d \geq 1, \quad r = p^d, \quad k = ar, \quad m \geq 2, \quad n = km, \quad \kappa \leq 0 < k \quad \text{and} \quad p \nmid \alpha,
\]
and polynomials
\[ g = x^k + \sum_{1 \leq i \leq n} g_i x^i, \]
\[ h = \sum_{1 \leq i \leq m} h_i x^i, \]
\[ f = g \circ h = h^k + \sum_{1 \leq i \leq n} g_i h_i, \] (5)
with \( h_m = 1, h_{m-1} \neq 0 \), and either \( g_k \neq 0 \) 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 \( g_k h_i \). Special situations arise when the latter two polynomials both contribute to a coefficient. We denote by
\[ h^{(i)} = \sum_{i < b \leq cm} h_b x^b \]
the top part of \( h_i \), so that \( h^{(m-1)} = 0 \). Furthermore, we write \( \text{coeff}(v, j) \) for the coefficient of \( x^j \) in a polynomial \( v \), and
\[ c_{i,j}(v) = \text{coeff}(v \circ (h - h^{(i)}), j). \]
Thus \( c_{m-1,j}(x^k) = \text{coeff}(h^k, j) \), and in particular, we have \( c_{m-1,j}(g) = f_j \) for all \( j \). To illustrate the usage of these \( c_{i,j} \), we consider \( E_1 \) below. At some point in the algorithm, we have determined \( g_k, h_{m-1}, \ldots, h_{i+1} \). The appropriate \( c_{i,j} \) exhibits \( h_i \) in a simple fashion, meaning that we can compute it from \( f_j \) and \( h^{(i)} \).

Let us define the rational number
\[ i_0 = m(\frac{\kappa-a}{r-1} - a + 1) = \frac{km - n}{r - 1} + m; \]
thus \( i_0 < m \), and \( i_0 \) is an integer if and only if
\[ r - 1 \mid (\kappa - a)m. \]

**Lemma 6.** For \( 1 \leq i \leq m \) and \( 0 \leq j \leq n \), we have the following.

\[ E_1: \text{If } i < m, \text{ then } \]
\[ c_{i,(n-1)m+i}(g_k x^i) = \kappa g_k h_i, \]
and \( c_{m-1,nm}(g_k x^i) = g_k. \)

\[ E_2: \text{If } i < m, \text{ then } \]
\[ c_{i,n-(m-1)i}(x^k) = a h_i. \]
If \( r \nmid j \), then \( \text{coeff}(h^k, j) = 0. \)

\[ E_3: \text{If } i_0 \in \mathbb{N}, \text{ then } \]
\[ c_{i_0,(n-1)m+i_0}(x^k + g_k x^n) = ah_0 + \kappa g_k h_{i_0}. \]

\[ E_4: \text{If } m = r \text{ and } \kappa = k = -1, \text{ then } \]
\[ c_{m-1,nm}(x^k + g_k x^n) = ah_{m-1} + g_k, \]
\[ c_{m-1,nm-1}(x^k + g_k x^n) = -g_k h_{m-1}. \]

In the following algorithm, the instruction "determine \( h_i \) (or \( g_k \)) by \( E_\mu \) (at \( x^\mu \)), for \( 1 \leq \mu \leq 4 \), means that the property \( E_\mu \) involves some quantity \( c_{i,j}(v) \) which is a summand in \( \text{coeff}(g \circ h, j) = f_j \); the other summands are already known, and we can solve for \( h_i \) (or \( g_k \)). 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 \( km \) of \( g_k h^n \) 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 \( p = \text{char} \mathbb{F}_q, d \geq 1, r = p^d \), 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 \( d \geq 2 \) 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 \( p \mid m \) then if \( m \mid j \) then return “failure” else set \( \kappa = j/m \). If \( p \nmid m \) then if \( m \mid j + 1 \) then return “failure” else set \( \kappa = (j + 1)/m \). If \( p \mid \kappa \), then return “failure”.

Calculate \( i_0 = (km - n)/(r - 1) + m. \)

3. If \( km \geq n - r + 2 \) then do the following.

a. Set \( g_k = f_{km}. \)

b. Determine \( h_i \), for \( i = m - 1, \ldots, 1 \) by \( E_1 \).

4. If \( km = n - r + 1 \) then do the following.

a. Set \( g_k = f_{km}. \)

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 \( km = n - r \) 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
\[ as^{s+1} - f_{km} s - f_{km-1} = 0. \] (8)
If \( S = \emptyset \) 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 \( g_k \) by \( E_1 \) and \( E_2 \) at \( x^{km} \), from \( f_{km} = ah_{m-1} + g_k. \)

c. For \( i = m - 2, \ldots, 1 \) determine \( h_i \) by \( E_1 \).

6. If \( km < n - r \) then do the following.

a. Determine \( h_{m-1} \) by \( E_2 \).

b. If \( r \nmid m \) then determine \( g_k \) by \( E_1 \) at \( x^{km} \) (as \( g_k = f_{km} \)), else by \( E_1 \) at \( x^{km-1} \) (via \( g_k h_{m-1} = f_{km-1} \)).

c. Determine \( h_i \) for decreasing \( i \) with \( m - 2 \geq i > i_0 \) 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 \( i_0 > i > 1 \) by \( E_1 \).

[We now know \( h. \)]

7. Compute the remaining coefficients \( g_1, \ldots, g_{m-1} \) 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 & Gerhard (1990a).

We first illustrate the algorithm in some examples.

**Example 9.** We let \(p = 5\), \(n = 50\), and \(k = 5\), so that \(d = 1 = m = 10\), and start with \(\kappa = 4 = r = 1\). We assume \(f_{20} = g_{20}h_{20} \neq 0\). Then
\[
\begin{align*}
h^5 + 4g^4h^4 = & \, x^{20} + h_2x^{15} + (h_5 + g_4)x^{10} + 4g_4h_9x^9 \\
+ & \, g_4(4h_8 + h_5^2)x^{8} + x^6 \cdot (x + h_7^2 + g_4(4h_8 + h_9h_6) \\
+ & \, h_8h_7 + h_5^2h_7 + h_6^2h_5 + h_7^3h_5) x^{25} + O(x^{34}).
\end{align*}
\]

Step 1 determines \(j = 39\), and step 2 finds \(\kappa = (39 + 1)/10 = 4\) in step 6. Step 6.a computes \(h_6\) at \(x^{49}\). This yields \(g_4\) at \(x^{39}\), step 6.c determines \(h_6\) at \(x^{39}\) by \(E_2\), step 6.d is skipped, and then step 6.e yields \(h_7, \ldots, h_1\) at \(x^{31}, \ldots, x^{35}\), 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
\[
\begin{align*}
h^5 + 3g_3h^3 = & \, x^{20} + h_2x^{15} + h_5^3x^{10} + h_7^3x^{25} \\
+ & \, (h_5^2 + g_3)x^{20} + 3g_3h_9x^{29} + g_3(3h_5^2 + 3h_8)x^{28} \\
+ & \, x^6 \cdot O(x) + (h_2^3 + g_3(3h_5 + 3h_6h_4 + 3h_8h_7 \\
+ & \, 3h_5^2h_7 + 3h_7^2h_5)) x^{25} + O(x^{24}).
\end{align*}
\]

Assuming that \(f_{20} = 3g_3h_6 \neq 0 \), the algorithm computes \(j = 29\), \(\kappa = (29 + 1)/10 = 3\). Then \(f_{20} = g_{20}h_{20} \neq 0\). 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 \(f_{20} = 0\):

\[
\begin{align*}
6 & \text{ for } 1 \cdot 124 \text{ values of } f_{20}, f_{19}, \\
2 & \text{ for } 47 \cdot 124 \text{ values of } f_{20}, f_{19}, \\
1 & \text{ for } 25 \cdot 124 \text{ values of } f_{20}, f_{19}, \\
0 & \text{ for } 52 \cdot 124 \text{ values of } f_{20}, f_{19}, \\
\end{align*}
\]

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

We denote by \(M(n)\) a multiplication time, so that polynomial degrees of \(m\) at \(n\) can be multiplied with \(M(n)\) operations in \(\mathbb{F}_q\). Then \(M(n)\) is in \(O(n \log n \log \log n)\); 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 \(p, q = p^r, d, r, a, k, \) as specified, \(g, h, \) and \(i_0\) as in 5 and 3, so that \(f = g \circ h\), set \(c = \gcd(d, e)\) and suppose further that
\[
\begin{align*}
\text{if } i_0 \in \mathbb{N} \text{ and } 1 < i_0 < m, \text{ then } (-k_0/a) ^{(q-1)/(q^r-1)} \neq 1.
\end{align*}
\]

On input \(f\), Algorithm 7 returns either “failure” or a set of at most \(\sigma(f)\) normal decompositions \((g^s, h^s)\) 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
\[
O(M(n) \log k (m + \log(kq)))
\]
or \(O^-((n(m + \log g))\) operations in \(\mathbb{F}_q\).

**Proof.** Since \(r = p^d \mid k\), we have \(\text{coeff}(h^k, j) = 0\) unless \(r \mid j\). Furthermore, \(g_i^k h_i = g_i x^m + k g_i h_i x^{m-1} + O(x^{c m - 2})\) and \(k g_i h_{i-1} \neq 0\), so that \(j + 1\) from step 1 equals \(k m (p \mid m) + k m - 1 (p \mid m)\). Thus \(k\) 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 \(j = \kappa (m-1) + i\) 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
\[
\begin{align*}
n - r (m - i) & \geq (\kappa - 1)m + i \text{ if and only if } i \geq i_0, \\
& \text{since the first linear function in } i \text{ has the slope } r > 1, \text{ greater than for the second one. Since } i \geq 1, \text{ it follows that } j > (\kappa - 1)m \text{ for all } j \text{ under consideration. For the low-degree part of } g \text{ we have}
\end{align*}
\]
\[
\text{deg}(g - g \cdot (x^k + g_n x^n)) \circ h) \leq (\kappa - 1)m < j,
\]
so that
\[
\text{f}_j = \text{coeff}(g \circ h, j) = \text{coeff}(h^k + g_n h^c, j)
\]
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 \(a s^t + k g_s\), is an \(\mathbb{F}_q\)-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 \(a s^t + k g_s = 0\), then \(-k_0/a = s^{r-1}\). Writing \(z = p^r\), so that \(z - 1 = \gcd(q - 1, r - 1)\), we have
\[
\begin{align*}
-\frac{k_0}{a} & = (q - 1)/(z - 1) = 1,
\end{align*}
\]
contradicting the condition (11).
For the correctness it is sufficient to show that all required quantities are known, in particular $c_{i,j}(g, x)$ in $E_1$ and $c_{i,j}(x^p)$ in $E_2$, and that the equations determine the coefficient to be computed. We have
$$\deg(h^k - x^n) = \deg((h^k - x^{am})^\gamma) \leq (am - 1)r = n - r,$$
so that $g_a = f_{km}$ in steps 3.a and 4.a. The preconditions of step 3 implies that for all $i < m$ we have
$$(\kappa - 1)m \geq n - r - m + 2 > n - rm + (r - 1)i,$$
$$n - r(m - i) < (\kappa - 1)m + i.$$
Thus from $E_1$ we have with $j = (\kappa - 1)m - i$
$$f_{(n-1)m+i} = \text{coeff}(h^k, j) + \text{coeff}(g_a h^r, j) = \text{coeff}(h^{(i)}k, j) + \kappa g_a h_i,$$
with $\kappa g_a \neq 0$, so that $h_i$ can be computed in step 3.b.

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

The only usage of $E_4$ occurs in step 5.a, where $\kappa = (n - r)/m = k - r/m$. Since $p \not| k, r$ is a power of $p$, and $p \not| \kappa$, this implies that $r = m$ and $\kappa = k - 1$. We have from $E_4$
$$f_{km} = ah_{km-1} + g_a,$$
$$f_{km-1} = g_a h_{km-1} = ah_{km-1} - f_{km} h_{km-1}.$$  
Thus $h_{km-1} \in S$ as computed in step 5.a and $g_a$ 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 $r \not| m$, then coeff($h^k, km$) = 0 by $E_2$, and otherwise coeff($h^k, km-1$) = 0. Thus $g_a$ 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 computing $h^{(i)}k$ for some $j < m$ and the various $r$th roots. The first comes to $O(m \cdot \log k \cdot \text{M}(n))$ and the second one to $O(m \cdot \log q)$ operations in $F_q$. $E_3$ 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 $O(M(r) \log r \log qr)$ operations (see von zur Gathen & Gerhard (2003), Corollary 14.16). The Taylor coefficients in step 7 can be calculated with $O(M(n) \log k)$ 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
$$O(M(n) \log k \cdot (m + \log(kq))). \tag{\Box}$$

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 $\sigma(f) \leq r + 1$. $N$ 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 derived to give the following lower bounds.

**Corollary 12.** Let $F_q$ have characteristic $p$ with $q = p^n$, and take integers $\ell \geq 2$, $r = p^\ell$, $t = ar$ with $p \not| \mu$, $m \geq 2$, $n = \ell m$, $c = gcd(d, e)$, $z = p^\ell$, $\mu = gcd(r - 1, m)$, $r^\ell = (r - 1)/\mu$, and let $G$ consist of the $(g, h)$ as in Theorem 10. Then we have the following lower bounds on the cardinality of $\gamma_{n,t}(G)$.

(i) If $r \not| m$ and $\mu = 1$:
$$q^{\ell+1}(1 - q^{-1})(1 - q^{-t})(1 - q^{-1}(1 + q^{-\ell+2}(1 - q^{-1})^2)).$$

(ii) If $r \not| m$:
$$q^{\ell+1}(1 - q^{-1})$$
$$((1 - q^{-1} + q^{-r+2}(1 - q^{-1})^2)(1 - q^{-t}))$$
$$- q^{-t-r^{-c}+2}(1 - q^{-1})^2(1 - q^{-r}(j))$$
$$((1 + q^{-r}(p-2)).$$

(iii) If $r = m$:
$$q^{\ell+1}(1 - q^{-1})^2 \frac{1}{2} + \frac{q^{-1}}{2s + 2} + \frac{q^{-1}}{2} - q^{-r} - q^{-r+1}$$
$$- q^{-1} \frac{1}{2}$$
$$\frac{1}{2} q^{-r}.$$

The algorithm works over any field of characteristic $p$ where each element has a $p$th root; in $F_q$, 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
$$\#D_n \geq \alpha_n \cdot \left(\frac{1}{2}(1 + \frac{1}{p+1})(1 - q^{-2}) + q^{-r} \right).$$

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
$$\#D_1 = \alpha_4 \cdot \frac{2}{3} (1 - q^{-2}) + q^{-2} = \alpha_4 \frac{2 + q^{-2}}{3},$$
$$\#D_4 = \frac{3}{4} \alpha_4 \text{ over } F_2,$$
$$\#D_4 = \frac{11}{16} \alpha_4 \text{ over } F_4.$$  

Bodin et al. (2009) state without proof that $D_n \approx \frac{1}{2} \alpha_n$ over $F_2$ for even $n \geq 6$.

4. DISTINCT-DEGREE COLLISIONS

The following are examples of collisions:
$$x^k w_i \circ x^k = x^{kn} w_i (x^n) = x^{kn} \circ x^k w(x^n),$$
for any polynomial $w \in F[x]$, where $F$ is a field (or even a ring), and
$$T_n(x, y^n) \circ T_n(x, y) = T_m(x, y) = T_n(x, y^n) \circ T_m(x, y),$$
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:

\[
\deg g = \deg h^* = m, \quad \deg h = \deg g^* = \ell, \tag{14}
\]

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

\[
f = g \circ h = g^* \circ h^*, \tag{16}
\]

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 \( s = [m/\ell] \) and \( c \in F \) so that

\[
f = (x - c)^k w^t(c') \circ x^k w^t(x') \circ (x + c),
\]

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

\[
k w + \ell x w' \neq 0 \quad \text{and} \quad p \nmid \ell,
\]

(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

\[
p \nmid n,
\]

\[
g = (x - T_n(b, z)) \circ T_m(x, z') \circ (x + T_l(b, z)),
\]

\[
h = (x - T_l(b, z)) \circ T_l(x, z) \circ (x + b),
\]

\[
g^* = (x - T_n(b, z)) \circ T_l(x, z^m) \circ (x + T_m(b, z)),
\]

\[
h^* = (x - T_m(b, z)) \circ T_m(x, z) \circ (x + b).
\]

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 \( \ell \) and \( m \) be integers with \( m > \ell \geq 2 \) and \( \gcd(\ell, m) = 1 \), \( n = \ell m \), \( s = [m/\ell] \), and \( t = \#(D_{n, \ell} \cap D_{n, m} \cap D_n) \). Using Kronecker’s \( \delta \), the following hold.

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

\[
t = (q^{s+\delta} + (1 - \delta)(q^\ell - q^\ell))(1 - q^{-1}).
\]

(ii) If \( p \nmid \ell \), 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 \( \ell \) be a prime number, \( m \neq \ell \) a multiple of \( \ell \) with \( p \nmid m \) and without a prime divisor less than \( \ell \), 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

\[
q^{2t + n^2 / 2 - 1}(1 - q^{-1}) \leq t \leq q^{2t + n^2 / 2 - 1}(1 - q^{-1})(1 + q^{-n/3}).
\]

(ii) If \( n = \ell^3 \), then \( t = q^{\ell^2 - 1}(1 - q^{-1}) \).

**Theorem 22.** Let \( \mathbb{F}_q \) be a finite field of characteristic \( p \), \( \ell \) 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

\[
t \leq q^{m + [1/p] + 1}(1 - q^{-1}).
\]

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

\[
t \leq q^{m + p - m/p + [m/p] + 1}(1 - q^{-1}).
\]

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 \( 2q^{n/2}/(1 - q^{-1}) \), with its dependence on \( \ell \) 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 \( p \nmid n \), \( \ell \) the smallest and second smallest nontrivial divisor of \( n \), respectively (with \( \ell_2 = 2 \) if \( n = \ell \) or \( n = \ell^2 \)), \( s = [n/\ell^2] \), and
\begin{equation}
\alpha_n = \begin{cases} 
0 & \text{if } n = \ell, \\
q^{2^i(1 - q^{-1})} & \text{if } n = \ell^2, \\
2q^{i+n/\ell}(1 - q^{-1}) & \text{otherwise,}
\end{cases} 
\end{equation}

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

\[ \beta_n = \begin{cases} 
0 & \text{if } n \in \{\ell, \ell^2, \ell^3, \ell \ell_2\}, \\
q^{-\ell} & \text{otherwise,}
\end{cases} 
\]

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

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

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

\section{COUNTING GENERAL DECOMPOSABLE POLYNOMIALS}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{tree.png}
\caption{The tree of case distinctions for estimating \#\(D_n\).}
\end{figure}

In the wild case \( p \nmid n \), 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.

<table>
<thead>
<tr>
<th>Figure 1</th>
<th>lower bound on #(D_n/\alpha_n)</th>
<th>upper</th>
</tr>
</thead>
<tbody>
<tr>
<td>I.A</td>
<td>1 ((1 + \frac{1}{\sqrt{q}})(1 - q^{-2}) + q^{-p} &gt; 1/2)</td>
<td>1</td>
</tr>
<tr>
<td>II.A.i</td>
<td>(1 - \beta_n^* \geq 1 - q^{-n/\ell - n/\ell^2 + 3})</td>
<td>1</td>
</tr>
<tr>
<td>II.A.ii.a</td>
<td>(1 - 2q^{-n/\ell - n/\ell^2 - 1})</td>
<td>1</td>
</tr>
<tr>
<td>II.A.ii.b</td>
<td>(1 - q^{-n/\ell + n/\ell^2 - 1})</td>
<td>1</td>
</tr>
<tr>
<td>II.B.i.a</td>
<td>(1 - (q^{-1} + q^{-p+1} + q^{-n/\ell - n/\ell^2 + 2}/2)</td>
<td>1</td>
</tr>
<tr>
<td>II.B.i.b</td>
<td>(1 - (q^{-1} - q^{-p})/2)</td>
<td>1</td>
</tr>
<tr>
<td>II.B.ii.a</td>
<td>(1 - (q^{-1} + q^{-p+1} - q^{-p} + q^{-\ell+1})/2)</td>
<td>1</td>
</tr>
<tr>
<td>II.B.ii.b</td>
<td>(1 - \frac{q^{-1} + q^{-p+1} - q^{-p} - q^{-\ell+1}}{2(1 + p^{-1})})</td>
<td>1</td>
</tr>
<tr>
<td>II.B.ii.b</td>
<td>(\frac{q^{-1} - q^{-p+1}}{2})</td>
<td>1</td>
</tr>
</tbody>
</table>

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

\begin{thm}
Let \( \mathbb{F}_q \) be a finite field of characteristic \( p \), and \( \ell \) 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.

\begin{thm}
Let \( \mathbb{F}_q \) be a finite field with \( q \) elements and characteristic \( p \), let \( \ell \) be the smallest prime divisor of the composite integer \( n \geq 2 \), and \( \alpha_n \) as in (24). Then the following hold.

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

(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 \( \#D_n \geq (3 - 2q^{-1})\alpha_n/4 \geq q^{2\sqrt{\frac{n}{2}}} / 4 \).

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

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

\end{thm}

\begin{openq}
• In the case where \( p = \ell \) and \( p^2 \nmid n \), 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?

\end{openq}
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 Aaimani 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


