Composition Collisions and Projective Polynomials

Statement of Results*

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

Mark Giesbrecht
Cheriton School of Computer Science
University of Waterloo, Waterloo, ON, N2L 3G1 Canada
mwg@cs.uwaterloo.ca
http://www.cs.uwaterloo.ca/~mwg

Konstantin Ziegler
B-IT, Universität Bonn
D-53113 Bonn, Germany
zieglerk@bit.uni-bonn.de
http://cosec.bit.uni-bonn.de/

ABSTRACT

The functional decomposition of polynomials has been a topic of great interest and importance in pure and computer algebra and their applications. The structure of compositions of (suitably normalized) polynomials $f = g \circ h$ in $\mathbb{F}_q[x]$ is well understood in many cases, but quite poorly when the degrees of both components are divisible by the characteristic p. This work investigates the decomposition of polynomials whose degree is a power of p. An (equal-degree) *i-collision* is a set of i distinct pairs (g, h) of polynomials, all with the same composition and $\deg g$ the same for all (g, h). Abhyankar (1997) introduced the *projective polynomials* $x^n + ax + b$, where n is of the form $(r^m - 1)/(r - 1)$ and r is a power of p. Our first tool is a bijective correspondence between i-collisions of certain additive trinomials, projective polynomials with i roots, and linear spaces with i Frobenius-invariant lines.

Bluher (2004b) has determined the possible number of roots of projective polynomials for $m = 2$, and how many polynomials there are with a prescribed number of roots. We generalize her first result to arbitrary m, and provide an alternative proof of her second result via elementary linear algebra.

If one of our additive trinomials is given, we can efficiently compute the number of its decompositions, and similarly the number of roots of a projective polynomial. The runtime of these algorithms depends polynomially on the sparse input size, and thus on the input degree only logarithmically.

For non-additive polynomials, we present certain decompositions and conjecture that these comprise all of the prescribed shape.

ISSAC 2010, 25–28 July 2010, Munich, Germany

Categories and Subject Descriptors

F.2.1 [**Analysis of Algorithms and Problem Complexity**]: Numerical Algorithms and Problems—*Computations on polynomials*

General Terms

Theory

Keywords

Univariate polynomial decomposition, additive polynomials, linearized polynomials, projective polynomials

1. INTRODUCTION

The *composition* of two polynomials $g, h \in F[x]$ over a field F is denoted by $f = g \circ h = g(h)$, and then (g, h) is a *decomposition* of f. In the 1920s, Ritt, Fatou, and Julia studied structural properties of these decompositions over $\mathbb{C}$, using analytic methods. Particularly important are two theorems by Ritt on uniqueness, in a suitable sense, of decompositions, the first one for (many) indecomposable components and the second one for two components, as above.

The theory was algebraicized by Dorey & Whaples (1974), Schinzel (1982, 2000), and others. Its use in a cryptographic context was suggested by Cade (1985). In computer algebra, the method of Barton & Zippel (1985) requires exponential time but works in all situations. A breakthrough result of Kozen & Landau (1989) was their polynomial-time algorithm to compute decompositions. One has to distinguish between the *tame case*, where the characteristic p does not divide $\deg g$ and this algorithm works (see von zur Gathen (1990a)), and the *wild case*, where p divides $\deg g$ (see von zur Gathen (1990b)). In the wild case, considerably less is known, mathematically and computationally. The algorithm of Zippel (1991) for decomposing rational functions suggests that the block decompositions of Landau & Miller (1985) (for determining subfields of algebraic number fields) can be applied to the wild case. Giesbrecht (1998) provides fast algorithms for the decomposition of additive (or linearized) polynomials,

*Subtitle suggested by the Programme Committee Chair in some sense an "extremely wild" case. We exploit their elegant structure here. An enumeration of number or structure of solutions in the wild case has defied both algebraic and computational analysis, and we attempt to address this here. Moreover, many of the algorithms we present here are sensitive to the sparse size of the input, as opposed to the degree, a property not exploited in the above-mentioned papers.

The task of counting compositions over a finite field of characteristic p was first considered in Giesbrecht (1988). Von zur Gathen (2009) presents general approximations to the number of decomposable polynomials. These come with satisfactory (rapidly decreasing) relative error bounds except when p divides $n = \deg f$ exactly twice. The goal of the present work is to study the easiest of these difficult cases, namely when $n = p^2$ and hence $\deg g = \deg h = p$. However, many of our results are valid for more general powers of p and stated accordingly.

We introduce the notion of an equal-degree *i-collision* of decompositions, which is a set of i pairs (g, h), all with the same composition and $\deg g$ the same for all (g, h). These are the only collisions we consider in this paper, and we omit the adjective "equal-degree" in the text. An i-collision is *maximal* if it is not contained in an $(i+1)$-collision. After some preliminaries in Section 2, we start in Section 3 with the particular case of additive polynomials. We relate the decomposition question to one about eigenspaces of the linear function given by the Frobenius map on the roots of f. This yields a complete description of all decompositions of certain additive trinomials in terms of the roots of the *projective polynomials* $x^n + ax + b$, introduced by Abhyankar (1997), where n is of the form $(r^m - 1)/(r - 1)$, for a power r of p. We prove that maximal i-collisions of additive polynomials of degree r^2 exist only when i is 0, 1, 2 or $r + 1$, count their numbers exactly, and show their relation to the roots of projective polynomials for $m = 2$. In this case Bluher (2004b) has determined, the number of roots that can occur, namely 0, 1, 2, or $r + 1$, and also for how many coefficients (a, b) each case happens. We obtain elementary proofs of a generalization of her first result to arbitrary m and of her counts for $m = 2$. From the proof we obtain a fast algorithm (polynomial in r and $\log q$) to count the number of roots over $\mathbb{F}_q$, called *rational* roots. More generally, in Section 4 an algorithm is provided to enumerate the possible number of right components of an additive polynomial of any degree. A fast algorithm is then presented to count the number of right components of an additive polynomial of any degree, which is shown to be equivalent to counting rational roots of projective polynomials of arbitrary degree. We also demonstrate theorems and fast algorithms to count and construct indecomposable additive polynomials of prescribed degree. In Section 5 we actually construct and enumerate all additive polynomials of degree r^2 with 0, 1, 2, or $r + 1$ collisions and establish connections to the counts of Bluher (2004b) and von zur Gathen (2009).

In Section 6 we move from additive to general polynomials. Certain $(r + 1)$-collisions are derived from appropriate roots of projective polynomials. We conjecture that these are all possibilities and present results on general i-collisions with $i \geq 2$ for $r = p$ that support our conjecture.

Due to the page restriction, no proofs appear here. They can be found in the full version (von zur Gathen, Giesbrecht & Ziegler, 2010).

2. THE BASIC SETUP

We consider polynomials $f, g, h \in \mathbb{F}_q[x]$ over a finite field $\mathbb{F}_q$ of characteristic p. Then $f = g \circ h = g(h)$ is the *composition* of g and h, (g, h) is a *decomposition* of f, and g and h are a *left* and *right component*, respectively, of f. Furthermore, f is *decomposable* if such (g, h) exist with $\deg g, \deg h \geq 2$, and *indecomposable* otherwise.

We call f *original* if its graph passes through the origin, that is, if $f(0) = 0$. Composition with linear polynomials introduces inessential ambiguities in decompositions. If $f = g \circ h, a \in \mathbb{F}_q^\times$, and $b \in \mathbb{F}_q$, then $af + b = (ag + b) \circ h$. Thus we may assume f to be monic original. Furthermore, if $a = \mathrm{lc}(h)^{-1}$ and $b = -ah(0)$, then $f = g \circ h = g((x - b)a^{-1}) \circ (ah + b)$ and the right component is monic original. Therefore we may also assume h to be monic original, and then g is so automatically. We thus consider the following two sets:

$$P_n(\mathbb{F}_q) = \{f \in \mathbb{F}_q[x] \colon f \text{ is monic and original of degree } n\},$$
$$D_n(\mathbb{F}_q) = \{f \in P_n(\mathbb{F}_q) \colon f \text{ is decomposable}\}.$$

We usually leave out the argument $\mathbb{F}_q$. The size of the first set is $\#P_n = q^{n-1}$, and determining (exactly or approximately) $\#D_n$ is one of the goals in this business. The number of all or all decomposable polynomials of degree n, not restricted to P_n, is $\#P_n$ or $\#D_n$, respectively, multiplied by $q(q - 1)$.

First, we consider the additive or linearized polynomials, which have a mathematically rich and highly useful structure in finite fields. First introduced in Ore (1933), they play an important role in the theory of finite and function fields, and they have found many applications in codes and cryptography. See Lidl & Niederreiter (1983), Chapter 3, for an introduction and survey over finite fields.

We focus on additive polynomials over finite fields, though some of these results will hold more generally in characteristic p. We take a power r of p and a power q of r. Let

$$\mathbb{F}_q[x; r] = \{\sum_{0 \leq i \leq m} a_i x^{r^i} : m \in \mathbb{Z}_{\geq 0},\ a_0, \ldots, a_m \in \mathbb{F}_q\}$$

be the ring of *r-additive* (or *linearized*, or simply *additive*) polynomials over $\mathbb{F}_q$. These are the polynomials such that $f(\alpha a + \beta b) = \alpha f(a) + \beta f(b)$ for any $\alpha, \beta \in \mathbb{F}_r$, and for any $a, b \in \overline{\mathbb{F}}_q$, where $\overline{\mathbb{F}}_q$ is an algebraic closure of $\mathbb{F}_q$. The additive polynomials form a (non-commutative) ring under the usual addition and composition. It is a principal left (and right) ideal ring with a left (and right) Euclidean algorithm.

An additive polynomial is squarefree if f' (the derivative of f) is nonzero, meaning that the linear coefficient of f is nonzero. If $f \in \mathbb{F}_q[x; r]$ is squarefree of degree r^m, then the set of all roots of f form an $\mathbb{F}_r$-vector space in $\overline{\mathbb{F}}_r$ of dimension m. Conversely, for any finite dimensional $\mathbb{F}_r$-vector space $W \subseteq \overline{\mathbb{F}}_r$, the lowest degree polynomial $f = \prod_{a \in W}(x - a) \in \overline{\mathbb{F}}_r[x]$ with W as its roots is a squarefree r-additive polynomial. Let σ_q denote the qth power Frobenius automorphism on $\overline{\mathbb{F}}_q$ over $\mathbb{F}_q$. If W is invariant under σ_q, then $f \in \mathbb{F}_q[x; r]$.

We have

$$x^p \circ h = \sigma_p(h) \circ x^p$$

for $h \in \mathbb{F}_q[x]$, where σ_p is the Frobenius automorphism on $\mathbb{F}_q$ over $\mathbb{F}_p$, which extends to polynomials coefficientwise. If $\deg h = p$ and $h \neq x^p$, this is a 2-collision and called a *Frobenius collision*. It is never part of i-collisions with $i \geq 3$.

Lemma 2.1. *Let $S \in \mathbb{F}_r^{m\times m}$ be the matrix representing the Frobenius σ_q. There is a bijection between S-invariant subspaces of $\mathbb{F}_r^{m\times 1}$ and right components $h \in \mathbb{F}_q[x;r]$ of f.*

We present two related approaches to investigate $f \in \mathbb{F}_q[x;r]$ of degree r^2. The first, working with normal forms of the Frobenius operator on the space of roots of f, gives a straightforward classification of the number of possible decompositions, though provides less insight into how many polynomials fall into each class. The second uses more structural information about the ring of additive polynomials and provides complete information on both the number of decompositions and the number of polynomials with each type of decomposition.

A non-squarefree $f = x^{r^2} + ax^r \in \mathbb{F}_q[x;r]$ is a 2-collision if $a \neq 0$ and has a unique decomposition if $a = 0$.

Closely related to decompositions are the following objects. Let r be a power of p, $m \geq 1$, and $\varphi_{r,m} = (r^m - 1)/(r-1)$. Abhyankar (1997) introduced the *projective polynomials*

$$\Psi_m^{(a,b)} = x^{\varphi_{r,m}} + ax + b$$

which have, over appropriate fields, nice Galois groups such as general linear or projective general linear groups. We assume q to be a power of r, and have for $m = 2$

$$\Psi_2^{(a,b)} = x^{r+1} + ax + b \qquad (2.1)$$

with $a, b \in \mathbb{F}_q$. In the case $ab \neq 0$, Bluher (2004b) has proven an amazingly precise result about the number of nonzero roots of (2.1). Namely, this number is $0, 1, 2$, or $r+1$, and she has exactly determined the number of parameters (a,b) for which each of the four possibilities occurs. In the case $a = 0$, the corresponding number is given in von zur Gathen (2008), Lemma 5.9.

Projective polynomials appear naturally in many situations. Bluher (2004a) used them to construct strong Davenport pairs explicitly and Dillon (2002) to build families of difference sets with certain Singer parameters. Bluher (2003) proved the equivalence of two such difference sets, using again projective polynomials and they played a central role in tackling the question of when a quartic power series over $\mathbb{F}_q$ is actually hyperquadratic (Bluher & Lasjaunias, 2006).

Helleseth, Kholosha & Johanssen (2008) used projective polynomials to find m-sequences of length $2^{2k}-1$ and $2^k - 1$. Helleseth & Kholosha (2010) studied projective polynomials further, providing criteria for the number of zeros in a field of characteristic 2, not assuming q to be a power of r. Zeng, Li & Hu (2008) applied the techniques of Bluher (2004b) to study certain p-ary codes.

3. ADDITIVE AND PROJECTIVE POLYNOMIALS

We assume that q is a power of r and r is a power of the characteristic p of $\mathbb{F}_q$. In this section we establish a general connection between decompositions of certain additive polynomials and roots of projective polynomials, and characterize the possible numbers of rational roots of the latter.

Lemma 3.1. *Let $m \geq 1$, $f = x^{r^m} + ax^r + bx$ and $h = x^r - h_0 x$ be in $\mathbb{F}_q[x;r]$ with $a, b, h_0 \in \mathbb{F}_q$. Then $f = g \circ h$ for some $g \in \mathbb{F}_q[x;r]$ if and only if $\Psi_m^{(a,b)}(h_0) = 0$.*

This lemma and Lemma 2.1 are the building blocks for the powerful equivalences summarized as follows.

Proposition 3.2. *Let r be a power of p, $m \geq 1$, $a, b \in \mathbb{F}_q$ and $f = x^{r^m} + ax^r + b$. There is a one-to-one correspondence between any two of the following sets.*

- *right components of f with degree r,*
- *roots of $\Psi_m^{(a,b)}$,*
- *σ_q-invariant linear subspaces of V_f with dimension 1.*

More generally, assume that $f \in \mathbb{F}_q[x;r]$ is any additive polynomial of degree r^m. We now list the possible numbers of right components in $\mathbb{F}_q[x;r]$. A *rational Jordan form* has the shape

$$S = \operatorname{diag}(J_{\alpha_1}^{e_{11}}, \ldots, J_{\alpha_1}^{e_{1k_1}}, \ldots, J_{\alpha_\ell}^{e_{\ell 1}}, \ldots, J_{\alpha_\ell}^{e_{\ell k_\ell}}) \in \mathbb{F}_r^{m\times m},$$

$$\text{where } J_{\alpha_i}^{e_{ij}} = \begin{pmatrix} C_{\alpha_i} & I_{s_i} & & 0 \\ & \ddots & \ddots & \\ & & \ddots & I_{s_i} \\ & & & C_{\alpha_i} \end{pmatrix} \in \mathbb{F}_r^{e_{ij}s_i \times e_{ij}s_i}, \quad (3.1)$$

and $\alpha_1, \ldots, \alpha_\ell \in \overline{\mathbb{F}}_r$ are the distinct non-conjugate roots of the characteristic polynomial of S (i.e., eigenvalues), $C_{\alpha_i} \in \mathsf{F}_r^{s_i \times s_i}$ is the companion matrix of α_i (assuming $[\mathbb{F}_r[\alpha_i] : \mathbb{F}_r] = s_i$) and I_{s_i} is the $s_i \times s_i$ identity matrix.

Let V_f be the $\mathbb{F}_r$-vector space of roots, and $S \in \mathbb{F}_r^{m\times m}$ the matrix representation of the Frobenius operation σ_q on $\overline{\mathbb{F}}_r$. It is well-known (see, e.g. Giesbrecht (1995)) that every matrix in $\mathbb{F}_r^{m\times m}$ is similar to one in rational Jordan form, and the number and multiplicity of eigenvectors is preserved by this transformation. Thus, we may assume S to be of the form described in (3.1). Since we are only interested here in σ_q-invariant subspaces of dimension 1, we ignore for now all α_i which are not in $\mathbb{F}_r$. The number of A-invariant lines — one dimensional subspaces invariant under A — is described as follows.

Theorem 3.3. *If $A \in \mathbb{F}_r^{m\times m}$ has rational Jordan normal form as in (3.1), then the number of A-invariant lines in $\mathbb{F}_r^{m\times 1}$ is*

$$\sum_{\substack{1\leq i\leq \ell \\ \alpha_i \in \mathbb{F}_r}} \varphi_{r,k_i}.$$

For example, in $\mathbb{F}_r^{3\times 3}$ we can list all matrix classes and the number of 1-dimensional invariant subspaces as follows:

$$\underset{r^2+r+1}{\begin{pmatrix}\alpha_1 & & \\ & \alpha_1 & \\ & & \alpha_1\end{pmatrix}}, \quad \underset{r+1}{\begin{pmatrix}\alpha_1 & 1 & \\ & \alpha_1 & \\ & & \alpha_1\end{pmatrix}}, \quad \underset{1}{\begin{pmatrix}\alpha_1 & 1 & \\ & \alpha_1 & 1 \\ & & \alpha_1\end{pmatrix}}, \quad \underset{2}{\begin{pmatrix}\alpha_1 & 1 & \\ & \alpha_1 & \\ & & \alpha_2\end{pmatrix}}$$

$$\underset{r+2}{\begin{pmatrix}\alpha_1 & & \\ & \alpha_1 & \\ & & \alpha_2\end{pmatrix}}, \quad \underset{3}{\begin{pmatrix}\alpha_1 & & \\ & \alpha_2 & \\ & & \alpha_3\end{pmatrix}}, \quad \underset{1}{\begin{pmatrix}\boxed{} & \\ & \alpha_1\end{pmatrix}}, \quad \underset{0}{\begin{pmatrix}\boxed{}\end{pmatrix}},$$

where the number of 1-dimensional invariant subspaces is listed beneath each matrix. Empty boxes indicate companion blocks associated with eigenvalues not in $\mathbb{F}_r$.

For a positive integer m, let Π_m be the set of partitions $\pi = (s_1, \ldots, s_k)$ with positive integers s_i and $s_1 + \cdots + s_k = m$, for any $\pi \in \Pi_m$, let $\varphi_r(\pi) = \varphi_{r,s_1} + \varphi_{r,s_2} + \cdots + \varphi_{r,s_k}$ and $\varphi_r(\Pi_m) = \{\varphi_r(\pi) \colon \pi \in \Pi_m\}$.

Theorem 3.4. *We consider the set*

$$S_{q,r,m} = \{i \in \mathbb{N} \colon \exists f \in \mathbb{F}_q[x;r], \deg f = r^m, \; f \text{ has a maximal } i\text{-collision}\}$$

of maximal collision sizes for additive polynomials. Then

$$S_0 = \{0\},$$
$$S_m = S_{m-1} \cup \varphi_r(\Pi_m).$$

As examples, we have

$$\begin{aligned} &S_0 = \{0\}, \\ &S_1 = S_0 \cup \{\varphi_r(1)\} = \{0, 1\}, \\ &S_2 = S_1 \cup \{\varphi_r(1,1), \varphi_r(2)\} = \{0, 1, 2, r+1\}, \\ &\qquad\text{(consistent with Bluher (2004b))} \\ &S_3 = S_2 \cup \{\varphi_r(3), \varphi_r(2) + 1, 3\}, \\ &S_4 = S_3 \cup \{\varphi_r(4), \varphi_r(3) + 1, 2\varphi_r(2), \varphi_r(2) + 2, 4\}. \end{aligned}$$

The size of S_m equals $\sum_{0\leq k\leq m} p(k)$, where $p(k)$ is the number of additive partitions of k. This grows exponentially in m (Hardy & Ramanujan, 1918) but is still surprisingly small considering the generality of the polynomials involved. By Proposition 3.2, S_m consists of the number of roots of any $\Psi_m^{(a,b)}$, and equivalently the number of σ_q-invariant linear subspaces of V_f of dimension 1 for any $f = x^{r^m} + ax^r + bx$.

We investigate the general result of Theorem 3.4 in the case $m = 2$ further. This leads, for each i, to an exact determination of how often i-collisions occur; consistent with Bluher (2004b). Assume that $f \in \mathbb{F}_q[x; r]$ is squarefree, with root space V_f. Again let σ_q be the Frobenius automorphism fixing $\mathbb{F}_q$, and $S \in \mathbb{F}_r^{2\times 2}$ its representation with respect to some fixed basis. The number of one-dimensional subspaces of V_f invariant under σ_q is equal to the number of nonzero vectors $w \in \mathbb{F}_r^{2\times 1}$ such that $Sw = \lambda w$ for some $\lambda \in \mathbb{F}_r$, that is, the number of eigenvalues of S. Each such w generates a one-dimensional σ_q-invariant subspace, and each such subspace is generated by $r - 1$ such w. Thus, the number of distinct σ_q-invariant subspaces of dimension one, and hence the number of right components in $\mathbb{F}_q[x; r]$ of degree r, is equal to the number of eigenvectors of S in $\mathbb{F}_r^2$, divided by $r - 1$.

We now classify σ_q according to the possible matrix similarity classes of S, as captured by its rational canonical form, and count the number of eigenvectors and components in each case. Note that the number of eigenvectors of S equals the number of eigenvectors of T when S is a similar matrix to T ($S \sim T$).

THEOREM 3.5. *Let $f \in \mathbb{F}_q[x; r]$ be squarefree of degree r^2. Suppose the Frobenius automorphism σ_q is represented by $S \in \mathbb{F}_r^{2\times 2}$, and $\Lambda \in \mathbb{F}_r[z]$ is the minimal polynomial of the matrix S. Then one of the following holds:*

Case 0: $S \sim \left(\begin{smallmatrix} 0 & \delta \\ 1 & \gamma \end{smallmatrix}\right)$, and $\Lambda = z^2 - \gamma z - \delta \in \mathbb{F}_r[z]$ is irreducible, and f is indecomposable.

Case 1: $S \sim \left(\begin{smallmatrix} \gamma & 1 \\ 0 & \gamma \end{smallmatrix}\right) \in \mathbb{F}_r^{2\times 2}$ with $\gamma \neq 0$, and $\Lambda = (z - \gamma)^2$, and f has a unique right component of degree r.

Case 2: $S \sim \left(\begin{smallmatrix} \gamma & 0 \\ 0 & \delta \end{smallmatrix}\right) \in \mathbb{F}_r^{2\times 2}$ for $\gamma \neq \delta$ with $\gamma\delta \neq 0$, when $\Lambda = (z - \gamma)(z - \delta)$, and f has a 2-collision.

Case $r + 1$: $S = \left(\begin{smallmatrix} \gamma & 0 \\ 0 & \gamma \end{smallmatrix}\right) \in \mathbb{F}_r^{2\times 2}$, for $\gamma \neq 0$, and f has an $(r + 1)$-collision.

4. ALGORITHMS FOR ADDITIVE POLYNOMIALS

Given $f \in \mathbb{F}_q[x; r]$ of degree r^2, using the techniques of Section 3, combined with basic algorithms from Giesbrecht (1998), we can quickly determine the number of collisions for f. The centre of $\mathbb{F}_q[x; r]$ will be a useful tool in understanding its structure, and is easily shown to be equal to

$$\mathbb{F}_r[x; q] = \left\{ \sum_{0\leq i\leq\kappa} a_i x^{q^i} : \kappa \in \mathbb{Z}_{\geq 0}, a_0, \ldots, a_\kappa \in \mathbb{F}_r \right\} \subseteq \mathbb{F}_q[x; r]$$

(see, e.g., Giesbrecht (1998)). This is isomorphic to the ring $\mathbb{F}_r[y]$ of polynomials under the usual addition and multiplication, via the isomorphism

$$f = \sum_{0\leq i\leq\kappa} a_i x^{q^i} \;\mapsto\; \tau(f) = \sum_{0\leq i\leq\kappa} a_i y^i$$

(see Lidl & Niederreiter (1983), Section 3.4). $\mathbb{F}_r[y]$ has the important property of being a commutative unique factorization domain. Every element $f \in \mathbb{F}_q[x; r]$ has a unique *minimal central left composition (mclc)* $f^* \in \mathbb{F}_r[x; q]$, the nonzero monic polynomial in $\mathbb{F}_r[x; q]$ of minimal degree such that $f^* = g \circ f$ for some $g \in \mathbb{F}_q[x; r]$. Given $\nu \in \overline{\mathbb{F}}_r$, we say that ν *belongs to* $f \in \mathbb{F}_q[x; r]$ if f is the nonzero polynomial in $\mathbb{F}_q[x; r]$ of lowest degree of which ν is a root.

FACT 4.1 (GIESBRECHT, 1998). *Let p be a prime, r a power of p and $q = r^d$. For $f \in \mathbb{F}_q[x; r]$ of degree r^m, we can find the minimal central left composition $f^* \in \mathbb{F}_r[x; q]$ with $O(d^3m^3)$ operations in $\mathbb{F}_r$.*

The following key theorem shows the close relationship between the minimal central left composition and the minimal polynomial of the Frobenius automorphism.

THEOREM 4.2. *Let $f \in \mathbb{F}_q[x; r]$ be squarefree of degree r^m with roots $V_f \subseteq \overline{\mathbb{F}}_r$. Fix an $\mathbb{F}_r$-basis $\mathcal{B} = \langle \nu_1, \ldots, \nu_m \rangle \in \overline{\mathbb{F}}_r^m$ for V_f, so that $V_f \cong \mathbb{F}_r^{m\times 1}$. Let $S \in \mathbb{F}_r^{m\times m}$ represent the action of the Frobenius automorphism σ_q on V_f with respect to $\mathcal{B}$. Then the image $\tau(f^*) \in \mathbb{F}_r[y]$ of the minimal central left composition $f^* \in \mathbb{F}_r[x; q]$ of f is equal to the minimal polynomial $\Lambda \in F_r[x]$ of the matrix S.*

It is useful to recall a little more about the ring $\mathbb{F}_q[x; r]$. Ore (1933) shows that for any $f, g \in \mathbb{F}_q[x; r]$, there exists a unique monic $h \in \mathbb{F}_q[x; r]$ of maximal degree, and $u, v, \in \mathbb{F}_q[x; r]$, such that $f = u \circ h$ and $g = v \circ h$, called the *greatest common right component (gcrc)* of f and g. Also, $h = \text{gcrc}(f, g) = \gcd(f, h)$, and the roots of h are those in the intersection of the roots of g and h. Furthermore, there exists a unique monic and nonzero $h \in \mathbb{F}_q[x; r]$ of minimal degree, and $u, v \in \mathbb{F}_q[x; r]$, such that $h = u \circ f$ and $h = v \circ g$, called the *least common left composition (lclc)* of f, g. The roots of h are the $\mathbb{F}_r$-vector space sum of the roots of f and g; this sum is direct if $\text{gcrc}(f, g) = 1$. In fact, there is an efficient Euclidean-like algorithm for computing the lclc and gcrc; see, Ore (1933), and Giesbrecht (1998) for an analysis.

We now present our algorithm to count decompositions of polynomials in $\mathbb{F}_q[x; r]$ of degree r^2.

ALGORITHM: `DecompositionCounting`
Input: ▸ $f \in \mathbb{F}_q[x; r]$ of degree r^2, where $q = r^d$
Output: ▸ The number of decompositions of f
(1) If $f'(0) = 0$ Then
(2) If $f = x^{r^2}$ Then Return 1
(3) Else Return 2
(4) Else $f^* \leftarrow \text{mclc}(f) \in \mathbb{F}_r[x; q]$
(5) If $\deg f^* = r$ Then Return $r + 1$
(6) Factor $\tau(f^*) \in \mathbb{F}_r[y]$ over $\mathbb{F}_r[y]$

(7) If $\tau(f^*) \in \mathbb{F}_r[y]$ is irreducible Then Return 0
(8) If $\tau(f^*) = (y-a)^2$ for some $a \in \mathbb{F}_r$ Then Return 1
(9) Return 2

Well-known factorization methods yield the following.

THEOREM 4.3. *The algorithm* `DecompositionCounting` *works as specified and requires an expected number of* $O(d^3)\log r$ *operations in* $\mathbb{F}_r$ *using a randomized algorithm, or* $d^{O(1)}\log r$ *operations with a deterministic algorithm (assuming the ERH).*

The algorithm `DecompositionCounting` also yields the number of rational roots of the projective polynomial $x^{r+1} + ax + b$ (Proposition 3.2).

For the remainder of this section we look at the problem of counting the number of irreducible right components of degree r of any additive polynomial $f \in \mathbb{F}_q[x;r]$ of degree r^m. The algorithm will run in time polynomial in m and $\log q$. This will also yield a fast algorithm to compute the number of rational roots of a projective polynomial $\Psi_m^{(a,b)} \in \mathbb{F}_q[x]$.

The approach is to compute explicitly the Jordan form of the Frobenius operator σ_q acting on the roots of f, as in (3.1). We show how to do this quickly, despite the fact that the actual roots of f may lie in an extension of exponential degree over $\mathbb{F}_q$.

ALGORITHM: `FindJordan`

Input: ▸ $f \in \mathbb{F}_q[x;r]$ monic squarefree of degree r^m, where r is a prime power

Output: ▸ Rational Jordan form $S \in \mathbb{F}_r^{m\times m}$ of the Frobenius automorphism $\sigma_q(a) = a^q$ (for $a \in \overline{\mathbb{F}}_r$) on V_f, as in (3.1)

(1) Compute $f^* \leftarrow \mathrm{mclc}(f) \in \mathbb{F}_r[x;q]$
(2) Factor $\tau(f^*) \leftarrow u_1^{\omega_1} u_2^{\omega_2} \cdots u_\ell^{\omega_\ell} \in \mathbb{F}_r[y]$, where the $u_i \in \mathbb{F}_r[y]$ are monic irreducible and pairwise distinct, and $\deg u_i = s_i$ for $1 \le i \le \ell$
(3) For i from 1 to ℓ do
(4) For j from 1 to ω_i do
(5) $h_{ij} \leftarrow \mathrm{gcrc}(\tau^{-1}(u_i^j), f)$
(6) $\xi_{ij} \leftarrow (\log_r h_{ij})/s_i$ (i.e., $\deg h_{ij} = r^{s_i \xi_{ij}}$)
(7) For j from 1 to $\omega_i - 1$ do
(8) $\delta_{ij} \leftarrow \xi_{ij} - \xi_{i,j+1}$
(9) $\delta_{i\omega_i} \leftarrow \xi_{i\omega_i}$
(10) $k_i \leftarrow \xi_{i1}$
(11) $(e_{i1}, \ldots, e_{ik_i}) \leftarrow (\underbrace{1,\ldots,1}_{\delta_{i1}}, \underbrace{2,\ldots,2}_{\delta_{i2}}, \ldots, \underbrace{\omega_i,\ldots,\omega_i}_{\delta_{i\omega_i}})$
(12) Return $S = \mathrm{diag}\left(J_{\alpha_1}^{e_{11}}, \ldots, J_{\alpha_1}^{e_{1k_1}}, \ldots, J_{\alpha_\ell}^{e_{\ell 1}}, \ldots, J_{\alpha_\ell}^{e_{\ell k_\ell}}\right)$

THEOREM 4.4. *The algorithm* `FindJordan` *works as specified. It requires an expected number of operations in* $\mathbb{F}_q$ *which is polynomial in* m *and* $\log r$ *(Las Vegas).*

Now given an $f \in \mathbb{F}_q[x;r]$ we can quickly compute the rational Jordan form of the Frobenius autormorphism on its root space. Computing the number of degree r factors (or indeed, the number of irreducible factors of any degree) is easy, following the same method as in Section 3.

THEOREM 4.5. *If the Frobenius automorphism of the root space of an* $f \in \mathbb{F}_q[x;r]$ *has rational Jordan form in the notation of Algorithm* `FindJordan` *where*

$$S = \mathrm{diag}\left(J_{\alpha_1}^{e_{11}}, \ldots, J_{\alpha_1}^{e_{1k_1}}, \ldots, J_{\alpha_\ell}^{e_{\ell 1}}, \ldots, J_{\alpha_\ell}^{e_{\ell k_\ell}}\right),$$
$$(e_{i1}, \ldots, e_{ik_i}) \leftarrow (\underbrace{1,\ldots,1}_{\delta_{i1}}, \underbrace{2,\ldots,2}_{\delta_{i2}}, \ldots, \underbrace{\omega_i,\ldots,\omega_i}_{\delta_{i\omega_i}})$$

for $1 \le i \le \ell$, *then the number of indecomposable right components of degree* r *is*

$$\sum_{s_i=1} \sum_{1\le j\le \omega_i} \delta_{ij} \cdot \frac{r^j - 1}{r-1}.$$

Thus, the number of right components of degree r of an additive polynomial of degree r^m can be computed in time polynomial in m and $\log q$, and also the number of roots in $\mathbb{F}_r$ of a projective polynomial (Lemma 3.1).

5. PROJECTIVE POLYNOMIALS AND ROOTS

We now actually construct and enumerate all the polynomials in each case 0, 1, 2, $r+1$ as in Theorem 3.5.

THEOREM 5.1. *Let* r *be a prime power and* q *a power of* r. *For* $i \in \mathbb{N}$ *let*

$$C_{q,r,m,i} = \{(a,b) \in \mathbb{F}_q^2 : x^{r^m} + ax^r + bx \text{ has a maximal } i\text{-collision in } \mathbb{F}_q[x;r]\},$$

$$c_{q,r,m,i} = \# C_{q,r,m,i},$$

and drop q, r, m *from the notation. For* $m = 2$, *the following holds:*

Case 0: C_0 *is the set of all* $f \in \mathbb{F}_q[x;r]$ *of degree* r^2 *whose minimal central left compositions* $f^* \in \mathbb{F}_r[x;q]$ *have degree* q^2 *and cannot be written as* $f^* = g^* \circ h^*$ *for* $g^*, h^* \in \mathbb{F}_r[x;q]$ *of degree* q, *or equivalently that the image* $\tau(f^*) \in \mathbb{F}_r[y]$ *of* f^* *is irreducible of degree 2. We have*

$$c_0 = \frac{r(q^2-1)}{2(r+1)}.$$

Case 1: C_1 *is the set of all* $f \in \mathbb{F}_q[x;r]$ *of degree* r^2 *with minimal central left composition* $f^* = g^* \circ g^*$ *for* $g^* = x^q - cx$ *for* $c \in \mathbb{F}_r^\times$, *and*

$$c_1 = \frac{q^2 - q}{r} + 1.$$

Case 2: C_2 *is the set of all* $f \in \mathbb{F}_q[x;r]$ *with minimal central left composition* $f^* = g^* \circ h^*$ *for* $g^*, h^* \in \mathbb{F}_r[x;q]$ *of degree* q *with* $\gcd(g^*, h^*) = 1$, *and*

$$c_2 = \frac{(q-1)^2 \cdot (r-2)}{2(r-1)} + q - 1.$$

Case $r+1$: C_{r+1} *is the set of all* $f \in \mathbb{F}_q[x;r]$ *of degree* r^2 *with minimal central left composition* $f^* = x^q + cx$, *for* $c \in \mathbb{F}_r^\times$, *and*

$$c_{r+1} = \frac{(q-1)(q-r)}{r(r^2-1)}.$$

Since $c_0 + c_1 + c_2 + c_{r+1} = q^2$, these are the only possible numbers of collisions of a degree r^2 polynomial in $\mathbb{F}_q[x;r]$.

In each case, the number of collisions of an $f \in \mathbb{F}_q[x;r]$ is determined by the factorization of its minimal central left composition f^* in $\mathbb{F}_r[x;q]$. Here $\deg \tau(f^*) \in \{1, 2\}$, and we can enumerate all such f^* in each class (irreducible linear, irreducible quadratic, perfect square, or product of distinct linear factors). We can decompose each such f^* using the algorithms of Giesbrecht (1998) to generate polynomials with a prescribed number of collisions.

We show now how to construct indecomposable additive polynomials of prescribed degree, and count their number. We also show how to construct additive polynomials with a single, unique complete decomposition and count the number of such polynomials.

The following theorem characterizes indecomposable polynomials of degree r^ℓ in terms of their minimal central left compositions. This theorem allows us to get hold of degree r right components from the roots of $\tau(f^*)$ in $\mathbb{F}_q$.

THEOREM 5.2 (GIESBRECHT, 1998, THEOREM 4.3). *Let $f^* \in \mathbb{F}_r[x;q]$ have degree q^ℓ, such that $\tau(f^*) \in \mathbb{F}_r[y]$ is irreducible (of degree ℓ). Then every indecomposable right component $f \in \mathbb{F}_q[x;r]$ of f^* has degree r^ℓ. Conversely, all $f \in \mathbb{F}_q[x;r]$ which are indecomposable of degree r^ℓ are such that $\tau(f^*) \in \mathbb{F}_r[y]$ is irreducible of degree ℓ, where $f^* \in \mathbb{F}_r[x;q]$ is the minimal central left composition of f.*

The following bound has been shown in Odoni (1999). Our methods here provide a simple proof. Let

$$I_r(n) = \sum_{d \mid n} \mu(n/d) r^d$$

be the number of monic irreducible polynomials in $\mathbb{F}_r[y]$ of degree n (see, e.g., Lidl & Niederreiter (1983), Theorem 3.25).

THEOREM 5.3. *Let q be a power of r. The number of monic indecomposable polynomials $f \in \mathbb{F}_q[x;r]$ of degree r^m is*

$$\frac{q^m - 1}{r^m - 1} I_r(m).$$

This implies there are (slightly) more indecomposable additive polynomials of degree r^m in $\mathbb{F}_q[x;r]$ than irreducible polynomials of degree m in $\mathbb{F}_q[y]$.

The above theorem also yields a reduction from the problem of finding indecomposable polynomials in $\mathbb{F}_q[x;r]$ of prescribed degree to that of decomposing polynomials in $\mathbb{F}_q[x;r]$. A fast randomized algorithm for decomposing additive polynomials is shown in Giesbrecht (1998), which requires a number of operations bounded by $(m + \log q)^{O(1)}$. Thus, we can just choose a random polynomial in $\mathbb{F}_q[x;r]$ of prescribed degree and check if it is irreducible, with a high expectation of success. A somewhat slower polynomial-time reduction from decomposing additive polynomials in $\mathbb{F}_q[x;r]$ to factoring in $\mathbb{F}_r[y]$ is also given in Giesbrecht (1998). This suggests the interesting question as to whether one can find indecomposable polynomials in $\mathbb{F}_q[x;r]$ of prescribed degree n in deterministic polynomial-time, assuming the ERH (à la Adleman & Lenstra (1986)).

We finish this section by establishing connections to the counts of Bluher (2004b) and von zur Gathen (2009). Proposition 3.2 yields an equivalent description of $C_{q,r,m,i}$ as

$$C_{q,r,m,i} = \{(a,b) \in \mathbb{F}_q^2 \colon \Psi_m^{(a,b)} \text{ has exactly } i \text{ roots in } \mathbb{F}_q\}.$$

Section 3 says that

$$C_{q,r,m,i} \neq \emptyset \implies i \in S_{q,r,m}$$

and $S_{q,r,m}$ is determined in Theorem 3.4. Furthermore, let

$$C^{(1)}_{q,r,m,i} = \{(a,b) \in C_{q,r,m,i} \colon b \neq 0\},$$
$$C^{(2)}_{q,r,m,i} = \{(a,b) \in C_{q,r,m,i} \colon ab \neq 0\},$$

and $c^{(j)}_{q,r,m,i} = \#C^{(j)}_{q,r,m,i}$ for $j = 1, 2$. Leaving out the indices, we have $C^{(2)} \subseteq C^{(1)} \subseteq C$. The set $C^{(1)}$ occurs naturally in general decompositions (Proposition 6.5 (iii) for $r = p$), and $C^{(2)}$ is the subject of Bluher (2004b). For an integer $m \geq 1$, let

$$\gamma_{q,r,m} = \gcd(\varphi_{r,m}, q - 1).$$

PROPOSITION 5.4. *We fix q, r, m as above and drop them from the notation of $C^{(j)}_{q,r,m,i}$ and $c^{(j)}_{q,r,m,i}$.*

(i) We have $C_i = C_i^{(1)}$ for all $i \notin \{1, \gamma_{m-1} + 1\}$, and

$$C_1 \setminus C_1^{(1)} = \{(a,0) \colon (-a)^{(q-1)/\gamma_{q,r,m-1}} \neq 1\},$$
$$C_{\gamma_{m-1}+1} \setminus C^{(1)}_{\gamma_{m-1}+1} = \{(a,0) \colon (-a)^{(q-1)/\gamma_{q,r,m-1}} = 1\},$$
$$c_1 = c_1^{(1)} + (q-1)(1 - \gamma^{-1}_{q,r,m-1}) + 1,$$
$$c_{\gamma_{m-1}+1} = c^{(1)}_{\gamma_{m-1}+1} + (q-1)\gamma^{-1}_{q,r,m-1}.$$

(ii) We have $C_i^{(1)} = C_i^{(2)}$ for all $i \notin \{0, \gamma_m\}$, and

$$C_0^{(1)} \setminus C_0^{(2)} = \{(0,b) \colon (-b)^{(q-1)/\gamma_{q,r,m}} \neq 1\},$$
$$C_{\gamma_m}^{(1)} \setminus C_{\gamma_m}^{(2)} = \{(0,b) \colon (-b)^{(q-1)/\gamma_{q,r,m}} = 1\},$$
$$c_0^{(1)} = c_0^{(2)} + (q-1)(1 - \gamma^{-1}_{q,r,m})$$
$$c_{\gamma_m}^{(1)} = c_{\gamma_m}^{(2)} + (q-1)\gamma^{-1}_{q,r,m}.$$

We note that Theorem 5.1 is also counting the number of possible solutions to the equations $x^{r+1} + ax + b$, as in Bluher's (2004) work. The comparison with Bluher's work is interesting because she does not consider the case $a = 0$ or $b = 0$ and because her work has multiple cases depending on whether d is even or odd and whether m is even or odd, whereas our counts have no such special cases.

The result in the (relatively straightforward) case $a = 0$ is consistent with the more general Lemma 5.9 of von zur Gathen (2008), where q is not required to be a power of r, but merely of p. As a corollary we obtain the counting result of Bluher (2004b) (at least over $\mathbb{F}_q$, when q is a power of r).

The constructive nature of our proofs allows us to build polynomials prescribed to be in any of these decomposition classes. This follows in the same manner as in the degree r^2 case. We generate elements of $\mathbb{F}_r[x;q]$ with the desired factorization pattern (which determines the number of collisions) and decompose these over $\mathbb{F}_q[x;r]$ using the algorithms of Giesbrecht (1998).

6. GENERAL COMPOSITIONS

The previous sections provide a good understanding of composition collisions for additive polynomials. We now move on to general polynomials of degree r^2, and provide some explicit non-additive collisions.

For any $f = \sum f_i x^i \in \mathbb{F}_q[x]$, we call $\deg_2 f = \deg(f - \mathrm{lc}(f) x^{\deg f})$ the *second-degree* of f, with $\deg_2 f = -\infty$ for monomials and zero.

Theorem 6.1. *Let q and r be powers of p, $\varepsilon \in \{0,1\}$, $u, s \in \mathbb{F}_q^{\times}$, $t \in T = \{t \in \mathbb{F}_q : t^{r+1} - \varepsilon ut + u = 0\}$, ℓ a positive divisor of $r-1$, $m = (r-1)/\ell$, and*

$$f = F(\varepsilon, u, \ell, s) = x(x^{\ell(r+1)} - \varepsilon us^r x^{\ell} + us^{r+1})^m,$$
$$g = G(u, \ell, s, t) = x(x^{\ell} - us^r t^{-1})^m,$$
$$h = H(\ell, s, t) = x(x^{\ell} - st)^m,$$

all in $\mathbb{F}_q[x]$. Then

$$f = g \circ h,$$

and f has a $\#T$-collision.

If a polynomial $f \in \mathbb{F}_q[x]$ is monic original, then so is $f_{(w)} = (x - f(w)) \circ f \circ (x + w)$ for all $w \in \mathbb{F}_q$. Every decomposition of f induces a decomposition of $f_{(w)}$, and all $f_{(w)}$ have the same number of decompositions as $f_{(0)} = f$.

Among all $F(\varepsilon, u, \ell, s)_{(w)}$, the $F(\varepsilon, u, \ell, s)_{(0)}$ is characterized by the vanishing of the coefficient of $x^{r^2 - \ell r - \ell - 1}$.

Proposition 6.2. *Let q and r be powers of p. Let ε, u, ℓ, s, t and ε^*, u^*, ℓ^*, s^*, t^* satisfy the conditions of Theorem 6.1, $w, w^* \in \mathbb{F}_q$, $f = F(\varepsilon, u, \ell, s)_{(w)}$, and $f^* = F(\varepsilon^*, u^*, \ell^*, s^*)_{(w^*)}$. The following holds:*

(i) If $f = f^*$, then $\varepsilon = \varepsilon^*$ and $\ell = \ell^*$.

(ii) If $\varepsilon = 1$ and $\ell < r-1$, then $f = f^*$ if and only if $u = u^*$, $s = s^*$ and $w = w^*$.

(iii) If $\varepsilon = 1$ and $\ell = r-1$, then $f = F(1, u, r-1, s)_{(0)}$ and $f = f^*$ if and only if $u = u^*$ and $s = s^*$.

(iv) If $\varepsilon = 0$ and $\ell < r-1$, then $f = F(0, -1, \ell, st)_{(w)}$ and $f = f^*$ if and only if $w = w^*$ and $(s/s^*)^{r+1} = 1$.

(v) If $\varepsilon = 0$ and $\ell = r-1$, then $f = F(0, -1, r-1, st)_{(0)}$ and $f = f^*$ if and only if $(s/s^*)^{r+1} = 1$.

Corollary 6.3. *Let p, q, r be as in Theorem 6.1, $\gamma = \gcd(r+1, q-1)$, $i \in \{2, r+1\}$, and N_i the number of $F(\varepsilon, u, \ell, s)_{(w)}$ which have a maximal i-collisions as constructed above. Then*

$$N_i = (1 - q + q \cdot d(r-1)) \left(c^{(2)}_{q,r,i} + \delta_{\gamma,i} \frac{q-1}{\gamma} \right),$$

where $d(r-1)$ is the number of divisors of $r-1$, $\delta_{i,j}$ is Kronecker's delta, and $c^{(2)}_{q,r,i}$ are determined by Theorem 5.1 and Proposition 5.4.

Von zur Gathen (2008), Lemma 3.29, determines $\gcd(r+1, q-1)$ explicitly.

Conjecture 6.4. *Any squarefree maximal i-collision with $i \geq 2$ at degree p^2 is of the form $\{(G(u, \ell, s, t)_{(w)}, H(\ell, s, t)_{(w)}) : t \in T\}$.*

In the following, we present partial results on this conjecture, concentrating on the simplest case $r = p$. We also give an upper bound on the number of decompositions a single polynomial can have in the case of degree p^2. No nontrivial estimate seems to be in the literature.

Proposition 6.5. *Let C be a non-Frobenius i-collision over $\mathbb{F}_q$ with $i \geq 2$ at degree p^2. There is an integer k with $1 \leq k < p$ and the following properties for all $(g, h) \in C$.*

(i) $\deg_2(g) = \deg_2(h) = k$.

(ii) For all $(g^*, h^*) \in C$ with $(g, h) \neq (g^*, h^*)$, we have $g_k \neq g_k^*$ and $h_k \neq h_k^*$.

(iii) Set $a = -f_{kp}$ and $b = k^{-1} f_{kp-p+k}$. Then $bh_k \neq 0$, and

$$h_k^{p+1} + ah_k + b = 0$$
$$g_k = -a - h_k^p = bh_k^{-1}.$$

(iv) $i \leq p + 1$.

We have $k = 1$ for additive polynomials, and $k = r - \ell$ in Theorem 6.1.

Proposition 6.6. *Take a non-Frobenius i-collision over $\mathbb{F}_q$ with $i \geq 2$ at degree p^2, and let k be the integer defined in Proposition 6.5. Then $k = 1$ or $k > p/2$. In particular, there are no collisions at degree p^2 with $k = 2$ if $p > 3$ nor with $k = 3$ if $p > 5$.*

7. CONCLUSION AND OPEN QUESTIONS

We have presented composition collisions with component degrees (r, r) for polynomials f of degree r^2, and observed a fascinating interplay between these examples—quite distinct in the additive and the $f_{r^2-r-1} \neq 0$ cases—and Abhyankar's projective polynomials and Bluher's statistics on their roots. Furthermore, we showed that our examples comprise all possibilities in the additive case, and provided large classes of examples in general. Showing the completeness of our examples in the general case is the main challenge left open here as Conjecture 6.4.

Generalizations go in two directions. One is degree r^k for $k \geq 3$. Additive polynomials are of special interest here, and the rational normal form of the Frobenius automorphism will play a major role. For general polynomials, the approximate counting problem is solved in von zur Gathen (2009) with a relative error of about q^{-1}, and it is desirable to reduce this, say to q^{-r+1}. The second direction is to look at degree ar^2 with $r \nmid a$. Now there are no additive polynomials, but for approximate counting, the best known relative error can be as large as 1. It would be interesting to also push this below q^{-1}, or even q^{-r+1}.

In some sections, we assume the field size q to be a power of the parameter r. As in Bluher's (2004) work, our methods go through for the general situation, where q and r are independent powers of the characteristic.

With respect to additive polynomials, a more thorough computational investigation of projective polynomials is warranted. Automatic generation of Bluher-like counting results for higher degree projective polynomials should be possible, as would be a more exact understanding of their possible collision numbers.

8. ACKNOWLEDGMENTS

The authors thank Toni Bluher for telling us about the applications of projective polynomials, and an anonymous referee for pointing us to Helleseth & Kholosha (2010).

The work of Joachim von zur Gathen and Konstantin Ziegler was supported by the B-IT Foundation and the Land Nordrhein-Westfalen. The work of Mark Giesbrecht was supported by NSERC Canada and MITACS.

References

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

LEONARD M. ADLEMAN & HENDRIK W. LENSTRA, JR. Finding Irreducible Polynomials over Finite Fields. In *Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing, Berkeley CA*, pages 350–355. ACM Press, 1986.

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

ANTONIA W. BLUHER. On $x^6 + x + a$ in Characteristic Three. *Designs, Codes and Cryptography*, **30**:85–95, 2003. URL `http://www.springerlink.com/content/r213567443r63360/fulltext.pdf`.

ANTONIA W. BLUHER. Explicit formulas for strong Davenport pairs. *Acta Arithmetica*, **112**(4):397–403, 2004a.

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

ANTONIA W. BLUHER & ALAIN LASJAUNIAS. Hyperquadratic power series of degree four. *Acta Arithmetica*, **124**(3):257–268, 2006.

JOHN J. CADE. A New Public-key Cipher Which Allows Signatures. In *Proceedings of the 2nd SIAM Conference on Applied Linear Algebra*, Raleigh NC A11. SIAM, 1985.

J. F. DILLON. Geometry, codes and difference sets: exceptional connections. In *Codes and designs (Columbus, OH, 2000)*, volume 10 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 73–85. de Gruyter, Berlin, 2002. URL `http://dx.doi.org/10.1515/9783110198119.73`.

F. DOREY & G. WHAPLES. Prime and Composite Polynomials. *Journal of Algebra*, **28**:88–101, 1974. URL `http://dx.doi.org/10.1016/0021-8693(74)90023-4`.

JOACHIM VON ZUR GATHEN. Functional Decomposition of Polynomials: the Tame Case. *Journal of Symbolic Computation*, **9**:281–299, 1990a. URL `http://dx.doi.org/10.1016/S0747-7171(08)80014-4`.

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

JOACHIM VON ZUR GATHEN. Counting decomposable univariate polynomials. *Preprint*, 92 pages, 2008. URL `http://arxiv.org/abs/0901.0054`.

JOACHIM VON ZUR GATHEN. An algorithm for decomposing univariate wild polynomials. *Journal of Symbolic Computation*, to appear, 32 pages, 2010.

JOACHIM VON ZUR GATHEN. The Number of Decomposable Univariate Polynomials. In JOHN P. MAY, editor, *Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation ISSAC2009, Seoul, Korea*, pages 359–366. 2009. ISBN 978-1-60558-609-0.

JOACHIM VON ZUR GATHEN, MARK GIESBRECHT & KONSTANTIN ZIEGLER. Composition collisions and projective polynomials, 2010. URL `http://arxiv.org/abs/1005.1087`.

MARK WILLIAM GIESBRECHT. Complexity Results on the Functional Decomposition of Polynomials. Technical Report 209/88, University of Toronto, Department of Computer Science, Toronto, Ontario, Canada, 1988. Available as `http://arxiv.org/abs/1004.5433`.

MARK GIESBRECHT. Nearly Optimal Algorithms for Canonical Matrix Forms. *SIAM J. Comp.*, **24**:948–969, 1995.

MARK GIESBRECHT. Factoring in Skew-Polynomial Rings over Finite Fields. *Journal of Symbolic Computation*, **26**(4):463–486, 1998. URL `http://dx.doi.org/10.1006/jsco.1998.0224`.

G. H. HARDY & S. RAMANUJAN. Asymptotic formulae in combinatory analysis. *Proceedings of the London Mathematical Society*, **17**(2):75–115, 1918.

TOR HELLESETH & ALEXANDER KHOLOSHA. $x^{2^l+1} + x + a$ and related affine polynomials over $GF(2^k)$. *Cryptography and Communications*, **2**(1):85–109, 2010.

TOR HELLESETH, ALEXANDER KHOLOSHA & AINA JOHANSSEN. m-Sequences of Different Lengths with Four-Valued Cross Correlation. *IEEE International Symposium on Information Theory*, 2008.

DEXTER KOZEN & SUSAN LANDAU. Polynomial Decomposition Algorithms. *Journal of Symbolic Computation*, **7**:445–456, 1989. An earlier version was published as Technical Report 86-773, Department of Computer Science, Cornell University, Ithaca NY, 1986.

S. LANDAU & G. L. MILLER. Solvability by Radicals is in Polynomial Time. *Journal of Computer and System Sciences*, **30**:179–208, 1985.

RUDOLF LIDL & HARALD NIEDERREITER. *Finite Fields*. Number 20 in Encyclopedia of Mathematics and its Applications. Addison-Wesley, Reading MA, 1983.

ROBERT WINSTON KEITH ODONI. On additive polynomials over a finite field. *Proceedings of the Edinburgh Mathematical Society*, **42**:1–16, 1999.

O. ORE. On a Special Class of Polynomials. *Transactions of the American Mathematical Society*, **35**:559–584, 1933.

ANDRZEJ SCHINZEL. *Selected Topics on Polynomials*. Ann Arbor; The University of Michigan Press, 1982. ISBN 0-472-08026-1.

ANDRZEJ SCHINZEL. *Polynomials with special regard to reducibility*. Cambridge University Press, Cambridge, UK, 2000. ISBN 0521662257.

XIANGYONG ZENG, NIAN LI & LEI HU. A class of nonbinary codes and their weight distribution. *ArXiv e-prints, arxiv 0802.3430v1*, 2008. URL `http://arxiv.org/PS_cache/arxiv/pdf/0802/0802.3430v1.pdf`.

RICHARD ZIPPEL. Rational Function Decomposition. In STEPHEN M. WATT, editor, *Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation ISSAC '91, Bonn, Germany*, pages 1–6. ACM Press, Bonn, Germany, 1991. ISBN 0-89791-437-6.