ARTICLE IN PRESS YJSCO:2027

Journal of Symbolic Computation ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Counting invariant subspaces and decompositions of additive polynomials

Joachim von zur Gathen[a], Mark Giesbrecht[b], Konstantin Ziegler[c]

[a] B-IT, Universität Bonn, D-53115 Bonn, Germany
[b] Cheriton School of Computer Science, University of Waterloo, Waterloo, ON, N2L 3G1, Canada
[c] University of Applied Sciences Landshut, D-84036 Landshut, Germany

ARTICLE INFO

Article history:
Received 6 July 2018
Accepted 26 April 2019
Available online xxxx

MSC:
68W30
12Y05

Keywords:
Univariate polynomial decomposition
Additive polynomials
Finite fields
Rational Jordan form

ABSTRACT

The functional (de)composition of polynomials is a topic in pure and computer algebra with many applications. The structure of decompositions of (suitably normalized) polynomials $f = g \circ h$ in $F[x]$ over a field F is well understood in many cases, but less well when the degree of f is divisible by the positive characteristic p of F. This work investigates the decompositions of *r-additive* polynomials, where every exponent and also the field size is a power of r, which itself is a power of p.

The decompositions of an r-additive polynomial f are intimately linked to the Frobenius-invariant subspaces of its root space V in the algebraic closure of F. We present an efficient algorithm to compute the rational Jordan form of the Frobenius automorphism on V. A formula of Fripertinger (2011) then counts the number of Frobenius-invariant subspaces of a given dimension and we derive the number of decompositions with prescribed degrees.

E-mail addresses: gathen@bit.uni-bonn.de (J. von zur Gathen), mwg@uwaterloo.ca (M. Giesbrecht), mail@zieglerk.net (K. Ziegler).

URLs: http://cosec.bit.uni-bonn.de/ (J. von zur Gathen), https://cs.uwaterloo.ca/~mwg (M. Giesbrecht), http://zieglerk.net (K. Ziegler).

https://doi.org/10.1016/j.jsc.2020.06.008
0747-7171/© 2020 Elsevier Ltd. All rights reserved.

1. Introduction

The *composition* of two polynomials $g, h \in F[x]$ over a field F is denoted as $f = g \circ h = g(h)$, and then (g, h) is a *decomposition* of f. If g and h have degree at least 2, then f is *decomposable* and g and h are *left* and *right components* of f, respectively.

Since the foundational work of Ritt, Fatou, and Julia in the 1920s on compositions over $\mathbb{C}$, a substantial body of work has been concerned with structural properties (e.g., Fried and MacRae (1969), Dorey and Whaples (1974), Schinzel (1982, 2000), Zannier (1993)), with algorithmic questions (e.g., Barton and Zippel (1985), Kozen and Landau (1989)), and more recently with enumeration, exact and approximate (e.g., Giesbrecht (1988), Blankertz et al. (2013), von zur Gathen (2014), Ziegler (2015, 2016)). A fundamental dichotomy is between the *tame case*, where the characteristic p of F does not divide $\deg g$, see von zur Gathen (1990a), and the *wild case*, where p divides $\deg g$, see von zur Gathen (1990b).

Zippel (1991) suggests that the block decompositions of Landau and Miller (1985) for determining subfields of algebraic number fields can be applied to decomposing rational functions even in the wild case. Blankertz (2014) proves this formally and shows that this idea can be used to compute all decompositions of a polynomial with an indecomposable right component. Giesbrecht (1998) provides fast algorithms for the decomposition of *additive* (or linearized) polynomials, where all exponents are powers of p. Subsequent improvements in the cost of factorization and basic operations have been made in Caruso and Le Borgne (2017, 2018). All these algorithms use time polynomial in the input degree.

We consider the following counting problem: given $f \in F[x]$ and a divisor d of its degree, how many (g, h) are there with $f = g \circ h$ and $\deg g = d$? Under a suitable normalization, the answer in the tame case is simple: at most one. However, we address this question for additive polynomials, in some sense an "extremely wild" case, and determine both the structure and the number of such decompositions. This involves three steps:

- a bijective correspondence between decompositions of an additive polynomial f and Frobenius-invariant subspaces of its root space V_f in an algebraic closure of F (Section 2),
- a description of the A-invariant subspaces of an F-vector space for a matrix $A \in F^{n\times n}$ in rational Jordan form (Section 3), and
- an efficient algorithm to compute the rational Jordan form of the Frobenius automorphism on V_f (Section 4). Its runtime is polynomial in $\log_p(\deg f)$.

A combinatorial result of Fripertinger (2011) counts the relevant Frobenius-invariant subspaces of V_f and thus our decompositions (Subsection 3.1). We also count the number of maximal chains of Frobenius-invariant subspaces and thus the complete decompositions. Our algorithm deals with squarefree polynomials, and we give a reduction for the general case (Subsection 2.2).

Some of the results in the present paper are described in an Extended Abstract (von zur Gathen et al., 2010). Versions of the present paper are available at https://arxiv.org/abs/1005.1087 and https://arxiv.org/abs/1912.00212. Implementations of all algorithms in `SageMath` are available at https://github.com/zieglerk/polynomial_decomposition.

2. Additive polynomials and vector spaces

Additive (or linearized) polynomials have a rich mathematical structure. Introduced by Ore (1933), they play an important role in the theory of finite and function fields and have found many applications in coding theory and cryptography. See Lidl and Niederreiter (1997, Section 3.4) for an introduction and survey. In this section, we establish connections between components of additive polynomials, subspaces of root spaces, and factors of so-called projective polynomials.

We focus on additive polynomials over finite fields F, though some of these results hold more generally for any field of characteristic $p > 0$. Let r be a power of p and let

Please cite this article in press as: von zur Gathen, J., et al. Counting invariant subspaces and decompositions of additive polynomials. J. Symb. Comput. (2020), https://doi.org/10.1016/j.jsc.2020.06.008

$$\mathsf{F}[x;r] = \left\{ \sum_{0\le i\le n} a_i x^{r^i} : n \in \mathbb{Z}_{\ge 0}, \quad a_0,\ldots,a_n \in \mathsf{F} \right\}$$

be the set of *r-additive* (or *r-linearized*) polynomials over F. For $\mathsf{F} = \mathbb{F}_r$, we fix an algebraic closure $\overline{\mathsf{F}} \supseteq \mathbb{F}_r$. Then these are the polynomials f such that $f(a\alpha + b\beta) = af(\alpha) + bf(\beta)$ for any $a, b \in \mathbb{F}_r$ and $\alpha, \beta \in \overline{\mathsf{F}}$. The r-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; see Ore (1933, Chapter 1, Theorem 1). For $f, h \in \mathsf{F}[x;r]$, we find

$$h \text{ is a factor of } f \iff h \text{ is a right component of } f \tag{2.1}$$

after comparing division with remainder of f by h (in $\mathsf{F}[x]$) and decomposition with remainder of f by h (in $\mathsf{F}[x;r]$). All components of an r-additive polynomial are p-additive, see Dorey and Whaples (1974, Theorem 4) and Giesbrecht (1988, Theorem 3.3).

An additive polynomial is squarefree if its derivative is nonzero, meaning that its linear coefficient a_0 is nonzero. To understand the decomposition behavior of additive polynomials, it is sufficient to restrict ourselves to monic squarefree elements of $\mathsf{F}[x;r]$. The general (monic non-squarefree) case is discussed in Subsection 2.2. For $f \in \mathsf{F}[x;r]$ with $\deg f = r^n$, we call n the *exponent* of f, denote it by $\operatorname{expn} f$, and write for $n \ge 0$

$$\mathsf{F}[x;r]_n = \{f \in \mathsf{F}[x;r] : f \text{ is monic squarefree with exponent } n\}.$$

For $f \in \mathsf{F}[x;r]_n$, the set V_f of all roots of f in an algebraic closure $\overline{\mathsf{F}}$ of F forms an $\mathbb{F}_r$-vector space of dimension n. From now on, we assume q to be a power of r, and let $\mathsf{F} = \mathbb{F}_q$ be a finite field with q elements. Then V_f is invariant under the qth power *Frobenius automorphism* σ_q, since for $\alpha \in \overline{\mathsf{F}}$ with $f(\alpha) = 0$ we have $f(\sigma_q(\alpha)) = f(\alpha^q) = f(\alpha)^q = 0$, thus $\sigma_q(V_f) \subseteq V_f$, and σ_q is injective. For $n \ge 0$, we define

$$L[\sigma_q;\mathbb{F}_r]_n = \left\{ n\text{-dimensional } \sigma_q\text{-invariant } \mathbb{F}_r\text{-linear subspaces of } \overline{\mathbb{F}_q} \right\},$$

$$\psi_n\colon \begin{array}{l} \mathbb{F}_q[x;r]_n \to L[\sigma_q;\mathbb{F}_r]_n, \\ \qquad f \mapsto V_f = \{\alpha \in \overline{\mathsf{F}} \colon f(\alpha) = 0\}. \end{array} \tag{2.2}$$

Conversely, for any n-dimensional $\mathbb{F}_r$-vector space $V \subseteq \overline{\mathsf{F}}$, the lowest degree monic polynomial $f_V = \prod_{\alpha\in V}(x-\alpha) \in \overline{\mathsf{F}}[x]$ with V as its roots is a squarefree r-additive polynomial of exponent n, see Ore (1933, Theorem 8). If V is invariant under σ_q, then $f_V \in \mathbb{F}_q[x;r]_n$. For $n \ge 0$, we define

$$\varphi_n\colon \begin{array}{l} L[\sigma_q;\mathbb{F}_r]_n \to \mathbb{F}_q[x;r]_n, \\ \qquad V \mapsto f_V = \prod_{\alpha\in V}(x-\alpha). \end{array} \tag{2.3}$$

Ore (1933, Chapter 1, §§ 3–4) gives a correspondence between monic squarefree p-additive polynomials and $\mathbb{F}_p$-vector spaces which generalizes as follows.

Proposition 2.4. *For r a power of a prime p, q a power of r, and $n \ge 0$, the maps ψ_n and φ_n are inverse bijections.*

2.1. Right components and invariant subspaces

The following refinement of Proposition 2.4 is a cornerstone of this paper. It provides a bijection between right components of a monic original $f \in \mathbb{F}_q[x;r]_n$ and σ_q-invariant subspaces of its root space $V_f \in L[\sigma_q;\mathbb{F}_r]_n$. The latter are analyzed with methods from linear algebra in Section 3. Those insights are then reflected back to questions about decompositions, providing results that seem hard to obtain directly.

Please cite this article in press as: von zur Gathen, J., et al. Counting invariant subspaces and decompositions of additive polynomials. J. Symb. Comput. (2020), https://doi.org/10.1016/j.jsc.2020.06.008

For $n \geq d \geq 0$, $f \in \mathbb{F}_q[x;r]_n$, and $V \in L[\sigma_q;\mathbb{F}_r]_n$, we define

$$\begin{aligned} H_d(f) = H_{q,r,d}(f) &= \{\text{right components } h \in \mathbb{F}_q[x;r]_d \text{ of } f\} \subseteq \mathbb{F}_q[x;r]_d, \\ L_d(V) = L_{q,r,d}(V) &= \{d\text{-dimensional } \sigma_q\text{-invariant } \mathbb{F}_r\text{-linear subspaces of } V\} \\ &\subseteq L[\sigma_q;\mathbb{F}_r]_d, \end{aligned}$$

where we omit q and r from the notation when they are clear from the context. We also set $H_{q,r,d}(f) = L_{q,r,d}(V) = \varnothing$ for $d < 0$.

Proposition 2.5. *Let $n \geq d \geq 0$, r be a power of a prime p, q a power of r, and $f \in \mathbb{F}_q[x;r]_n$. Then the restrictions of ψ_d and φ_d are inverse bijections between $H_{q,r,d}(f)$ and $L_{q,r,d}(V_f)$.*

Proof. For $h \in H_d(f)$, we have $h \mid f$ by (2.1), and thus $V_h \subseteq V_f$. Since $h \in \mathbb{F}_q[x;r]_d$, we have $\dim V_h = d$ and $V_h \in L_d(V_f)$. Conversely, for $W \in L_d(f)$, we have $W \subseteq V_f$ and f_W is a squarefree divisor of f with $\operatorname{expn} f_W = d$. From (2.1), we have $f_W \in H_d(f)$. Thus, $\psi_d(\varphi_d(L_d(f))) \subseteq L_d(f)$ and $\varphi_d(\psi_d(H_d(f))) \subseteq H_d(f)$. Since both sets are finite and both maps are injective, we have equalities and the claim follows. □

Thus, under the conditions of Proposition 2.5, we have for $h \in \mathbb{F}_q[x;r]_d$

$$h \mid f \iff V_h \subseteq V_f \iff h \in H_d(f), \tag{2.6}$$

as an extension of (2.1).

2.2. General additive polynomials

We generalize Proposition 2.5 from squarefree to all monic additive polynomials. We can write *any* monic $\bar{f} \in \mathsf{F}[x;r]$ as $g \circ x^{r^m}$ with unique $m \geq 0$ and unique monic squarefree $g \in \mathsf{F}[x;r]$. Then

$$\bar{f} = g \circ x^{r^m} = x^{r^m} \circ f \tag{2.7}$$

with unique monic squarefree $f \in \mathsf{F}[x;r]$ and the coefficients of f are the r^mth roots of the coefficients of g, see Giesbrecht (1988, Section 3). Composing an additive polynomial with x^{r^m} from the left leaves the root space invariant and we have

$$V_{\bar{f}} = V_{x^{r^m} \circ f} = V_f.$$

We now relate the right components of $\bar{f}$ to the right components of f.

Proposition 2.8. *Let $m, n \geq 0$, $m + n \geq d \geq 0$, r be a power of a prime p and q a power of r, $0 \leq d \leq m + n$, and $f \in \mathbb{F}_q[x;r]_n$. For monic $\bar{f} = x^{r^m} \circ f \in \mathbb{F}_q[x;r]$ with exponent $m + n$, we have a bijection between any two of the following three sets:*

(i) {monic right components $\bar{h} \in \mathbb{F}_q[x;r]$ of $\bar{f}$ with exponent d},
(ii) the union of all $H_i(f)$ for $d - m \leq i \leq d$, and
(iii) the union of all $L_i(V_f)$ for $d - m \leq i \leq d$.

Proof. We begin with a bijection between (i) and (ii). Following (2.7), we can write every $\bar{h}$ in (i) as $x^{r^{d-i}} \circ h$ with unique i satisfying $d - m \leq i \leq d$ and unique monic squarefree $h \in \mathbb{F}_q[x;r]_i$. Then $V_h \subseteq V_{\bar{f}} = V_f$ and $h \in H_i(f)$ by (2.6). Conversely, let $d - m \leq i \leq d$ and $h \in H_i(f)$. Then $f = g \circ h$ for some $g \in \mathbb{F}_q[x;r]_{n-i}$ and $\bar{f} = x^{r^{m-d+i}} \circ \tilde{g} \circ x^{r^{d-i}} \circ h$, where the coefficients of $\tilde{g}$ are the r^{d-i}th roots of the coefficients of g. Thus $\bar{h} = x^{r^{d-i}} \circ h$ is a monic right component of $\bar{f}$ with exponent d. Together this yields a one-to-one correspondence between (i) and (ii).

Proposition 2.5 provides a bijection between (ii) and (iii). □

We note that for $d > n$, all three sets are empty.

2.3. Projective and subadditive polynomials

As an aside, we exhibit two further sets of polynomials that are in bijective correspondence with $H_d(f)$; this will not be used beyond this subsection, but illustrates the wide range of applications. Let $f = \sum_{0\le i\le n} a_i x^{r^i} \in F[x;r]$ and t be a positive divisor of $r-1$. We have $f = x\cdot(\pi_t(f)\circ x^t)$ for $\pi_t(f) = \sum_{0\le i\le n} a_i x^{(r^i-1)/t}$. Abhyankar (1997) introduced the *projective polynomials*

$$\pi_{r-1}(x^{r^n} + a_1 x^r + a_0 x) = x^{(r^n-1)/(r-1)} + a_1 x + a_0, \tag{2.9}$$

which may have, over function fields of positive characteristic, nice Galois groups such as projective general or projective special linear groups. Projective polynomials appear naturally in coding theory (e.g., Helleseth et al. (2008), Zeng et al. (2008)) and the study of difference sets (e.g., Dillon (2002), Bluher (2003)). They can be used to construct strong Davenport pairs explicitly (Bluher, 2004a) and determine whether a quartic power series is actually hyperquadratic (Bluher and Lasjaunias, 2006). The linear shifts of (2.9) are closely related to group actions on irreducible polynomials over $\mathbb{F}_q$ (Stichtenoth and Topuzoğlu, 2012). The cardinality of the value set of a (possibly non-additive) polynomial $f\in\mathbb{F}_q[x]$ is determined by the maximal s, t such that $f = x^s\cdot(\bar{f}\circ x^t)$ for some $\bar{f}\in\mathbb{F}_q[x]$ (Akbary et al., 2009). Bluher (2004b) shows that (2.9) has exactly 0, 1, 2, or $r+1$ roots in $\mathbb{F}_q$ for q a power of r. Helleseth and Kholosha (2010) count the roots for q and r independent powers of 2.

The polynomial

$$\rho_t(f) = x\cdot(x^t\circ\pi_t(f)) = x\cdot(\pi_t(f))^t$$

is called (r,t)-*subadditive* (or simply *subadditive*). We have $\rho_t(f)\circ x^t = x^t\circ f$ and in particular $\rho_1(f) = f$. Subadditive polynomials were introduced by Cohen (1990) to study their role as permutation polynomials. Henderson and Matthews (1999) connect their decomposition behavior to that of additive polynomials and provide the bijection between (i) and (iii) in the following proposition. Coulter et al. (2004) use this connection to apply Odoni's (1999) counting formula for p-additive polynomials and Giesbrecht's (1998) decomposition algorithm for additive polynomials to subadditive polynomials.

Proposition 2.10. *Let $n\ge d\ge 0$, r be a power of a prime p, q a power of r, t a positive divisor of $r-1$, and $f\in\mathbb{F}_q[x;r]_n$. Then we have bijections between any two of the following three sets.*

(i) $H_d(f)$,
(ii) the set of monic factors of $\pi_t(f)$ that are of the form $\pi_t(h)$ for some $h\in F[x;r]_d$, and
(iii) the set of monic (r,t)-subadditive right components of $\rho_t(f)$ of degree r^d.

In particular, the maps π_t and ρ_t are bijections from (i) to (ii) and to (iii), respectively.

Proof. For the bijection between (i) and (ii), it is sufficient to show that the following statements are equivalent for $h\in\mathbb{F}_q[x;r]_d$:

- h is a right component of f;
- $h = x\cdot(\pi_t(h)\circ x^t)$ is a factor of $f = x\cdot(\pi_t(f)\circ x^t)$;
- $\pi_t(h)$ is a factor of $\pi_t(f)$.

The first two items are equivalent by (2.1), and so are the last two since $\pi_t(h)\pi_t(f)$ is coprime to x for squarefree h and f.

The bijection between (i) and (iii) is due to Henderson and Matthews (1999, Theorem 4.1). □

Please cite this article in press as: von zur Gathen, J., et al. Counting invariant subspaces and decompositions of additive polynomials. J. Symb. Comput. (2020), https://doi.org/10.1016/j.jsc.2020.06.008

Irreducible factors in (ii) correspond to components in (i) and (iii) that are indecomposable over $\mathbb{F}_q[x;r]$ and $\rho_t(\mathbb{F}_q[x;r])$, respectively. For $d=1$ and $t=r-1$, this yields the following criterion by Ore.

Fact 2.11 *(Ore 1933, Theorem 3). For n, r, and F as in Proposition 2.10, $f \in \mathbb{F}_q[x;r]_n$ and $a \in \mathsf{F}^\times$, we have*

$$x^r - ax \in H_1(f) \Longleftrightarrow \pi_{r-1}(f)(a) = 0.$$

3. The rational Jordan form

The usual Jordan (normal) form of a matrix contains the eigenvalues. It is unique up to permutations of the Jordan blocks. The rational Jordan form of a matrix is a generalization, with eigenvalues in a proper extension of the ground field being represented by the companion matrix of their minimal polynomial. Forms akin to the rational Jordan form were investigated already by Frobenius (1911) and the underlying decomposition of the vector space is described by Gantmacher (1959, Chapter VII). A detailed discussion of rational normal forms can be found in Lüneburg (1987, Chapter 6).

Let A be a square matrix with entries in F. We factor the *minimal polynomial* of A over F completely and obtain $\operatorname{minpoly}(A) = u_1^{k_1} \cdots u_t^{k_t} \in \mathsf{F}[y]$ with t pairwise distinct monic irreducible $u_i \in \mathsf{F}[y]$ and $k_i > 0$ for $1 \le i \le t$. We call u_i an *eigenfactor* of A and $\ker(u_i(A))$ its *eigenspace*.

For any $u = \sum_{0\le i\le m} a_i y^i \in \mathsf{F}[y]$ with $a_m = 1$, we have the *companion matrix*

$$C_u = \begin{pmatrix} 0 & & & & -a_0 \\ 1 & \ddots & & & -a_1 \\ 0 & \ddots & \ddots & & \vdots \\ & \ddots & \ddots & 0 & \vdots \\ & & 0 & 1 & -a_{m-1} \end{pmatrix} \in \mathsf{F}^{m\times m}$$

with $\operatorname{minpoly}(C_u) = u$. The *rational Jordan block* of *order* $\ell > 0$ for u is

$$J_u^{(\ell)} = \begin{pmatrix} C_u & I_m & & \\ & C_u & \ddots & \\ & & \ddots & I_m \\ & & & C_u \end{pmatrix} \in \mathsf{F}^{(\ell m)\times(\ell m)},$$

where I_m is the $m \times m$ identity matrix. For linear $u = y - a \in \mathsf{F}[y]$, we have $C_u = (a)$ and the rational Jordan blocks are the Jordan blocks of the usual *Jordan form*. The arrangement of rational Jordan blocks along the main diagonal gives a rational Jordan form.

Definition 3.1. A *rational Jordan matrix* over F is a matrix of the shape

$$A = \operatorname{diag}(J_{u_1}^{(\ell_{11})}, \ldots, J_{u_1}^{(\ell_{1s_1})}, \ldots, J_{u_t}^{(\ell_{t1})}, \ldots, J_{u_t}^{(\ell_{ts_t})}) \tag{3.2}$$

with $t \ge 1$, pairwise distinct monic irreducible $u_1, \ldots, u_t \in \mathsf{F}[y]$, $s_i \ge 1$, and $\ell_{i1} \ge \ell_{i2} \ge \cdots \ge \ell_{is_i}$ for $1 \le i \le t$.

Giesbrecht (1995, Lemma 8.1) shows that $\operatorname{minpoly}(J_u^{(\ell)}) = u^\ell$, and thus $\operatorname{minpoly}(A) = u_1^{\ell_{i1}} \cdots u_t^{\ell_{t1}}$. Every matrix over F is similar to a rational Jordan matrix over F, see, e.g., Giesbrecht (1995, Theorem 8.3), which we call the *rational Jordan form* of the matrix. The eigenvalues and their multiplicities are preserved by this similarity transformation and the rational Jordan form is unique up to permutation of the rational Jordan blocks. Giesbrecht (1995, Corollary 8.6) shows how to transform an $n \times n$ matrix over F into rational Jordan form using $O^\sim(n^\omega + n \log r)$ field operations, where ω is

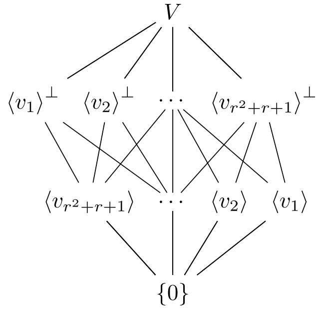
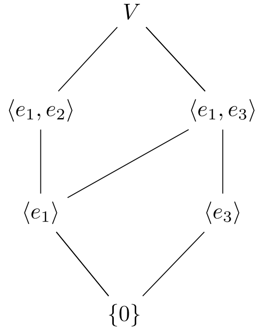
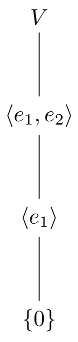
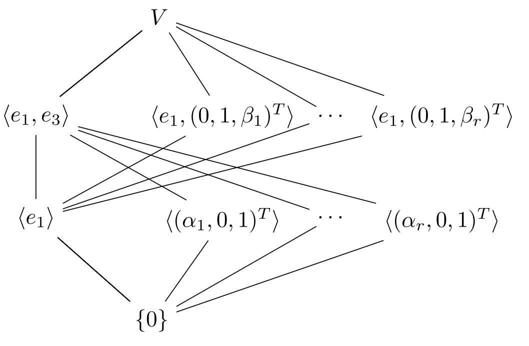
Please cite this article in press as: von zur Gathen, J., et al. Counting invariant subspaces and decompositions of additive polynomials. J. Symb. Comput. (2020), https://doi.org/10.1016/j.jsc.2020.06.008

the exponent of square matrix multiplication over F. This matches the lower bound $\Omega(n^{\omega})$ for this problem up to polylogarithmic factors. The "textbook" method gives $\omega \le 3$ and Le Gall (2014) shows $\omega < 2.3728639$.

We extract the purely combinatorial data from a rational Jordan form $A \in F^{n \times n}$ as in (3.2). For $1 \le i \le t$ and $1 \le j \le \ell_{i1}$, let λ_{ij} denote the number of rational Jordan blocks of order j for the eigenfactor u_i. The formulae for λ_{ij} over the algebraic closure, see, e.g., Gantmacher (1959, p. 155), generalize as

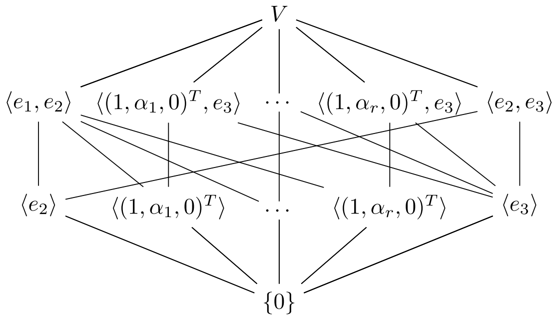
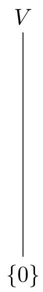
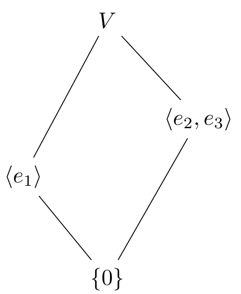
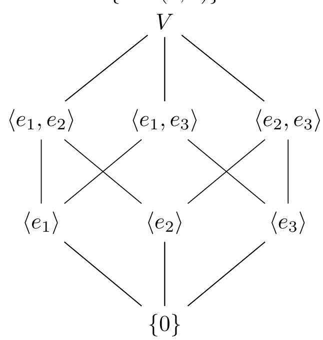
$$\begin{aligned}\lambda_{ij} \cdot \deg u_i &= \mathrm{rk}(u_i^{j-1}(A)) - 2\mathrm{rk}(u_i^{j}(A)) + \mathrm{rk}(u_i^{j+1}(A)) \\ &= 2\mathrm{nul}(u_i^{j}(A)) - \mathrm{nul}(u_i^{j-1}(A)) - \mathrm{nul}(u_i^{j+1}(A)),\end{aligned} \tag{3.3}$$

Table 3.4 All similarity classes of rational Jordan forms $A \in F^{3\times 3}$, where $a, b, c \in F$ are pairwise distinct eigenvalues and the eigenfactors $y^2 - b_1 y - b_0$ and $y^3 - c_2 y^2 - c_1 y - c_0$ are irreducible over F.

A	$\begin{pmatrix} a & & \\ & a & \\ & & a \end{pmatrix}$	$\begin{pmatrix} a & 1 & \\ & a & \\ & & b \end{pmatrix}$
$\lambda(A)$	$\{(1;3)\}$	$\{(1;0,1),(1;1)\}$
$\mathcal{L}(A)$		
$\#L_1(A) = \#L_2(A)$	r^2+r+1	2
$\#\text{chains}(A)$	$(r^2+r+1)(r+1)$	3
A	$\begin{pmatrix} a & 1 & \\ & a & 1 \\ & & a \end{pmatrix}$	$\begin{pmatrix} a & 1 & \\ & a & \\ & & a \end{pmatrix}$
$\lambda(A)$	$\{(1;0,0,1)\}$	$\{(1;1,1)\}$
$\mathcal{L}(A)$		
$\#L_1(A) = \#L_2(A)$	1	$r+1$
$\#\text{chains}(A)$	1	$2r+1$

 YJSCO:2027

Table 3.4 (*continued*)

A	$\begin{pmatrix} a & & \\ & a & \\ & & b \end{pmatrix}$	$\begin{pmatrix} 0 & & c_0 \\ 1 & 0 & c_1 \\ & 1 & c_2 \end{pmatrix}$
$\lambda(A)$	$\{(1;2),(1;1)\}$	$\{(3;1)\}$
$\mathcal{L}(A)$		
$\#L_1(A) = \#L_2(A)$	$r+2$	0
$\#\text{chains}(A)$	$3(r+1)$	1
A	$\begin{pmatrix} a & & \\ & 0 & b_0 \\ & 1 & b_1 \end{pmatrix}$	$\begin{pmatrix} a & & \\ & b & \\ & & c \end{pmatrix}$
$\lambda(A)$	$\{(1;1),(2;1)\}$	$\{3 \times (1;1)\}$
$\mathcal{L}(A)$		
$\#L_1(A) = \#L_2(A)$	1	3
$\#\text{chains}(A)$	2	6

where $u_i^0(A) = I_n$ and $\text{nul}B = n - \text{rk}B$ is the *nullity* of B for any $B \in \mathsf{F}^{n\times n}$. The vector $\lambda(u_i) = (\deg u_i; \lambda_{i1}, \lambda_{i2}, \ldots, \lambda_{i\ell_{i1}})$ of positive integers is the *species* of u_i (in A). This abstracts away the arrangement of the rational Jordan blocks as well as the actual factors u_i. The multiset of all the species of eigenfactors in A is then called the *species* $\lambda(A)$ *of* A. This notion was introduced by Kung (1981) over the algebraic closure and generalized to finite fields by Fripertinger (2011).

Table 3.4 gives all similarity classes of rational Jordan forms A in $\mathsf{F}^{3\times 3}$ and their species. The notation $3 \times (1;1)$ indicates that the species $(1;1)$ occurs three times in the multiset. We also list, for every species, the lattice $\mathcal{L}(A)$ of A-invariant subspaces in a 3-dimensional F-vector space, the number $\#L_1(A)$ of 1-dimensional A-invariant subspaces, and the number $\#\text{chains}(A)$ of maximal A-invariant subspace chains (3.6).

In the next subsection, we derive the latter from the species. In Section 4, we show how to compute the rational Jordan form of the Frobenius automorphism on the root space of an additive polynomial *without* the (costly) computation of a basis.

Please cite this article in press as: von zur Gathen, J., et al. Counting invariant subspaces and decompositions of additive polynomials. J. Symb. Comput. (2020), https://doi.org/10.1016/j.jsc.2020.06.008

3.1. The number of invariant subspaces

Let r be a power of the prime p and $A \in \mathbb{F}_r^{n\times n}$ be a rational Jordan matrix as in (3.2) with $\operatorname{minpoly}(A) = u_1^{k_1} \cdots u_t^{k_t}$, where $u_1, \dots, u_t \in \mathbb{F}_r[y]$ are pairwise distinct monic irreducible, and $k_i > 0$ for $1 \le i \le t$. A operates on every n-dimensional $\mathbb{F}_r$-vector space V and we have the corresponding *primary vector space decomposition*

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_t, \tag{3.5}$$

where $V_i = \ker(u_i^{k_i}(A))$ is the *generalized eigenspace* of u_i for $1 \le i \le t$.

We ask two counting questions, motivated by the connection to decomposition.

(i) What is the number $\#L_d(A)$ of d-dimensional A-invariant subspaces of V for a given d?
(ii) What is the number $\#\text{chains}(A)$ of maximal chains

$$\{0\} = U_0 \subsetneq U_1 \subsetneq \cdots \subsetneq U_e = V \tag{3.6}$$

of A-invariant subspaces U_j for $0 \le j \le e$, where e is the Krull dimension of V?

The A-invariant subspaces of V constitute the complete lattice $\mathcal{L}(A)$ with minimum $\{0\}$ and maximum V. In this lattice's Hasse diagrams, question (i) asks for the number of nodes of a given dimension and question (ii) asks for the number of paths from the minimum to the maximum.

First, we discuss question (i). Let $\mathsf{g}(A) = \sum_{0\le d\le n} \mathsf{g}_d z^d \in \mathbb{Z}_{\ge 0}[z]$ be the *generating function* for the number $\mathsf{g}_d = \#L_d(A)$ of d-dimensional A-invariant subspaces of V. The A-invariant subspace lattice $\mathcal{L}(A)$ is self-dual, see Brickman and Fillmore (1967, Theorem 3), and thus the generating function is symmetric with $\mathsf{g}_d = \mathsf{g}_{n-d}$ for all $0 \le d \le n$.

Let A_i denote the restriction of A to V_i as in (3.5), and $\mathcal{L}(A_i)$ and $\mathsf{g}(A_i)$ be the lattice and generating function of the A_i-invariant subspaces of V_i, respectively. Brickman and Fillmore (1967, Theorem 1) show that

$$\mathcal{L}(A) = \prod_{1\le i\le t} \mathcal{L}(A_i) \text{ and thus } \mathsf{g}(A) = \prod_{1\le i\le t} \mathsf{g}(A_i). \tag{3.7}$$

Thus it suffices to study *A-primary vector spaces*, where $\operatorname{minpoly}(A) = u^k$ is the kth power of an irreducible polynomial u of some degree m. If an n-dimensional A-primary vector space has species $\lambda(A) = \{(m, \lambda_1, \lambda_2, \dots, \lambda_k)\}$, then there is a rational Jordan form $B \in \mathbb{F}_r^{n/m\times n/m}$ with species $\lambda(B) = \{(1, \lambda_1, \lambda_2, \dots, \lambda_k)\}$ and

$$\mathcal{L}(A) \cong \mathcal{L}(B) \text{ and } \mathsf{g}(A) = \mathsf{g}(B) \circ z^m. \tag{3.8}$$

It is therefore enough to study A-primary vector spaces, where $\operatorname{minpoly}(A)$ is the power of a linear polynomial. In this situation, we now compute $\mathsf{g}_1(A)$.

From the theory of q-series, we use the *q-bracket* (also *q-number*)

$$[n]_q = \frac{q^n - 1}{q - 1}$$

of an integer n.

Lemma 3.9. *Let $A \in \mathbb{F}_r^{n\times n}$ be a rational Jordan form as in (3.2) with $\operatorname{minpoly}(A) = u^k$ for some linear $u \in \mathbb{F}_r[y]$, $k > 0$, and species $\lambda(A) = \{(1; \lambda_1, \lambda_2, \dots, \lambda_k)\}$. Then the number of A-invariant lines in an n-dimensional $\mathbb{F}_r$-vector space V is*

$$\mathsf{g}_1(A) = [s]_r, \tag{3.10}$$

where $s = \sum_{1\le j\le k} \lambda_j$.

Proof. For $v \in V \setminus \{0\}$, the following are equivalent for the line $\langle v \rangle$:

- $\langle v \rangle$ is A-invariant.
- $\langle v \rangle$ is in the eigenspace of the linear eigenfactor u (a factor of A's minimal polynomial).

For a linear eigenfactor u, the eigenspace has dimension $\dim(\ker(u(A))) = \sum_{1 \le j \le k} \lambda_j = s$ and thus contains $(r^s - 1)/(r-1)$ lines. □

With $\mathsf{g}_0 = 1$, (3.7), and (3.8), we now compute g_1 for a rational Jordan form A with arbitrary minimal polynomial.

Proposition 3.11. *Let $A \in \mathbb{F}_r^{n \times n}$ be in rational Jordan form as in (3.2) with species $\lambda(A) = \{(\deg u_i; \lambda_{i1}, \lambda_{i2}, \ldots, \lambda_{i\ell_{i1}}) \colon 1 \le i \le t\}$. Then the number of A-invariant lines in $\mathbb{F}_r^n$ is*

$$\mathsf{g}_1(A) = \sum_{\substack{1 \le i \le t \\ \deg u_i = 1}} [s_i]_r, \tag{3.12}$$

where $s_i = \sum_{1 \le j \le \ell_{i1}} \lambda_{ij}$ for $1 \le i \le t$.

This answers question (i) for $d = 1$. For $d > 1$, the number g_d of d-dimensional A-invariant subspaces can be derived from the species with the formulas of Fripertinger (2011). We make them available through the `SageMath`-package accompanying this paper.

For perspective, formula (3.12) allows us to determine exactly the possible values for the number of right components of an additive polynomial that have exponent 1. By Fact 2.11, this is equivalent to finding the possible number of roots of certain projective polynomials. Let

$$M_{q,r,n,1} = \{\#H_1(f) \colon f \in \mathbb{F}_q[x; r]_n\} \tag{3.13}$$

be the set of possible numbers of right components of exponent 1 for monic squarefree r-additive polynomials of exponent n over $\mathbb{F}_q$.

For a positive integer m, let Π_m be the set of unordered partitions (multisets) $\pi = \{\pi_1, \ldots, \pi_k\}$ of m with positive integers π_i and $\pi_1 + \cdots + \pi_k = m$. For any partition $\pi \in \Pi_m$, we define the r-bracket $[\pi]_r = [\pi_1]_r + [\pi_2]_r + \cdots + [\pi_k]_r$. Then (3.12) yields the following theorem.

Theorem 3.14. *Let $M_n = M_{q,r,n,1}$ be as in (3.13) and define*

$$\begin{aligned} \widehat{M}_0 &= \{0\}, \\ \widehat{M}_i &= \widehat{M}_{i-1} \cup \{[\pi]_r \colon \pi \in \Pi_m\} \end{aligned}$$

for $1 \le i \le n$. Then $M_n \subseteq \widehat{M}_n$.

Generally, $M_n = \widehat{M}_{q,r,n,1}$ for all but a few triples (q, r, n), especially over small fields $\mathbb{F}_q$ where not all possible (similarity classes of) Jordan forms may occur. As an example, for $q = r = n = 2$, we have merely two monic squarefree polynomials under consideration. That is simply not enough to cover all four cases in $\hat{M}_2$. A list of the first seven values follows.

$$\begin{aligned} \widehat{M}_0 &= \{0\}, \\ \widehat{M}_1 &= \widehat{M}_0 \cup \{[1]_r\} = \{0, 1\}, \\ \widehat{M}_2 &= \widehat{M}_1 \cup \{2[1]_r, [2]_r\} = \{0, 1, 2, r+1\}, \ \text{(consistent with Bluher (2004b))} \\ \widehat{M}_3 &= \widehat{M}_2 \cup \{3, [2]_r + 1, [3]_r\} \\ &= \{0, 1, 2, 3, r+1, r+2, r^2+r+1\}, \end{aligned}$$

$$\begin{aligned}
\widehat{M}_4 &= \widehat{M}_3 \cup \{4, [2]_r + 2, 2[2]_r, [3]_r + 1, [4]_r\} \\
&= \{0, 1, 2, 3, 4, r+1, r+2, r+3, 2r+2, r^2+r+1, r^2+r+2, \\
&\qquad r^3+r^2+r+1\}, \\
\widehat{M}_5 &= \widehat{M}_4 \cup \{5, [2]_r + 3, 2[2]_r + 1, [3]_r + 2, [3]_r + [2]_r, [4]_r + 1, [5]_r\} \\
&= \{0, 1, 2, 3, 4, 5, r+1, r+2, r+3, r+4, 2r+2, 2r+3, \\
&\qquad r^2+r+1, r^2+r+2, r^2+r+3, r^2+2r+2, \\
&\qquad r^3+r^2+r+1, r^3+r^2+r+2, r^4+r^3+r^2+r+1\}, \\
\widehat{M}_6 &= \widehat{M}_5 \cup \{6, [2]_r + 4, 2[2]_r + 2, 3[2]_r, [3]_r + 3, [3]_r + [2]_r + 1, 2[3]_r, \\
&\qquad\quad [4]_r + 2, [4]_r + [2]_r, [5]_r + 1, [6]_r\} \\
&= \{0, 1, 2, 3, 4, 5, 6, r+1, r+2, r+3, r+4, r+5, 2r+2, 2r+3, 2r+4, 3r+3, \\
&\qquad r^2+r+1, r^2+r+2, r^2+r+3, r^2+r+4, r^2+2r+2, r^2+2r+3, \\
&\qquad 2r^2+2r+2, r^3+r^2+r+1, r^3+r^2+r+2, r^3+r^2+r+3, \\
&\qquad r^3+r^2+2r+2, r^4+r^3+r^2+r+1, r^4+r^3+r^2+r+2, \\
&\qquad r^5+r^4+r^3+r^2+r+1\}.
\end{aligned}$$

The size of $\widehat{M}_n$ equals $\sum_{0 \le k \le n} p(k)$, where $p(k)$ is the number of additive partitions of k. For $n \to \infty$, $p(n)$ grows exponentially as $\exp(\pi\sqrt{2n/3})/(4n\sqrt{3})$ (Hardy and Ramanujan, 1918), but is still surprisingly small considering the generality of the polynomials involved.

Concerning question (ii), we recall that all maximal chains (3.6) have equal length by the Krull-Schmidt Theorem. Let $A \in \mathbb{F}_r^{n \times n}$ be in rational Jordan form on V and let #chains(A) denote the number of all maximal A-invariant chains (3.6). If the lattice is a grid, these are the binomial coefficients.

The number of A-invariant chains depends only on the species $\lambda(A)$ and we write #chains$(\lambda(A)) =$ #chains(A). For every minimal nonzero A-invariant subspace U, there is a canonical bijection – given by $/U$ and $\oplus U$ – between the chains for V that start with $U_1 = U$ and chains for V/U. Thus, we have the recursion formula

$$\#\text{chains}(\lambda(A)) = \sum_{\substack{\text{minimal, nonzero} \\ A\text{-invariant } U \subseteq V}} \#\text{chains}(\lambda(A|_{V/U})), \tag{3.15}$$

where $A|_{V/U}$ is A taken as a linear transformation on the quotient vector space V/U, of dimension $n - \dim(U)$.

We now have two tasks.

- Find all minimal nonzero A-invariant $U \subset V$.
- Derive $\lambda(A|_{V/U})$ for each such U.

Every minimal nonzero A-invariant subspace $U \subseteq V$ is contained in the eigenspace $V_i = \ker(u_i^{k_i}(A))$ for a unique $i \le t$ and we can partition the formula (3.15) in the light of the vector space decomposition (3.5) as

$$\#\text{chains}(\lambda(A)) = \sum_{\text{eigenfactors } u_i} \; \sum_{\substack{\text{minimal, nonzero} \\ A\text{-invariant } U \subseteq V_i}} \#\text{chains}(\lambda(A|_{V/U})). \tag{3.16}$$

As for question (i) above, we make two simplifications. First, it is sufficient to study A where minpoly$(A) = u_1^{k_1} \cdots u_t^{k_t}$ is the product of linear u_i by (3.7) and (3.8). Second, we will deal only with primary vector spaces, i.e. a single eigenfactor u_i, and thus only the inner sum in (3.16).

Please cite this article in press as: von zur Gathen, J., et al. Counting invariant subspaces and decompositions of additive polynomials. J. Symb. Comput. (2020), https://doi.org/10.1016/j.jsc.2020.06.008

Example 3.17. We have the following base case. If $A = (J_u^{(\ell)})$ consists only of a single Jordan block, i.e. $\lambda = \{(1; 0, \dots, 0, \lambda_\ell = 1)\}$, we have a unique maximal chain of A-invariant subspaces

$$0 \subsetneq \langle e_1 \rangle \subsetneq \langle e_1, e_2 \rangle \subsetneq \cdots \subsetneq V$$

and #chains$(A) = 1$. For completeness, we note that $U = \langle e_1 \rangle$ is the unique minimal nonzero A-invariant subspace, $A|_{V/U} = (J_u^{(\ell-1)})$, and $\lambda(A|_{V/U}) = \{(1; 0, \dots, 0, \lambda_{\ell-1} = 1)\}$.

For $\lambda(A) = \{(1; \lambda_1, \dots, \lambda_k)\}$, we already know that the number of minimal nonzero A-invariant subspaces is $[\sum_{1 \le i \le k} \lambda_i]_r$ from (3.8) and (3.10). We need to scrutinize them further. For

$$A = \operatorname{diag}(J_u^{(\ell_1)}, J_u^{(\ell_2)}, \dots, J_u^{(\ell_s)})$$

with $u = y - a$, $\ell_1 \ge \cdots \ge \ell_s$, minpoly$(A) = u^{\ell_1}$, $s = \sum \lambda_j$, and $\lambda_{j'} = \#\{\ell_j = j' : 1 \le j \le s\}$, we re-index the basis of V as

$$e_{11}, \dots, e_{1\ell_1}, e_{21}, \dots, e_{2\ell_2}, \dots, e_{s1}, \dots, e_{s\ell_s}. \tag{3.18}$$

The d-dimensional eigenspace is $\ker u(A) = \langle e_{11}, e_{21}, \dots, e_{s1} \rangle$ and contains $[s]_r$ lines, that is, 1-dimensional subspaces, and these are the only minimal non-zero subspaces.

Let U be an A-invariant subspace. We define its *support* supp(U) (in the basis (3.18)) as the set of all base vectors for which $e_{ij} \cdot U \ne 0$. For a minimal, that is, 1-dimensional, U, we have $j = 1$ for all e_{ij} in its support, since these are the base vectors that span the eigenspace.

The support links the subspace U to the Jordan blocks that act non-trivially on U. Of particular interest are the Jordan blocks of minimal size that act non-trivially on U. We define

$$\operatorname{depth}(U) = \min\{\ell_j : e_{j1} \in \operatorname{supp}(U)\}.$$

Note that there may be several Jordan blocks of size depth(U) acting on the support of U.

Example 3.19. For $A = \begin{pmatrix} a & 1 & \\ & a & \\ & & a \end{pmatrix}$, we have $\langle e_1 \rangle$ of depth 2 and $\langle e_1 + \alpha e_3 \rangle$ for $\alpha \in \mathbb{F}_r$ of depth 1. And these are all $r + 1$ nonzero minimal A-invariant subspaces.

To make (3.15) applicable, we now determine the number of minimal nonzero A-invariant subspaces of depth j for $1 \le j \le k$. Let $\lambda = (1; \lambda_1, \dots, \lambda_k)$ be the species of the eigenvalue under consideration. The possible values for the depth of a nonzero minimal A-invariant subspace range from 1 to k, where $k = \max \ell_j$ and the following counting formula follows easily by inclusion-exclusion.

Proposition 3.20. *Let A be primary on V, with species $\lambda(A) = \{(1; \lambda_1, \dots, \lambda_k)\}$.*

(i) The number of A-invariant subspaces with depth i is

$$\#\operatorname{depth}(\lambda, i) = r^{\lambda_{i+1} + \cdots + \lambda_k} [\lambda_i]_r.$$

(ii) Let U be an A-invariant subspace with depth i. Then A is well-defined on V/U and has species

$$\lambda(A|_{V/U}) = \lambda_{\hat{i}} = \begin{cases} (1; \lambda_1 - 1, \lambda_2, \dots, \lambda_k) & \text{if } i = 1, \\ (1; \lambda_1, \dots, \lambda_{i-1} + 1, \lambda_i - 1, \dots, \lambda_k) & \text{otherwise}. \end{cases}$$

(iii) The number of maximal A-invariant chains is given by the recursion

$$\#\operatorname{chains}(\{(1; 1)\}) = 1,$$
$$\#\operatorname{chains}(\lambda(A)) = \sum_{1 \le j \le k} \#\operatorname{depth}(\lambda, j) \cdot \#\operatorname{chains}(\lambda_{\hat{j}}).$$

Proof. (i) For $i = k$, we have $[\lambda_k]_r$ eigenspaces of depth k. For $i < k$, we have $[\lambda_i + \lambda_{i+1} + \cdots + \lambda_k]_r$ eigenspaces of depth at least i and we find by direct computation

$$\begin{aligned}\#\mathrm{depth}(\lambda, i) &= [\lambda_i + \lambda_{i+1} + \cdots + \lambda_k]_r - [\lambda_{i+1} + \cdots + \lambda_k]_r \\ &= \frac{r^{\lambda_i+\lambda_{i+1}+\cdots+\lambda_k} - 1}{r-1} - \frac{r^{\lambda_{i+1}+\cdots+\lambda_k} - 1}{r-1} \\ &= r^{\lambda_{i+1}+\cdots+\lambda_k} \cdot [\lambda_i]_r,\end{aligned}$$

as claimed.

(ii) We dealt with the base case in Example 3.17.

Without loss of generality, we assume that e_{11} is in the support of U and that the corresponding first Jordan block has size equal to the depth of U. We have

$$U = \langle e_{11} + \alpha_2 e_{21} + \cdots + \alpha_s e_{s1} \rangle$$

for some $\alpha_j \in \mathbb{F}_r$ and $\alpha_j \neq 0$ only if the corresponding Jordan block is larger than the first one. We turn (3.18) into the following basis for V/U:

$$\begin{gathered} e_{12} + \alpha_2 e_{22} + \cdots + \alpha_s e_{s2} + U, \\ e_{13} + \alpha_2 e_{23} + \cdots + \alpha_s e_{s3} + U, \\ \vdots \\ e_{1\ell_1} + \alpha_2 e_{2\ell_1} + \cdots + \alpha_s e_{s\ell_1} + U, \\ e_{21} + U, \ldots, e_{2\ell_2} + U, \\ \vdots \\ e_{s1} + U, \ldots, e_{s\ell_s} + U. \end{gathered}$$

In other words, we drop the projection of the first base vector (due to the linear dependence introduced by U) and modify the base vectors for the first Jordan block. A direct computation shows that $A|_{V/U}$ is in rational Jordan form, its first Jordan block is equal to the first Jordan block of A reduced by size 1, and all other Jordan blocks “remained” unchanged.

(iii) This follows from (3.16) using (i) and (iii). □

In the general case of several eigenfactors we obtain $\#\mathrm{chains}(A)$ by (3.16) using the formulae in Proposition 3.20 (iii) for each eigenfactor.

4. The Frobenius automorphism on the root space

In this section, we present an efficient algorithm to compute the rational Jordan form of the Frobenius automorphism on the root space of a squarefree monic additive polynomial f. With the results of Subsection 3.1, this yields the number of right components of f of a given degree. The straightforward approach suffers from possibly exponential costs for the description of the root space V_f, see Example 4.12.

The *centre* of the Ore ring $\mathbb{F}_q[x; r]$ will be a useful tool. For q a power of r, so that $\mathbb{F}_r \subseteq \mathbb{F}_q$, it equals

$$\mathbb{F}_r[x; q] = \Big\{ \sum_{0 \le i \le n} a_i x^{q^i} : n \in \mathbb{Z}_{\ge 0}, \quad a_0, \ldots, a_n \in \mathbb{F}_r \Big\} \subseteq \mathbb{F}_q[x; r],$$

see, e.g., Giesbrecht (1998, Section 3). Every element $f \in \mathbb{F}_q[x; r]$ has a unique *minimal central left component* $f^* \in \mathbb{F}_r[x; q]$, the unique monic polynomial in $\mathbb{F}_r[x; q]$ of minimal degree such that $f^* =$

$g \circ f$ for some nonzero $g \in \mathbb{F}_q[x;r]$. For squarefree f, it is the monic generator of the largest two-sided ideal $I(f)$ contained in the left ideal generated by f. The ideal $I(f)$ is then known as the *bound* of f, see Jacobson (1943, page 83).

Fact 4.1 *(Giesbrecht 1998, Lemma 4.2). Let r be a power of a prime p and $q = r^d$. For $f \in \mathbb{F}_q[x;r]$ of exponent n, we can find its minimal central left component $f^* \in \mathbb{F}_r[x;q]$ with $O(n^3 d\mathsf{M}(d) + n^2 d^2 \mathsf{M}(d) \log d) \subseteq O^{\sim}(n^3 d^2 + n^2 d^3)$ operations in $\mathbb{F}_r$, where $\mathsf{M}(d)$ is the number of operations to multiply two polynomials over $\mathbb{F}_r$ with degree at most d each.*

The "schoolbook" method gives $\mathsf{M}(d) = O(d^2)$ and Harvey and van der Hoeven (2019a) show $\mathsf{M}(d) = O(d \log d\, 4^{\log^* d})$. The recent, as yet unpublished, preprint of Harvey and van der Hoeven (2019b) claims $\mathsf{M}(d) = O(d \log d)$, which many consider to be the best achievable asymptotic bound.

Le Borgne (2012, Theorem II.3.2) gives an algorithm for f^* with $O^{\sim}(n^\omega d^\omega + n^2 d^2 \log r)$ operations in $\mathbb{F}_r$, where d and n are as above and ω is an exponent of square matrix multiplication over $\mathbb{F}_r$.

The centre $\mathbb{F}_r[x;q]$ is a commutative subring of $\mathbb{F}_q[x;r]$ and isomorphic to $\mathbb{F}_r[y]$ with the usual addition and multiplication via

$$\tau: \begin{array}{c} \mathbb{F}_r[x;q] \to \mathbb{F}_r[y], \\ f = \sum_{0 \le i \le n} a_i x^{q^i} \mapsto \tau(f) = \sum_{0 \le i \le n} a_i y^i, \end{array}$$

see McDonald (1974, pages 24–25). The isomorphic image $\mathbb{F}_r[y]$ is a unique factorization domain and factorizations in $\mathbb{F}_r[y]$ are in one-to-one correspondence with decompositions in $\mathbb{F}_r[x;q]$ into central components. The following main theorem shows the close relationship between the minimal central left component of an additive polynomial and the minimal polynomial of the Frobenius automorphism on its root space.

Theorem 4.2. *Let r be a power of a prime p and q a power of r. Let $f \in \mathbb{F}_q[x;r]_n$ be monic squarefree of exponent n with root space $V_f \subseteq \overline{\mathbb{F}_q}$ and minimal central left component $f^* \in \mathbb{F}_r[x;q]$. Then the image $\tau(f^*) \in \mathbb{F}_r[y]$ is the minimal polynomial of the qth power Frobenius automorphism σ_q on the $\mathbb{F}_r$-vector space V_f.*

Proof. For a central $g = \sum_{0 \le i \le m} g_i x^{q^i} \in \mathbb{F}_r[x;q]$, we have $\tau(g) = \sum_{0 \le i \le m} g_i y^i \in \mathbb{F}_r[y]$ and $(\tau(g)) \times (\sigma_q) = g$, and the following are equivalent:

- g is a right or left component of f;
- $g(\alpha) = 0$ for all $\alpha \in V_f$;
- $(\tau(g)(\sigma_q))(\alpha) = 0$ for all $\alpha \in V_f$.

The first two items are equivalent by (2.1) and the squarefreeness of f and since g is central. The last two items are equivalent since $\tau(g)(\sigma_q) = g$.

Thus, g is a central left component of f if and only if $\tau(g)$ annihilates σ_q on V_f. Since f^* and the minimal polynomial of σ_q are the unique monic polynomials of minimal degree with these properties, respectively, we have the claimed equality. □

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, called the *greatest common right component* (gcrc) of f and g, such that $f = u \circ h$ and $g = v \circ h$ for some $u, v \in \mathbb{F}_q[x;r]$. Also, $h = \mathrm{gcrc}(f,g) = \gcd(f,g)$, and the roots of h are those in the intersection of the roots of f and g, in other words $V_{\mathrm{gcrc}(f,g)} = V_f \cap V_g$. In fact, there is an efficient Euclidean-like algorithm for computing the gcrc; see Ore (1933) and Giesbrecht (1998) for an analysis. The usual Euclidean algorithm for $\gcd(f,g)$ is insufficient, since the degrees of f and g may be exponential in their exponents.

Fact 4.3 *(Giesbrecht 1998, Lemma 2.1). Let r be a power of a prime p and* $q = r^d$*. For* $f, g \in \mathbb{F}_q[x; r]$ *of exponent n, we can find* $\mathrm{gcrc}(f, g) \in \mathbb{F}_q[x; r]$ *with* $O(n^2 \mathsf{M}(d) d \log d) \subseteq O^{\sim}(n^2 d^2)$ *operations in* $\mathbb{F}_r$*, where* $\mathsf{M}(d)$ *is as in Fact 4.1.*

4.1. A fast algorithm for the rational Jordan form of σ_q *on* V_f

We now determine the rational Jordan form of the Frobenius automorphism on the root space of an additive polynomial. We begin with a factorization of the minimal polynomial and then compute every eigenfactor's species independently. The following proposition deals with the base case, where the minimal polynomial is the power of an irreducible polynomial.

Proposition 4.4. *Let r be a power of a prime p, q a power of r,* $f \in \mathbb{F}_q[x; r]_n$ *monic squarefree of exponent n with minimal central left component* $f^* \in \mathbb{F}_r[x; q]$*, and* σ_q *the qth power Frobenius automorphism on* V_f*. If* $\tau(f^*) = u^k$ *for an irreducible* $u \in \mathbb{F}_r[y]$ *and* $k > 0$*, then*

$$\tau^{-1}(u^j)) = u^j(\sigma_q), \tag{4.5}$$

$$\ker(u^j(\sigma_q)) = V_{\mathrm{gcrc}(f, \tau^{-1}(u^j))}, \tag{4.6}$$

$$\prod_{\alpha \in \ker(u^j(\sigma_q))} (x - \alpha) = \mathrm{gcrc}(f, \tau^{-1}(u^j)) \tag{4.7}$$

for all j with $0 \le j \le k+1$*, where* $u^0(\sigma_q)$ *is the identity on* V_f*.*

Proof. Let $0 \le j \le k+1$. If we write $u^j = \sum_i w_i y^i$ with all $w_i \in \mathbb{F}_r$, then $\tau^{-1}(u^j) = \sum_i w_i x^{q^i} = u^j(\sigma_q)$, which is (4.5). The kernels of these two maps on V_f form the same subset of V_f, so that $V_{\tau^{-1}(u^j)} \cap V_f = V_{\mathrm{gcrc}(f, \tau^{-1}(u^j))}$. This shows (4.6).

Furthermore, the bijection $\varphi_{\dim(\ker(u^j(\sigma_q)))}$ from (2.3) maps the left and right hand sides of (4.6) to the left and right hand sides of (4.7), respectively. □

Corollary 4.8. *In the notation and under the assumption of Proposition 4.4, let u be irreducible of degree m and* $\nu_j = \mathrm{expn}(\mathrm{gcrc}(f, \tau^{-1}(u^j)))$ *for* $0 \le j \le k+1$*. Then the species of the rational Jordan form of* σ_q *on* V_f *is* $\{(m; \lambda_1, \lambda_2, \ldots, \lambda_k)\}$*, where*

$$\lambda_j = (2\nu_j - \nu_{j-1} - \nu_{j+1})/m, \tag{4.9}$$

for $1 \le j \le k$*.*

Proof. For monic squarefree $g \in \mathbb{F}_q[x; r]$, we have $\mathrm{expn}\, g = \dim V_g$ due to the bijection (2.2). For $0 \le j \le k+1$, $\mathrm{gcrc}(f, \tau^{-1}(u^j))$ is monic squarefree and thus

$$\nu_j = \dim(V_{\mathrm{gcrc}(f, \tau^{-1}(u^j))}) = \dim(\ker(u^j(\sigma_q))) = \mathrm{nul}(u^j(S))$$

by (4.6). The claim follows from (3.3). □

In the case of a minimal polynomial with arbitrary factorization, we treat every eigenfactor separately with Corollary 4.8, see Giesbrecht (1998, Theorem 4.1). The result is Algorithm 4.10. It computes the rational Jordan form of the Frobenius automorphism on the root space of a given $f \in \mathbb{F}_q[x; r]_n$.

Theorem 4.11. *Algorithm 4.10 works correctly as specified and takes an expected number of* $O^{\sim}(n^3 d^4)$ *field operations in* $\mathbb{F}_r$*.*

Proof. The notation in the algorithm corresponds to that of the rational Jordan form (3.2) and Corollary 4.8. In Step 1, we know from Theorem 4.2 that f^* is the minimal polynomial of S. Therefore all

Algorithm 4.10: `RationalJordanForm`

Input: r-additive monic squarefree $f \in \mathbb{F}_q[x;r]_n$ of exponent n, where $q = r^d$ and r is a power of a prime p
Output: rational Jordan form $S \in \mathbb{F}_r^{n\times n}$ as in (3.2) of the qth power Frobenius automorphism on V_f

1 $f^* \leftarrow$ minimal central left component of f
2 $u_1^{k_1} u_2^{k_2} \cdots u_t^{k_t} \leftarrow$ factorization of $\tau(f^*)$ into pairwise distinct monic irreducible $u_i \in \mathbb{F}_r[y]$ with $k_i > 0$ for $1 \le i \le t$
3 $S \leftarrow \varnothing$ `// initialize "empty matrix"`
4 **for** $i \leftarrow 1$ **to** t **do**
  `// determine the species of` u_i
5 **for** $j \leftarrow 0$ **to** $k_i + 1$ **do**
6   $h_j \leftarrow \operatorname{gcrc}(f, \tau^{-1}(u_i^j))$
7   $\nu_j \leftarrow \operatorname{expn} h_j$ `// equal to` $\operatorname{nul}(u_i^j(S))$
8 $m \leftarrow \deg_y u_i$
9 **for** $j \leftarrow 1$ **to** k_i **do**
10   $\lambda_j \leftarrow (2\nu_j - \nu_{j-1} - \nu_{j+1})/m$ `// employ (4.9)`
11   $S \leftarrow \operatorname{diag}(S, \underbrace{J_{u_i}^{(j)}, \ldots, J_{u_i}^{(j)}}_{\lambda_j\text{-times}})$ `// append Jordan blocks`
12 **return** S

rational Jordan blocks correspond to factors of f^* (determined in Step 2) and we only need to figure out every eigenfactor's species. By Giesbrecht (1998, Theorem 4.1), we can treat every eigenfactor separately (Steps 4–11) and align the resulting rational Jordan blocks along the main diagonal (Step 11, initialized in Step 3).

For every eigenfactor u_i the first inner loop (Steps 5–7) determines ν_j as defined in Corollary 4.8 for $0 \le j \le k_i + 1$. The second inner loop (Steps 9–11) derives the number λ_j of rational Jordan blocks of order j for u_i (Step 10) via formula (4.9) and extends S along its main diagonal accordingly (Step 11).

Doing this for all eigenfactors and all possible orders returns the specified output in Step 12.

We assume that the isomorphism τ and its inverse are free operations. If the polynomials are stored as vectors of coefficients, these operations merely change the way this information is interpreted. We also take for granted a free operation to determine the exponent of an additive and the degree of an "ordinary" polynomial in Steps 7 and 8, respectively. Finally, we neglect the (cheap) integer arithmetic in Step 10.

Step 1 uses $O^{\sim}(n^3d^2 + n^2d^3)$ field operations in $\mathbb{F}_r$, see Fact 4.1. We have $\operatorname{expn} f^* \le dn$ and thus $\deg_y \tau(f^*) \le n$. The factorization in Step 2 can be done in random polynomial time with $O^{\sim}(n^2 + n\log r)$ field operations in $\mathbb{F}_r$, see, e.g. von zur Gathen and Gerhard (2013, Corollary 14.30). The worst case occurs when $\tau(f^*)$ is the nth power of a linear eigenfactor u. The $n+2$ powers of u can be obtained with $O^{\sim}(n^2)$ field operations in $\mathbb{F}_r$. The additive polynomial $\tau^{-1}(u^j)$ has exponent dj and each gcrc in Step 6 requires $O^{\sim}(\max(n, dj)^2 d^2) \subseteq O^{\sim}(n^2d^4)$ field operations in $\mathbb{F}_r$, see Step 4.3. The complete inner loop thus requires $O^{\sim}(n^3d^4)$ field operations which dominates the costs of the previous steps. □

Only the distinct-degree factorization in Step 2 requires randomization. But this granularity is necessary for our approach as the following example shows. Let

$$A = \begin{pmatrix} a & & & \\ & a & & \\ & & a & \\ & & & b \end{pmatrix}, \quad B = \begin{pmatrix} a & & & \\ & a & & \\ & & b & \\ & & & b \end{pmatrix} \in \mathbb{F}_r^{4\times 4},$$

with distinct nonzero $a, b \in \mathbb{F}_r$. Then A and B are two rational Jordan forms with distinct species $\{(1;3), (1;1)\}$ and $\{2 \times (1;2)\}$, respectively, but equal minimal polynomial $u = (y-a)(y-b)$. The single equal-degree factor has multiplicity 1 and yields only the information $\dim\ker u(A) = \dim\ker u(B) = 4$, that is the sum of orders of blocks corresponding to eigenfactors of degree 1.

Caruso and Le Borgne (2017) give an algorithm for the species of the Frobenius operator on the n-dimensional module $\mathbb{F}_q[x;r]/(\mathbb{F}_q[x;r]\cdot f)$, as in von zur Gathen et al. (2010), and count complete

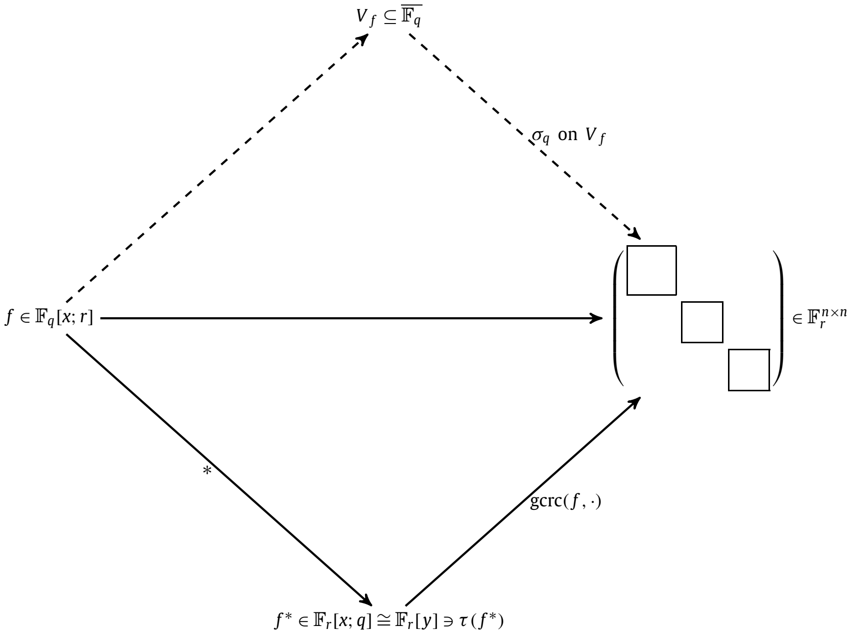


Fig. 4.13. Algorithm 4.10 computes the rational Jordan form of the Frobenius automorphism on the root space V_f of f while avoiding the expensive computation (dashed) of and on the root space itself.

decompositions, as in Fripertinger (2011). Related counting problems are also considered in Le Borgne (2012).

The costs of Algorithm 4.10 are only polynomial in $\operatorname{expn} f$ and $\log q$, despite the fact that the actual roots of f may lie in an extension of exponential degree over $\mathbb{F}_q$ as illustrated in the following example and Fig. 4.13 .

Example 4.12. Let $q = r$ and $f \in \mathbb{F}_q[y]$ be primitive of degree n. Its *additive q-associate* $\tau^{-1}(f)$ factors into x and the irreducible $\tau^{-1}(f)/x$ of degree $q^n - 1$ over $\mathbb{F}_q$, see Lidl and Niederreiter (1997, Theorem 3.63). Thus, the splitting field of the additive $\tau^{-1}(f)$ is an extension of $\mathbb{F}_q$ of degree $q^n - 1$.

Together with the results of Subsection 3.1, we can now count the number of irreducible right components of degree r of any r-additive polynomial $f \in \mathbb{F}_q[x;r]$ of exponent n. This also yields a fast algorithm to compute the number of certain factors and right components of projective and subadditive polynomials as described in Subsection 2.3.

Example 4.14. Boucher and Ulmer (2014) build self-dual codes from factorizations of $x^{r^n} - ax$ beating previously known minimal distances. Over $\mathbb{F}_4[x;2]$, they exhibit 3, 15, 90, and 543 complete decompositions for $x^{2^2} + x$, $x^{2^4} + x$, $x^{2^6} + x$, and $x^{2^8} + x$, respectively.

In this section, we assume the field size q to be a power of the parameter r. As in Bluher's (2004b) work, our methods go through for the general situation, where $q = p^d$ and $r = p^e$ are independent powers of the characteristic. Then $\mathbb{F}_q \cap \mathbb{F}_r = \mathbb{F}_s$ for $s = p^{\gcd(d,e)}$ and the centre of $\mathbb{F}_q[x;r]$ is $\mathbb{F}_s[x;t]$ for $t = p^{\operatorname{lcm}(d,e)}$.

5. Conclusion and open questions

We investigated the structure and number of all right components of an additive polynomial. This involved three steps:

- a bijective correspondence between decompositions of an additive polynomial f and Frobenius-invariant subspaces of its root space V_f in an algebraic closure of F (Section 2),
- a description of the A-invariant subspaces of an F-vector space for a rational Jordan form $A \in F^{n \times n}$ (Section 3), and
- an efficient algorithm for the rational Jordan form of the Frobenius automorphism on V_f (Section 4). Its runtime is polynomial in $\log_p(\deg f)$.

A combinatorial result of Fripertinger (2011) counts the relevant Frobenius-invariant subspaces of V_f and thus our decompositions (Subsection 3.1). We also count the number of maximal chains of Frobenius-invariant subspaces and thus the complete decompositions.

In Theorem 3.14, we describe the small set of possible values for the number of right components of exponent r of a given additive polynomial. The natural "inverse" question asks for the number of additive polynomials that admit a given number of right components.

The root space V_f has exponentially (in the exponent of f) many elements, and the field over which it is defined may have exponential degree. The efficiency of our algorithms in Section 4 is mainly achieved by avoiding any direct computation with V_f.

6. Acknowledgments

This work was supported by the German Academic Exchange Service (DAAD) in the context of the German-Canadian PPP program. In addition, Joachim von zur Gathen and Konstantin Ziegler were supported by the B-IT Foundation and the Land Nordrhein-Westfalen. Mark Giesbrecht acknowledges the support of the Natural Sciences and Engineering Research Council of Canada (NSERC). Cette recherche a été financée par le Conseil de Recherches en Sciences Naturelles et en Génie du Canada (CRSNG).

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Abhyankar, S.S., 1997. Projective polynomials. Proc. Am. Math. Soc. 125, 1643–1650. http://www.jstor.org/stable/2162203.

Akbary, A., Ghioca, D., Wang, Q., 2009. On permutation polynomials of prescribed shape. Finite Fields Appl. 15, 195–206. https://doi.org/10.1016/j.ffa.2008.12.001.

Barton, D.R., Zippel, R., 1985. Polynomial decomposition algorithms. J. Symb. Comput. 1, 159–168.

Blankertz, R., 2014. A polynomial time algorithm for computing all minimal decompositions of a polynomial. ACM Commun. Comput. Algebra 48 (187), 13–23.

Blankertz, R., von zur Gathen, J., Ziegler, K., 2013. Compositions and collisions at degree p^2. J. Symb. Comput. 59, 113–145. https://doi.org/10.1016/j.jsc.2013.06.001. Also available at http://arxiv.org/abs/1202.5810. Extended abstract. In: Proceedings of the 2012 International Symposium on Symbolic and Algebraic Computation ISSAC 2012. Grenoble, France, 2012, pp. 91–98.

Bluher, A.W., 2003. On $x^6 + x + a$ in characteristic three. Des. Codes Cryptogr. 30, 85–95. https://doi.org/10.1023/A:1024711426896.

Bluher, A.W., 2004a. Explicit formulas for strong Davenport pairs. Acta Arith. 112, 397–403. https://doi.org/10.4064/aa112-4-5.

Bluher, A.W., 2004b. On $x^{q+1} + ax + b$. Finite Fields Appl. 10, 285–305. https://doi.org/10.1016/j.ffa.2003.08.004.

Bluher, A.W., Lasjaunias, A., 2006. Hyperquadratic power series of degree four. Acta Arith. 124, 257–268.

Boucher, D., Ulmer, F., 2014. Self-dual skew codes and factorization of skew polynomials. J. Symb. Comput. 60, 47–61. https://doi.org/10.1016/j.jsc.2013.10.003.

Brickman, L., Fillmore, P.A., 1967. The invariant subspace lattice of a linear transformation. Can. J. Math. 19, 810–822. https://doi.org/10.4153/CJM-1967-075-4.

Caruso, X., Le Borgne, J., 2017. A new faster algorithm for factoring skew polynomials over finite fields. J. Symb. Comput. 79, 411–443. https://doi.org/10.1016/j.jsc.2016.02.016.

Caruso, X., Le Borgne, J., 2018. Fast multiplication of skew polynomials. In: Burr, M. (Ed.), Proceedings of the 2018 International Symposium on Symbolic and Algebraic Computation ISSAC '14. ACM Press, Kaiserslautern, Germany, pp. 77–84.

Cohen, S.D., 1990. The factorable core of polynomials over finite fields. J. Aust. Math. Soc. A 49, 309–318. https://doi.org/10.1017/S1446788700030585.

Coulter, R.S., Havas, G., Henderson, M., 2004. On decomposition of sub-linearised polynomials. J. Aust. Math. Soc. 76, 317–328. https://doi.org/10.1017/S1446788700009885.

Dillon, J.F., 2002. Geometry, codes and difference sets: exceptional connections. In: Codes and Designs. Columbus, OH, 2000. In: Ohio State Univ. Math. Res. Inst. Publ., vol. 10. De Gruyter, Berlin, pp. 73–85.

Dorey, F., Whaples, G., 1974. Prime and composite polynomials. J. Algebra 28, 88–101. https://doi.org/10.1016/0021-8693(74)90023-4.

Fried, M.D., MacRae, R.E., 1969. On the invariance of chains of fields. Ill. J. Math. 13, 165–171.

Fripertinger, H., 2011. The number of invariant subspaces under a linear operator on finite vector spaces. Adv. Math. Commun. 5, 407–416. https://doi.org/10.3934/amc.2011.5.407.

Frobenius, G., 1911. Über den Rang einer Matrix. Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften, vol. 1, pp. 20–29. https://archive.org/details/sitzungsberichte1911deut. Erster Halbband. Januar bis Juni.

Gantmacher, F.R., 1959. The Theory of Matrices, Vol. I. Chelsea Publishing Company, New York.

von zur Gathen, J., 1990a. Functional decomposition of polynomials: the tame case. J. Symb. Comput. 9, 281–299. https://doi.org/10.1016/S0747-7171(08)80014-4. Extended abstract. In: Proceedings of the 28th Annual IEEE Symposium on Foundations of Computer Science. Los Angeles CA, 1987.

von zur Gathen, J., 1990b. Functional decomposition of polynomials: the wild case. J. Symb. Comput. 10, 437–452. https://doi.org/10.1016/S0747-7171(08)80054-5.

von zur Gathen, J., 2014. Counting decomposable univariate polynomials. Special Issue. Comb. Probab. Comput. 01 (24). https://doi.org/10.1017/S0963548314000388, 294–328. Extended abstract. In: Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation ISSAC '09. Seoul, Korea, 2009. Preprint, 2008, available at http://arxiv.org/abs/0901.0054.

von zur Gathen, J., Gerhard, J., 2013. Modern Computer Algebra, third ed. Cambridge University Press, Cambridge, UK. http://cosec.bit.uni-bonn.de/science/mca/. Other editions: 1999, 2003, Chinese edition, Japanese translation.

von zur Gathen, J., Giesbrecht, M., Ziegler, K., 2010. Composition collisions and projective polynomials: statement of results. In: Watt, S. (Ed.), Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation ISSAC '10. ACM Press, Munich, Germany, pp. 123–130. Preprint available at http://arxiv.org/abs/1005.1087.

Giesbrecht, M., 1988. Some Results on the Functional Decomposition of Polynomials. Master's thesis. Department of Computer Science, University of Toronto. Technical Report 209/88. Available at http://arxiv.org/abs/1004.5433.

Giesbrecht, M., 1995. Nearly optimal algorithms for canonical matrix forms. SIAM J. Comput. 24, 948–969.

Giesbrecht, M., 1998. Factoring in skew-polynomial rings over finite fields. J. Symb. Comput. 26, 463–486. https://doi.org/10.1006/jsco.1998.0224.

Hardy, G.H., Ramanujan, S., 1918. Asymptotic formulae in combinatory analysis. Proc. Lond. Math. Soc. 17, 75–115.

Harvey, D., van der Hoeven, J., 2019a. Faster polynomial multiplication over finite fields using cyclotomic coefficient rings. J. Complex. 54. https://doi.org/10.1016/j.jco.2019.03.004.

Harvey, D., van der Hoeven, J., 2019b. Polynomial multiplication over finite fields in time $O(n \log n)$ URL. https://hal.archives-ouvertes.fr/hal-02070816. Preprint.

Helleseth, T., Kholosha, A., 2010. $x^{2^l+1} + x + a$ and related affine polynomials over GF(2^k). Cryptogr. Commun. 2. https://doi.org/10.1007/s12095-009-0018-y.

Helleseth, T., Kholosha, A., Johanssen, A., 2008. m-sequences of lengths $2^{2^k} - 1$ and $2^k - 1$ with at most four-valued cross correlation. In: Golomb, S.W., Parker, M.G., Pott, A., Winterhof, A. (Eds.), Proceedings of the 5th International Conference on Sequences and Their Applications. Lexington KY. Springer-Verlag, Lexington, KY, USA, pp. 106–120.

Henderson, M., Matthews, R., 1999. Composition behaviour of sub-linearised polynomials over a finite field. In: Finite Fields: Theory, Applications, and Algorithms. Waterloo, ON, 1997. In: Contemp. Math., vol. 225. Amer. Math. Soc., Providence, RI, pp. 67–75.

Jacobson, N., 1943. The Theory of Rings. American Mathematical Society, New York.

Kozen, D., Landau, S., 1989. Polynomial decomposition algorithms. J. Symb. Comput. 7, 445–456. https://doi.org/10.1016/S0747-7171(89)80027-6. An earlier version was published as Technical Report 86-773. Cornell University, Department of Computer Science, Ithaca, New York, 1986.

Kung, J.P., 1981. The cycle structure of a linear transformation over a finite field. Linear Algebra Appl. 36, 141–155. https://doi.org/10.1016/0024-3795(81)90227-5.

Landau, S., Miller, G.L., 1985. Solvability by radicals is in polynomial time. J. Comput. Syst. Sci. 30, 179–208.

Le Borgne, J., 2012. Représentations galoisiennes et φ-modules: aspects algorithmiques. Ph.D. thesis. Université de Rennes 1.

Le Gall, F., 2014. Powers of tensors and fast matrix multiplication. In: Proceedings of the 2014 International Symposium on Symbolic and Algebraic Computation ISSAC '14. Kobe, Japan, pp. 296–303. Also available at http://arxiv.org/abs/1401.7714.

Lidl, R., Niederreiter, H., 1997. Finite Fields, 2nd ed. Encyclopedia of Mathematics and Its Applications, vol. 20. Cambridge University Press, Cambridge, UK. First published by Addison-Wesley, Reading MA, 1983.

Lüneburg, H., 1987. On the Rational Normal Form of Endomorphisms: A Primer to Constructive Algebra. Wissenschaftsverlag, Mannheim.

McDonald, B.R., 1974. Finite Rings with Identity. Marcel Dekker, Inc., New York.

Odoni, R.W.K., 1999. On additive polynomials over a finite field. Proc. Edinb. Math. Soc. 42, 1–16.

Ore, O., 1933. On a special class of polynomials. Trans. Am. Math. Soc. 35, 559–584.

Schinzel, A., 1982. Selected Topics on Polynomials. The University of Michigan Press, Ann Arbor.
Schinzel, A., 2000. Polynomials with Special Regard to Reducibility. Cambridge University Press, Cambridge, UK.
Stein, W.A., et al., 2014. Sage Mathematics Software (Version 6.1.1). The Sage Development Team. http://www.sagemath.org.
Stichtenoth, H., Topuzoğlu, A., 2012. Factorization of a class of polynomials over finite fields. Finite Fields Appl. 18, 108–122. https://doi.org/10.1016/j.ffa.2011.07.005.
Zannier, U., 1993. Ritt's second theorem in arbitrary characteristic. J. Reine Angew. Math. 445, 175–203. http://eudml.org/doc/153580.
Zeng, X., Li, N., Hu, L., 2008. A class of nonbinary codes and their weight distribution. arXiv:0802.3430v1.
Ziegler, K., 2015. Counting classes of special polynomials. Dissertation. Rheinische Friedrich-Willhelms-Universität Bonn, Bonn, Germany. http://hss.ulb.uni-bonn.de/2015/3981/3981.htm.
Ziegler, K., 2016. Tame decompositions and collisions. In: Special Issue on the Conference ISSAC 2014: Symbolic Computation and Computer Algebra. J. Symb. Comput., 244–268. https://doi.org/10.1016/j.jsc.2015.11.017. Preprint available at arXiv:1402.5945, 2014. Extended abstract. In: Proceedings of the 2014 International Symposium on Symbolic and Algebraic Computation ISSAC '14. Kobe, Japan, 2014.
Zippel, R., 1991. Rational function decomposition. In: Watt, S.M. (Ed.), Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation ISSAC '91. Bonn, Germany. ACM Press, Bonn, Germany, pp. 1–6.