Factoring and Decomposing Ore Polynomials over $\mathbb{F}_q(t)$

Mark Giesbrecht
School of Computer Science
University of Waterloo
Waterloo, Ontario, Canada
mwg@uwaterloo.ca

Yang Zhang
Department of Applied Mathematics
University of Western Ontario
London, Ontario, Canada
yzhang@scl.csd.uwo.ca

ABSTRACT

We present algorithms for computing factorizations and least common left multiple (LCLM) decompositions of Ore polynomials over $\mathbb{F}_q(t)$, for a prime power $q = p^\mu$. Our algorithms are effective in $\mathbb{F}_q(t)[\mathcal{D};\sigma,\delta]$, for any automorphism σ and σ-derivation δ of $\mathbb{F}_q(t)$. On input $f \in \mathbb{F}_q(t)[\mathcal{D};\sigma,\delta]$, the algorithms run in time polynomial in $\deg_{\mathcal{D}}(f)$, $\deg_t(f)$, p and μ.

Categories and Subject Descriptors

I.1 [**Symbolic and Algebraic Manipulation**]: Algorithms

General Terms

Algorithms

Keywords

Factoring, Ore polynomial, modular, eigenring

1. INTRODUCTION

The Ore polynomials $\mathsf{F}(t)[\mathcal{D};\sigma,\delta]$, over a field of rational function $\mathsf{F}(t)$, are the polynomials in $\mathsf{F}(t)[\mathcal{D}]$ under the usual addition and (generally non-commutative) multiplication such that

$$\mathcal{D}a(t) = \sigma(a(t))\mathcal{D} + \delta(a(t)) \quad \text{for any } a(t) \in \mathsf{F}(t).$$

Here σ is any automorphism of $\mathsf{F}(t)$ and a δ is a σ-derivation, that is, δ is an F-linear map such that for $a, b \in \mathsf{F}(t)$, $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$. This ring has been well studied mathematically at least since Ore [1933b]; we draw heavily on the excellent expositions in Cohn [1985, 1995], as well as Jacobson [1943, 1996] in this paper. $\mathsf{F}(t)[\mathcal{D};\sigma,\delta]$ is a principal left (right) ideal domain, and hence admits unique monic least common left (right) multiples (LCLMs) and greatest common right (left) divisors (GCRDs). Efficient algorithms for basic operations and an introduction to the computational theory are given in Bronstein and Petkovšek [1994].

We present algorithms for the following two problems in Ore polynomial domains over $\mathbb{F}_q(t)$, the field of rational functions over the finite field $\mathbb{F}_q$ with $q = p^\mu$ elements where p is prime. Given $f \in \mathbb{F}_q(t)[\mathcal{D};\sigma,\delta]$:

(1) **Factorization:** find $g, h \in \mathbb{F}_q(t)[\mathcal{D};\sigma,\delta] \setminus \mathbb{F}_q(t)$ such that $f = gh$, or a certify that f is irreducible in $\mathbb{F}_q(t)[\mathcal{D};\sigma,\delta]$ (there is no such factorization).

(2) **LCLM-decomposition:** find $g, h \in \mathbb{F}_q(t)[\mathcal{D};\sigma,\delta]$ of positive degree in $\mathcal{D}$ such that $f = \mathrm{lclm}(g,h)$ and $\mathrm{gcrd}(g,h) = 1$, or certify that f is indecomposible in $\mathbb{F}_q(t)[\mathcal{D};\sigma,\delta]$ (there is no such decomposition).

The number of steps required by our algorithms is polynomial in $\deg_{\mathcal{D}}(f)$, $\deg_t(f)$, p and μ.

We consider a general class of Ore polynomials. Over $\mathbb{F}_q(t)$, we let σ be any automorphism fixing $\mathbb{F}_q$, so $\sigma(t) = (\sigma_1 t + \sigma_2)/(\sigma_3 t + \sigma_4)$, for $\sigma_1, \sigma_2, \sigma_3, \sigma_4 \in \mathbb{F}_q$ such that $\sigma_1\sigma_4 - \sigma_2\sigma_3 \neq 0$. The σ-derivation δ is arbitrary, and can be specified completely by $\delta(t) \in \mathbb{F}_q(t)$. Standard canonicalization to the pure shift, pure dilation, and pure derivation cases will be presented in Section 2. As well, we summarize the costs and coefficient bounds on basic operations in Section 2.

The main idea of our algorithms is that the *eigenring* can be used to factor and LCLM-decompose any $f \in \mathbb{F}_q(t)[\mathcal{D};\sigma,\delta]$. A similar idea is employed in Giesbrecht [1992, 1998] to give efficient algorithms for factoring and LCLM-decomposing Ore polynomials over $\mathbb{F}_q[\mathcal{D};\tau]$, where τ is a Frobenius automorphism of $\mathbb{F}_q$. Indeed, this is one of the original settings for Ore polynomials explored by Ore [1933a, 1934]. Properties of the eigenring, and an efficient algorithm to compute it, are presented in Section 3. For notational convenience we will generally write $\mathfrak{S} := \mathbb{F}_q(t)[\mathcal{D};\sigma,\delta]$. Following Ore [1932, 1933b, 1934], but essentially using the language of Cohn [1985], we define the *idealizer* of $\mathfrak{S}f$ to be $I(\mathfrak{S}f) = \{u \in \mathfrak{S} \mid fu \in \mathfrak{S}f\}$. $I(\mathfrak{S}f)$ is the largest subalgebra of $\mathfrak{S}$ in which $\mathfrak{S}f$ is a two-sided ideal. The *eigenring* $E(\mathfrak{S}f)$ of $\mathfrak{S}f$ is defined as the quotient $E(\mathfrak{S}f) = I(\mathfrak{S}f)/\mathfrak{S}f$. The eigenring is an associative algebra over the field of constants $\mathsf{K} = \{a(t) \in \mathbb{F}_q(t) : a(t)\mathcal{D} = \mathcal{D}a(t)\}$.

ISSAC'03, August 3–6, 2003, Philadelphia, Pennsylvania, USA.
Copyright 2003 ACM 1-58113-641-2/03/0008 ...$5.00.

In Section 3, we develop the central theory behind our algorithms. The first key point, which has been used in the differential case by van der Put [1996], is that $\mathbb{F}_q(t)$ is a *finite algebraic extension of* K. In particular, $\mathsf{K} \cong \mathbb{F}_q(T)$, for an indeterminate T. We prove here that this is the case for all rings of Ore polynomials over $\mathbb{F}_q(t)$. (This is in contrast to the case over $\mathsf{F}(t)$, for a field F of characteristic zero, where the field of constants is F.) Over $\mathbb{F}_q(t)$, the eigenring $E(\mathfrak{S}f)$ is isomorphic to a finite dimensional associative algebra (of relatively small dimension) over K.

The second key point is that every non-trivial zero-divisor in $E(\mathfrak{S}f)$ yields a non-trivial factorization of f, *and* f is irreducible if and only if $E(\mathfrak{S}f)$ is a division algebra. For LCLM-decompositions, we show correspondingly that any pair of orthogonal idempotents in $E(\mathfrak{S}f)$ yield a non-trivial LCLM-decomposition of f, and f is LCLM-decomposable if and only if $\mathsf{E}(\mathfrak{S}f)$ possesses no such orthogonal idempotents.

Finally, we note that there are efficient algorithms for the problem of finding zero divisors and idempotents in finite dimensional associative algebras over $\mathsf{K} = \mathbb{F}_q(T)$. Ivanyos et al. [1994] provide an efficient algorithm for computing the Jacobson radical and primitive orthogonal idempotents in the semi-simple part. We extend this in a straightforward way to produce orthogonal idempotents in the algebra itself (should they exist). That we can demonstrate our algorithms to require polynomial time relies on the fact that the algorithm of Ivanyos et al. [1994] requires time polynomial in the dimension of the input associative algebra and the degree (in T) of the structure constants.

In Section 4, we employ this correspondence between zero divisors in the eigenring and factorizations to split reducible polynomials. Similarly, in Section 5, we use the correspondence between orthogonal idempotents in the eigenring and LCLM-decompositions to compute LCLM-decompositions.

While we do not give the explicit exponents, the dominant cost is the decomposition of the eigenring, and this requires time about $O((\deg_{\mathcal{D}}(f) + \deg_t(f) + p + \mu)^6)$. Note that the algorithm runs in time polynomial in p, not $\log p$, reflecting the fact the dimension of the eigenring is polynomial in p.

Relation to other factoring methods

The earliest and most famous method for factoring differential operators goes back to Beke [1894]. Many factorization algorithms are based on Beke's algorithm for computing first order factors and then computing higher order factors by using the exterior power method. In many cases these methods are quite expensive in practice. Recently, a number of authors have pursued different approaches.

By considering the exponential parts of linear differential operators, van Hoeij [1997] gives a new efficient factorization algorithm. Since the existence of hyperexponential solutions is equivalent to the existence of right factors of degree 1, Bronstein and Petkovšek [1996] describes an algorithm that reduces the problem of factoring in Ore polynomial to finding all the irreducible right factors of degree 1. Singer [1996] gives a method to decide if a linear differential operator is reducible without having to find a factor. He uses the fact that each differential operator L is associated to a linear algebraic group G, its Galois, and the reductive property of G decides if L is reductive. He shows that factorization can be reduced to solving an so-called mixed equation in many cases. Van Hoeij [1996] provides an efficient method to compute the solutions of this equation.

Most closely related to our work here, van der Put [1995, 1996, 1997] gives procedures for factoring differential operators over $\mathbb{Q}(t)$ and $\mathbb{F}_p(t)$ by considering the so-called p-curvature. In principle these techniques can be generalized to the case of difference operators: see van der Put and Singer [1997], Sections 5.1 and 5.2. Very recently, Cluzeau [2003] presents algorithms for factoring differential systems with coefficients in $\mathbb{F}_p(t)$.

2. CANONICAL SKEW POLYNOMIAL RINGS

While Ore's skew polynomials, with both an automorphism and a derivation, appear quite general, there are in fact only a small number of representative cases. In this section we briefly present this well-known reduction. Throughout this section we consider the ring $\mathfrak{S} := \mathbb{F}_q(t)[\mathcal{D}; \sigma, \delta]$, where σ is an automorphism of $\mathbb{F}_q(t)$ fixing $\mathbb{F}_q$ and δ is a σ-derivation of $\mathbb{F}_q(t)$. While we state the results over $\mathbb{F}_q(t)$, much of what we say will hold over $\mathsf{F}(t)$ for any perfect field F.

2.1 Reducing to the pure automorphism and derivation cases

It is well known that if $\mathbb{F}_q(t)[\mathcal{D}; \sigma, \delta]$ has both a non-trivial automorphism σ*and* non-trivial σ-derivation δ, then, after a change of variables, $\mathfrak{S}$ is isomorphic to a ring $\mathfrak{S}' = \mathbb{F}_q(t)[\mathcal{D}'; \sigma']$ with only an automorphism (i.e., whose derivation is identically zero) by means of the substitution:

$$\mathcal{D} \to \frac{\mathcal{D} + \delta(t)}{t - \sigma(t)},$$

See Cohn [1985], Proposition 3.1, page 498. This change of variables is computationally efficient. Thus, we need only consider the pure automorphism case $\mathbb{F}_q(t)[\mathcal{D}; \sigma]$ and the pure derivation case $\mathbb{F}_q(t)[\mathcal{D}; \delta]$.

2.2 Automorphism classes and the shift and dilation cases

In this subsection we assume that $\mathfrak{S} := \mathbb{F}_q(t)[\mathcal{D}; \sigma]$. We show that any such ring is isomorphic to a ring $\mathbb{F}_q(t)[\overline{\mathcal{D}}; \overline{\sigma}]$ of difference operators (i.e., where $\overline{\sigma}(t) = t + \gamma$ for $\gamma \in \mathbb{F}_q$), or a ring of dilation operators (i.e., where $\overline{\sigma}(t) = \xi t$ for some $\xi \in \mathbb{F}^*_{q^2}$) over a quadratic field extension. This classification is straightforward (and well known), and the transformation is computationally efficient.

Every automorphism of $\mathbb{F}_q(t)$ which fixes $\mathbb{F}_q$ has the property that

$$\sigma(t) = \frac{\sigma_1 t + \sigma_2}{\sigma_3 t + \sigma_4} \quad \text{where } \det \begin{pmatrix} \sigma_1 & \sigma_2 \\ \sigma_3 & \sigma_4 \end{pmatrix} \neq 0.$$

The automorphisms form a group under composition, and it is easily proven that $\mathrm{Aut}(\mathbb{F}_q(t)) \cong \mathrm{PGL}(2, \mathbb{F}_q)$, the projective general linear group of invertible 2×2 matrices over $\mathbb{F}_q$ modulo scalar multiples of the identity. In particular, there is an isomorphism

$$\mathrm{Aut}(\mathbb{F}_q(t)) \to \mathrm{PGL}(2, \mathbb{F}_q), \qquad \frac{\sigma_1 t + \sigma_2}{\sigma_3 t + \sigma_4} \;\mapsto\; \begin{pmatrix} \sigma_1 & \sigma_2 \\ \sigma_3 & \sigma_4 \end{pmatrix}.$$

Since every matrix is similar to a matrix in Jordan form, every $s \in \mathbb{F}_q^{2\times 2}$ satisfies either

$$\text{Case (1)} \quad \exists u \in \mathbb{F}_{q^2}^{2\times 2}, \text{ such that } usu^{-1} = \begin{pmatrix} \alpha^q & 0 \\ 0 & \alpha \end{pmatrix}, \quad \text{for } \alpha \in \mathbb{F}_{q^2};$$

$$\text{Case (2)} \quad \exists u \in \mathbb{F}_q^{2\times 2} \text{ such that } usu^{-1} = \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}, \quad \text{for } \alpha \in \mathbb{F}_q.$$

Note that in Case (1), s generally has distinct eigenvalues and hence a generally irreducible minimal polynomial over $\mathbb{F}_q$. Thus the eigenvalues, and transformation matrices to the Jordan form, lie in a quadratic extension $\mathbb{F}_{q^2}$ of $\mathbb{F}_q$. In Case (2) s has a repeated eigenvalues, which must lie in $\mathbb{F}_q$.

This notion of normal form is easily extended to the skew polynomial ring itself. Suppose σ is represented in $\mathrm{PGL}(2, \mathbb{F}_q)$ by $s \in \mathbb{F}_q^{2\times 2}$ and usu^{-1} is in Jordan form as above. Let τ be the fractional linear transformation corresponding to u. Then

$$\overline{\sigma} := \tau \circ \sigma \circ \tau^{-1} = \begin{cases} \xi t, \text{ for } \xi = \alpha^{q-1} \in \mathbb{F}_{q^2}^{*}, \text{ a \textit{dilation}, or} \\ t + \gamma, \quad \text{for } \gamma = \alpha^{-1} \in \mathbb{F}_q, \text{ \textit{a shift.}} \end{cases}$$

The map τ, which is itself an automorphism of $\mathbb{F}_q(t)$, is naturally extended to $\mathbb{F}_q(t)[\mathcal{D}; \sigma]$, by $\tau(\mathcal{D}) = \overline{\mathcal{D}}$, whence $\mathbb{F}_q(t)[\mathcal{D}; \sigma] \cong \mathbb{F}_q(t)[\overline{\mathcal{D}}; \overline{\sigma}]$.

To factor an $f \in \mathbb{F}_q(t)[\mathcal{D}; \sigma]$ we may thus factor the polynomial $\tau(f)$. This ring isomorphism is efficiently computable, and thus we assume from now on that σ is either a shift or dilation over $\mathbb{F}_q(t)$, where q is redefined as appropriate.

2.3 Derivation operators

It is easily observed that the derivation operator, in the pure derivation ring $\mathbb{F}_q(t)[\mathcal{D}; \delta]$, satisfies the standard algebraic properties of differentiation. In particular, δ is $\mathbb{F}_q$-linear and $\delta(t^n) = nt^{n-1}\delta(t)$. We can specify the derivation operator completely by specifying the value of $\delta(t) \in \mathbb{F}_q(t)$, and for any rational function $r(t) \in \mathbb{F}_q(t)$, we have $\delta(r(t)) = r'(t)\delta(t)$, where $r'(t) \in \mathbb{F}_q(t)$ is the usual first derivative of r with respect to t. For simplicity, we will assume that $\delta(t)$ is of constant degree, and do not consider its degree explicitly in our analyses.

2.4 Representation and basic operations with skew polynomials

To standardize our representation of $f \in \mathbb{F}_q(t)[\mathcal{D}; \sigma, \delta]$, we write

$$f = \sum_{0 \le i \le n} a_i(t)\mathcal{D}^i,$$

where the $a_0(t), \ldots, a_n(t) \in \mathbb{F}_q(t)$ are always written to the left of the power of $\mathcal{D}$. Let $c \in \mathbb{F}_q[t]$ be the LCM of the denominators of coefficients of f. It is obvious that $c \cdot f \in \mathbb{F}_q[t][\mathcal{D}; \sigma, \delta]$, and if $c \cdot f = f_1 f_2 \cdots f_k$, for $f_1, \ldots, f_k \in \mathbb{F}_q(t)[\mathcal{D}; \sigma, \delta]$, then $f = (c^{-1} \cdot f_1) f_2 \cdots f_k$. There is no necessity that polynomials in $\mathbb{F}_q[t][\mathcal{D}; \sigma, \delta]$ factor over $\mathbb{F}_q[t][\mathcal{D}; \sigma, \delta]$, and indeed there may be reducible polynomials in $\mathbb{F}_q[t][\mathcal{D}; \sigma, \delta]$ such that every complete factorization involves at least one factor in $\mathbb{F}_q(t)[\mathcal{D}; \sigma, \delta] \setminus \mathbb{F}_q[t][\mathcal{D}; \sigma, \delta]$. We may, however, assume that our input comes from $\mathbb{F}_q[t][\mathcal{D}; \sigma]$ or $\mathbb{F}_q[t][\mathcal{D}; \delta]$ and our output is in $\mathbb{F}_q(t)[\mathcal{D}; \sigma]$ or $\mathbb{F}_q(t)[\mathcal{D}; \delta]$ respectively.

Basic operations with skew polynomials are performed with the polynomials in standard representation. These basic operations are addition, subtraction, multiplication, division with remainder, greatest common right (left) divisor (GCRD), and least common left multiple (LCLM). Many good algorithms have been developed for these operations (see, e.g., Bronstein and Petkovšek [1994], Li [1998], van der Hoeven [2002]) We note the following crude bounds on the costs of these algorithms and on the size of the output (see Li [2002]).

Theorem 2.1. *Let $f, g \in \mathbb{F}_q(t)[\mathcal{D}; \sigma, \delta]$, and $h_1 = f + g$, $h_2 = fg$, $h_3 = \mathrm{rem}(f, g)$, $h_4 = \mathrm{quo}(f, g)$ (i.e., $f = \mathrm{quo}(f, g)g + \mathrm{rem}(f, g)$ for the unique $\mathrm{quo}(f, g)$, and $\mathrm{rem}(f, g) \in \mathbb{F}_q(t)[\mathcal{D}; \sigma, \delta]$ such that $\deg_{\mathcal{D}}(\mathrm{rem}(f, g)) < \deg_{\mathcal{D}}(g)$), $h_5 = \mathrm{lclm}(f, g)$, and $h_6 = \mathrm{gcrd}(f, g)$). Then bounds on the degrees in $\mathcal{D}$ for $h_1, \ldots, h_6$ are as in the usual polynomial case, while*

$$\deg_t(h_i) = O\left((\deg_{\mathcal{D}}(f) + \deg_{\mathcal{D}}(g))(\deg_t(f) + \deg_t(g))\right)$$

for $1 \le i \le 6$. The cost of computing $h_1, \ldots, h_6$ is bounded by

$$O\left((\deg_{\mathcal{D}}(f) + \deg_{\mathcal{D}}(g))^5 (\deg_t(f) + \deg_t(g))^2\right)$$

operations in $\mathbb{F}_q$.

3. THE EIGENRING OF ORE POLYNOMIALS OVER FINITE FIELDS

In this section we describe the centre of the ring of Ore polynomials $\mathbb{F}_q(t)[\mathcal{D}; \sigma, \delta]$, where $\mathfrak{S} := \mathbb{F}_q(t)[\mathcal{D}; \sigma]$ for an automorphism σ, or $\mathfrak{S} := \mathbb{F}_q(t)[\mathcal{D}; \delta]$ for a derivation δ. In each case the centre turns out to be the usual polynomial ring $\mathbb{F}_q(T)[Y]$, for independent indeterminates T and Y. Hence the centre is a unique factorization domain. We then observe that every polynomial in $\mathfrak{S}$ has a non-trivial left multiple in the centre, the *minimal central multiple*. We then describe the eigenring of a polynomial and give its properties. In particular, how zero-divisors in the eigenring correspond to factors of the original polynomial. We also show how to construct the eigenring efficiently.

An element $f \in \mathfrak{S}$ is *invariant* if $\mathfrak{S}f = f\mathfrak{S}$. An invariant element f^* such that $\mathfrak{S}f \supseteq \mathfrak{S}f^*$ is called a *bound* for f, and f is said to be *bounded*, if there exists a non-trivial bound. Closely related to the invariant elements in $\mathfrak{S}$ is the centre $\mathfrak{C}$ of $\mathfrak{S}$, those elements which commute with every element of $\mathfrak{S}$. Every element $f \in \mathfrak{S}$ has a minimal central left (and right) multiple

$\hat{f} \in \mathfrak{C}\backslash\{0\}$, the (monic) polynomial of lowest degree in the centre which is a left (right) multiple of f. Jacobson [1943], Chapter 3, Theorem 11 shows that the central left and right multiples are in fact equal. Thus, we refer to $\hat{f}$ as simply the *minimal central multiple* of f.

3.1 The centre in the pure automorphism case

We first consider the shift and dilation cases. To describe the centre of $\mathfrak{S}$, we must first understand the constant field K of σ, whose elements are fixed by the automorphism. Following Ore [1933a], we say an $\varphi \in \mathbb{F}_q[t]$ is *additive* if $\varphi(\alpha+\beta) = \varphi(\alpha) + \varphi(\beta)$ for any $\alpha, \beta \in \overline{\mathbb{F}_q}$, where $\overline{\mathbb{F}_q}$ is the algebraic closure of $\mathbb{F}_q$. The additive polynomials in $\mathbb{F}_q[t]$, where $q = p^\mu$, are exactly those of the form $\varphi = \sum_{0\le i\le\mu} \varphi_i t^{p^i} \in \mathbb{F}_q[t]$.

Theorem 3.1. *Let K be the constant field of σ.*

- *If $\sigma(t) = t+\gamma$ for some $\gamma \in \mathbb{F}_q^*$ then $\mathsf{K} = \mathbb{F}_q(\varphi(t))$, where $\varphi \in \mathbb{F}_q[t]$ is the additive polynomial of smallest degree such that $\varphi(\gamma) = 0$.*
- *If $\sigma(t) = \xi t$ for some $\xi \in \mathbb{F}_q^*$ then $\mathsf{K} = \mathbb{F}_q(t^\nu)$, where ν is the multiplicative order of ξ.*

Proof. First observe that $\sigma(\varphi(t)) = \varphi(t+\gamma) = \varphi(t) + \varphi(\gamma) = \varphi(t)$, so $\varphi(t)$ is invariant under σ, as is $t^q - t$. Thus $\mathbb{F}_q(t^q - t) \subseteq \mathsf{K} \subseteq \mathbb{F}_q(t)$. By Lurōth's theorem $\mathsf{K} = \mathbb{F}_q(v(t))$ for some $v \in \mathbb{F}_q[t]$, and there exists a $u \in \mathbb{F}_q[t]$ such that $t^q - t = u(v(t))$. Since $t^q - t$ is additive, by Theorem 3.3 of Giesbrecht [1988] we find u, v are also additive. Letting φ be the additive polynomial of minimal degree with root γ ensures that $\mathsf{K} = \mathbb{F}_q(\varphi(t))$.

In the dilation case, $h(t) = \sum_{0\le i\le m} h_i t^i \in \mathbb{F}_q[t]$ is fixed by σ when $\sigma(h(t)) = h(\xi t)$ This is true only if for all i, $h_i = 0$ or $\xi^i = 1$, i.e., when $h \in \mathbb{F}_q[t^\nu]$. By Montgomery [1980], Page 71, the only rational functions which are fixed by σ are quotients of polynomials in K, and hence $\mathsf{K} = \mathbb{F}_q(t^\nu)$ □

For consistency, we will let $\nu := \deg\varphi$ in the shift case. Thus, in both the shift and the dilation case we can write the ground field as an algebraic extension of degree ν over the constant field K of σ. It should be noted that in all cases it is straightforward to compute the constant field.

The centre of $\mathfrak{S}$ is characterized by the following:

Theorem 3.2. *The centre $\mathfrak{C}$ of a pure automorphism Ore polynomial ring is characterized as follows.*

- *Usual: When $\sigma(t) = t$, $\mathfrak{C} = \mathbb{F}_q(T)[Y]$ where $T = t$ and $Y = \mathcal{D}$;*
- *Shift: When $\sigma(t) = t+\gamma$ for $\gamma \in \mathbb{F}_q^*$, then $\mathfrak{C} = \mathbb{F}_q(T)[Y]$, where $T = \varphi(t)$ as in Theorem 3.1, and $Y = \mathcal{D}^\nu$;*
- *Dilation: When $\sigma(t) = \xi t$ is a dilation, then $\mathfrak{C} = \mathbb{F}_q(T)[Y]$ where $T = t^\nu$ and $Y = \mathcal{D}^\nu$, and σ has multiplicative order ν.*

Thus in all cases $\mathfrak{C}$ is a usual, commutative polynomial ring.

Proof. For $f = \sum_{0\le i\le n} a_i(t)\mathcal{D}^i \in \mathfrak{S}$ to be in the centre, $t \cdot f = f \cdot t$ or

$$\sum_{0\le i\le n} a_i(t)t{\cdot}\mathcal{D}^i = \sum_{0\le i\le n} a_i(t)\mathcal{D}^i{\cdot}t = \sum_{0\le i\le n} a_i(t){\cdot}\sigma^i(t){\cdot}\mathcal{D}^i,$$

whence either $a_i(t) = 0$ or $\sigma^i(t) = t$. In other words $\mathfrak{C} \subseteq \mathbb{F}_q(t)[\mathcal{D}^\nu;\sigma]$.

We note also that $\mathcal{D}\cdot f = f\cdot\mathcal{D}$ or

$$\mathcal{D}{\cdot}\sum_{0\le i\le n} a_i(t)\mathcal{D}^i = \sum_{0\le i\le n} \sigma(a_i(t))\mathcal{D}^{i+1} = \sum_{0\le i\le n} a_i(t){\cdot}\mathcal{D}^{i+1}.$$

Thus, $\sigma(a_i(t)) = a_i(t)$, or in other words, $a_i(t) \in \mathsf{K}$ for $0 \le i \le n$.

Combining these two conditions yields the centre, as specified in the theorem. □

There is a close relationship between the centre, the minimal central multiples and the invariant elements. In the automorphism case $\mathbb{F}_q(t)[\mathcal{D};\sigma]$, Jacobson [1996], Theorem 1.1.22, shows every invariant element f^* has the form $f^* = a(t)\mathcal{D}^k\hat{f}$ for $\hat{f} \in \mathfrak{C}$, $a(t) \in \mathbb{F}_q(t)$ and $k \in \mathbb{Z}_{\ge 0}$.

3.2 The centre and minimal central multiples in $\mathbb{F}_q(t)[\mathcal{D};\delta]$

In the derivation case, the constant subfield of $\mathbb{F}_q(t)$ in $\mathbb{F}_q(t)[\mathcal{D};\delta]$ is $\mathsf{K} = \{a(t) \in \mathbb{F}_q(t) : \delta(a(t)) = 0\}$.

Lemma 3.3. *The constant subfield of $\mathbb{F}_q(t)[\mathcal{D};\delta]$ is $\mathbb{F}_q(t^p)$.*

Proof. We first consider the kernel of δ in the polynomial ring $\mathbb{F}_q[t]$. Suppose $a(t) = a_n t^n + a_{n-1}t^{n-1} + \cdots + a_0 \in \mathbb{F}_q[t]$, and $\delta(a(t)) = 0$. Then

$$\begin{aligned} 0 &= \delta(a(t)) \\ &= na_nt^{n-1}\delta(t) + (n-1)a_{n-1}t^{n-2}\delta(t) + \cdots + a_1\delta(t) \\ &= (na_nt^{n-1} + (n-1)a_{n-1}t^{n-2} + \cdots + a_1)\delta(t). \end{aligned} \tag{1}$$

Since $\delta(t) \ne 0$, it follows that

$$a(t) = a_{mp}(t^p)^m + a_{(m-1)p}(t^p)^{m-1} + \cdots + a_pt^p + a_0 \in \mathbb{F}_q[t^p],$$

where $m = n/p \in \mathbb{N}$, or in other words, $a(t) \in \mathbb{F}_q[t^p]$.

To identify the kernel of δ in $\mathbb{F}_q(t)$, Corollary 3.9, Bergen and Montgomery [1986] implies that the only fractions in the kernel of δ are fractions of polynomials in the kernel of δ. That is, the kernel of δ is $\mathbb{F}_q(t^p)$. □

We note that $\mathbb{F}_q(t)$ is an algebraic extension of $\mathsf{K} = \mathbb{F}_q(t^p)$ of degree p. For consistency with the automorphism case we let $\nu = p = [\mathbb{F}_q(t) : \mathsf{K}]$.

Lemma 3.4. *The centre of $\mathbb{F}_q(t)[\mathcal{D};\delta]$ is $\mathbb{F}_q(t^p)[\mathcal{D}^p]$.*

Proof. This is proven in Amitsur [1957]. See Jacobson [1996], Theorem 1.1.32. □

For consistency with the automorphism case, we let $T = t^p$ and $Y = D^p$, so the centre of $\mathbb{F}_q(t)[\mathcal{D};\delta]$ is the commutative polynomial ring $\mathbb{F}_q(T)[Y]$.

Again there is a close relationship between the centre, the minimal central multiples and the invariant elements. In the pure derivation case $\mathbb{F}_q(t)[\mathcal{D};\delta]$, Amitsur [1957] shows $f^* = a(t)\hat{f}$ for $\hat{f} \in \mathfrak{C}$ and $a(t) \in \mathbb{F}_q(t)$.

3.3 Constructing the eigenring

To completely factor an $f \in \mathfrak{S}$, we construct a finite dimensional associative algebra $\mathfrak{A}$ over the constant subfield K, with the property that each non-trivial zero divisor in $\mathfrak{A}$ yields a non-trivial factorization of f. A candidate for $\mathfrak{A}$ might be the quotient $\mathfrak{S}/\mathfrak{S}f$, but it is in general only an $\mathfrak{S}$-module, and not an algebra. While we could in principle decompose this module directly, the algorithmic machinery to do so has not been completely developed. $\mathfrak{S}/\mathfrak{S}f$ is only an algebra when $\mathfrak{S}f$ is a two-sided ideal in $\mathfrak{S}$. To regain some of the desirable structure of finite algebras, we follow Cohn [1985], Section 0.7, and introduce the eigenring. Define

$$I(\mathfrak{S}f) = \{u \in \mathfrak{S} \mid fu \in \mathfrak{S}f\}$$

the *idealizer* of $\mathfrak{S}f$. The set $I(\mathfrak{S}f)$ is the largest subalgebra of $\mathfrak{S}$ in which $\mathfrak{S}f$ is a two-sided ideal. The *eigenring* $E(\mathfrak{S}f)$ of $\mathfrak{S}f$ is defined as the quotient

$$E(\mathfrak{S}f) = I(\mathfrak{S}f)/\mathfrak{S}f,$$

a finite dimensional K-algebra since $\mathfrak{S}$ is an K-algebra and $\mathfrak{S}f$ a two-sided ideal in $I(\mathfrak{S}f)$.

The key facts about $E(\mathfrak{S}f)$, which we shall prove in the coming subsections, are that it is a division ring if and only if f is irreducible, and that non-trivial zero divisors in $E(\mathfrak{S}f)$ allow us to compute non-trivial factors of f efficiently. We shall also prove that pairs of orthogonal idempotents summing to the identity in $E(\mathfrak{S}f)$ correspond to LCLM-decompositions.

Computationally, we will represent the eigenring as a finite dimensional subalgebra of a matrix ring over K, where K is the field of constants in $\mathbb{F}_q(t)$. If $\deg f = n$, the eigenring $E(\mathfrak{S}f)$ is isomorphic to the K-algebra

$$\begin{aligned}\mathfrak{A} &= \{u \in I(\mathfrak{S}f) \mid \deg u < n\}\\ &= \{u \in \mathfrak{S} \mid fu \in \mathfrak{S}f \text{ and } \deg u < n\} \cong E(\mathfrak{S}f)\end{aligned}$$

under addition in $\mathfrak{S}$ and multiplication in $\mathfrak{S}$ reduced modulo f (i.e., each element in $E(\mathfrak{S}f)$ is represented by its unique residue modulo f of degree less than n).

To compute a K-basis for $\mathfrak{A}$, let $W \subseteq \mathfrak{S}$ be the set of all $g \in \mathfrak{S}$ with $\deg g < n$. As a K-vector space W is isomorphic to $\mathfrak{S}/\mathfrak{S}f$, with K-basis

$$\{t^i\mathcal{D}^j \mid 0 \le i < \nu,\ 0 \le j < n\},$$

and dimension $n\nu$. Multiplication on the left by f induces an K-linear map $\Psi : W \to W$: if $u \in W$ then $\Psi(u) = v$, where $fu = wf + v$ for $w \in \mathfrak{S}$ and $v \in \mathfrak{S}$, the unique remainder, with degree less than n. Clearly $v \in W$. The elements of $\mathfrak{A}$ are exactly those elements in the null space of Ψ, a basis which is found by constructing a matrix for Ψ (an $n\nu \times n\nu$ matrix over K) and then using linear algebra over K to compute a basis for the null space. This matrix is computed by evaluating Ψ at each of the basis elements of W, i.e., finding $\Psi(t^i\mathcal{D}^j)$ for $0 \le i < \nu$ and $0 \le j < n$.

Thus, $\mathfrak{A}$ can be presented by means of a K-basis $A_1, \ldots, A_m \in W$ of polynomials under multiplication in $\mathfrak{S}$ reduced modulo f, or as a K-basis $\mathfrak{A}_1, \ldots, \mathfrak{A}_m \in \mathsf{K}^{n\nu\times n\nu}$ of matrices, where $\mathfrak{A}_i$ specifies the linear action of A_i on W. Finding such a basis for $\mathfrak{A}$ involves only $n\nu$ divisions with remainder in $\mathfrak{S}$ of polynomials of degree less than n in $\mathcal{D}$ and less than $\max\{\deg_t f, q\}$ in t, followed by linear algebra to find the kernel of Ψ. We obtain the following.

Theorem 3.5. *A basis $A_1, \ldots, A_m \in W$ for $\mathfrak{A}$ as a reduced polynomial algebra, or a basis $\mathfrak{A}_1, \ldots, \mathfrak{A}_m \in \mathsf{K}^{n\nu\times n\nu}$ for $\mathfrak{A}$ as a matrix algebra, can be found in time polynomial in $\deg_{\mathcal{D}} f$, $\deg_t f$ and p.*

3.4 Reducibility and the eigenring

We show that non-trivial zero-divisors exists in $E(\mathfrak{S}f)$ if and only if f has a non-trivial factorization.

Theorem 3.6. *Let $f \in \mathfrak{S}$. Then f has a non-trivial factorization if and only if $E(\mathfrak{S}f)$ has non-trivial zero divisors.*

Proof. Any non-trivial zero divisor in $E(\mathfrak{S}f)$ yields a non-trivial factorization of f. For if $u, v \in I(\mathfrak{S}f)$, with $u, v \notin \mathfrak{S}f$ and $uv \in \mathfrak{S}f$, it follows that $\mathrm{gcrd}(f, u) \neq 1$. To see this, suppose conversely that $\mathrm{gcrd}(f, u) = 1$. There exist $s, t \in \mathfrak{S}$ such that $sf + tu = 1$ and $sfv + tuv = v$. But $fv \in \mathfrak{S}f$ and $uv \in \mathfrak{S}f$ so $v \in \mathfrak{S}f$, a contradiction. If u, v are represented in the basis W, then they have degree (in $\mathcal{D}$) less than that of f, and hence $\mathrm{gcrd}(f, u)$ is a non-trivial right factor of f.

To prove the converse, assume f is not irreducible, and $f = gh$ for $g, h \in \mathfrak{S}$ of positive degree. Let $\hat{f} \in \mathfrak{C} = \mathsf{K}[Y]$ be the minimal central multiple of f.

First suppose $\hat{f}$ is reducible as a polynomial in $\mathsf{K}[Y]$, that is, $\hat{f} = \hat{g}\hat{h}$ for $\hat{g}, \hat{h} \in \mathsf{K}[Y] \setminus \mathsf{K}$. Since $\hat{g}, \hat{h} \in \mathfrak{C}$, both $\hat{g}$ and $\hat{h} \in I(\mathfrak{S}f)$. By the minimality of $\deg \hat{f}$, we also know $\hat{g}, \hat{h} \notin \mathfrak{S}f$, i.e., $\hat{g} + \mathfrak{S}f, \hat{h} + \mathfrak{S}f \in E(\mathfrak{S}f) \setminus \{0\}$. Finally, since $\hat{g}\hat{h} \in \mathfrak{S}f$, we see $\hat{g} + \mathfrak{S}f, \hat{h} + \mathfrak{S}f$ are zero divisors in $E(\mathfrak{S}f)$.

Now assume that $\hat{f}$ is irreducible as a polynomial in $\mathsf{K}[Y]$ (and $f = gh$ is reducible in $\mathfrak{S}$), we show that in fact $f = \mathrm{lclm}(f_1, f_2)$ for some $f_1, f_2 \in \mathfrak{S}$ of positive degree such that $\mathrm{gcrd}(f_1, f_2) = 1$, i.e., f is *LCLM-decomposable*. In this case there exist $g_1, g_2 \in \mathfrak{S}$ such that $g_1f_1 + g_2f_2 = 1$. Let $h_1 = g_1f_1$ and $h_2 = g_2f_2$, neither of which are equivalent to zero modulo f. Then

$$fh_1 = f(1 - g_2f_2) \in \mathfrak{S}f_2 \quad \text{and} \quad fh_1 = fg_1f_1 \in \mathfrak{S}f_1,$$

so $fh_1 \in \mathfrak{S}f$. Similarly $fh_2 \in \mathfrak{S}f$, so $h_1, h_2 \in I(\mathfrak{S}f)$. Moreover, $h_1h_2 = h_1 - h_1^2 = h_2 - h_2^2$, which is right-equivalent to zero modulo both f_1 and f_2, and hence modulo f. Thus $(h_1 + \mathfrak{S}f)(h_2 + \mathfrak{S}f) \in \mathfrak{S}f$ and $h_1 + \mathfrak{S}f$ and $h_2 + \mathfrak{S}f$ are non-trivial zero divisors in $E(\mathfrak{S}f)$.

Still assuming that $\hat{f}$ is irreducible as a polynomial in $\mathsf{K}[Y]$ yet f is reducible, we now show that f is in fact LCLM-decomposable. Since $\mathfrak{S}\hat{f}$ is a maximal two-sided ideal in $\mathfrak{S}$, $E(\mathfrak{S}f) = \mathfrak{S}/\mathfrak{S}\hat{f}$ is a (finite dimensional) simple algebra and

$$0 \subsetneq \underbrace{E(\mathfrak{S}f)(f+\mathfrak{S}\hat{f})}_{\mathfrak{F}} \subsetneq \underbrace{E(\mathfrak{S}f)(h+\mathfrak{S}\hat{f})}_{\mathfrak{H}} \subseteq E(\mathfrak{S}f)$$

is a tower of left ideals in $E(\mathfrak{S}f)$. Since $E(\mathfrak{S}f)$ is simple there exists a complementary ideal $\mathfrak{G}$ such that $\mathfrak{H} \cap \mathfrak{G} = \mathfrak{F}$ and $\mathfrak{F} + \mathfrak{G} = 1$. $E(\mathfrak{S}f)$ inherits from $\mathfrak{S}$ the property of being a left principal ideal ring. That is, there exists a unique monic $\bar{g} \in \mathfrak{S}$ of minimal degree such that $\mathfrak{G} = \bar{g} + \mathfrak{S}\hat{f}$, called the *minimal left modular generator* of $\mathfrak{G}$. This follows easily from the fact that if $\bar{g}_1 + \mathfrak{S}\hat{f}, \bar{g}_2 + \mathfrak{S}\hat{f} \in \mathfrak{G}$, then $\operatorname{gcrd}(\bar{g}_1, \bar{g}_2) + \mathfrak{S}\hat{f} \in \mathfrak{G}$. Thus $\mathfrak{G} = \bar{g} + \mathfrak{S}\hat{f}$, $f = \operatorname{lclm}(h, \bar{g})$ and $\operatorname{gcrd}(h, \bar{g}) = 1$. Thus f is decomposable, and hence its eigenring has zero divisors. □

Note that the above theorem does not hold in general, at least in the derivation case in characteristic 0. Singer [1996] exhibits reducible polynomials whose eigenrings are division algebras. Essentially, it is the fact that $\mathbb{F}_q(t)$ is an *algebraic* extension of the field of constants that allows for the more representative structure of the eigenring.

3.5 Decomposability and the eigenring

For a given polynomial $f \in \mathfrak{S}$, we now show a correspondence between the existence of a pair of non-trivial orthogonal idempotents summing to the identity in $E(\mathfrak{S}f)$, and the existence of a non-trivial LCLM-decomposition of f.

Recall that two idempotents e_1, e_2 in an algebra are orthogonal if $e_1e_2 = e_2e_1 = 0$.

THEOREM 3.7. *Let $e_1, e_2 \in I(\mathfrak{S}f)$ be such that $\bar{e}_1 = e_1 + \mathfrak{S}f$ and $\bar{e}_2 = e_2 + \mathfrak{S}f \in E(\mathfrak{S}f)$ are non-trivial orthogonal idempotents such that $e_1 + e_2 \in 1 + \mathfrak{S}f$ (so $e_1e_2 \in \mathfrak{S}f$ and $e_1^2 - e_1, e_2^2 - e_2 \in \mathfrak{S}f$). Let $f_i \in \mathfrak{S}\backslash\{0\}$ be the polynomial of minimal degree such that $f_ie_i \subseteq \mathfrak{S}f$, for $i = 1, 2$. Then $f = \operatorname{lclm}(f_1, f_2)$ and $\operatorname{gcrd}(f_1, f_2) = 1$.*

PROOF. For $i = 1, 2$, the set $J_i = \{u \in \mathfrak{S} : ue_i \in \mathfrak{S}f\}$ is a left ideal in $\mathfrak{S}$. Since $\mathfrak{S}$ is a principal left ideal ring, J_i is generated by a unique monic $f_i \in \mathfrak{S}$. Note that f_i is a right factor of f since $f \in J_i$ (because $e_i \in I(\mathfrak{S}f)$).

For any $h \in \mathfrak{S}$ such that $h \in \mathfrak{S}f_1$ and $h \in \mathfrak{S}f_2$, then $h + \mathfrak{S}f = h(e_1 + e_2) + \mathfrak{S}f$. But $he_i \in \mathfrak{S}f$, so $h \in \mathfrak{S}f$. Hence $f = \operatorname{lclm}(f_1, f_2)$.

We now show $\operatorname{gcrd}(f_1, f_2) = 1$. Let $g_1 = \operatorname{gcrd}(f, e_1)$, $g_2 = \operatorname{gcrd}(f, e_2)$. Clearly $\operatorname{gcrd}(g_1, g_2) = \operatorname{gcrd}(f, e_1, e_2) = 1$ since $e_1 + e_2 \in 1 + \mathfrak{S}f$. There exist $v_i, w_i \in \mathfrak{S}$ such that $v_if + w_ie_i = g_i$. Now $g_2e_1 = (v_2f + w_2e_2)e_1 = v_2fe_1 + w_2e_2e_1 \in \mathfrak{S}f$. Thus $f_1 \,|\, g_2$. Similarly $f_2 \,|\, g_1$. Since $\operatorname{gcrd}(g_1, g_2) = 1$, it follows that $\operatorname{gcrd}(f_1, f_2) = 1$. □

THEOREM 3.8. *Given $f \in \mathfrak{S}$, and f_1, f_2 of positive degree such that $\operatorname{gcrd}(f_1, f_2) = 1$ and $f = \operatorname{lclm}(f_1, f_2)$, there exist non-trivial orthogonal idempotents $\bar{e}_1, \bar{e}_2 \in E(\mathfrak{S}f)$ whose sum is $1 \in E(\mathfrak{S}f)$.*

PROOF. Since $\operatorname{gcrd}(f_1, f_2) = 1$, there exists $g_1, g_2 \in \mathfrak{S}$ such that $g_1f_1 + g_2f_2 = 1$. Let $h_1 = g_1f_1$ and $h_2 = g_2f_2$, neither of which lie in $\mathfrak{S}f$. Then $fh_1 = f(1 - g_2f_2) = f - fg_2f_2 \in \mathfrak{S}f_2$ and $fh_1 = fg_1f_1 \in \mathfrak{S}f_1$, so $fh_1 \in \mathfrak{S}f$. Similarly $fh_2 \in \mathfrak{S}f$, so $h_1, h_2 \in I(\mathfrak{S}f)$. We assign $\bar{e}_1 = h_1 + \mathfrak{S}f$, and $\bar{e}_2 = h_2 + \mathfrak{S}f$ and note that both are in $E(\mathfrak{S}f) = I(\mathfrak{S}f)/\mathfrak{S}$. Moreover, $h_1h_2 = h_1 - h_1^2 = h_2 - h_2^2 \in \mathfrak{S}f$, since its is clearly in $\mathfrak{S}f_1$ and $\mathfrak{S}f_2$, and hence in $\mathfrak{S}f$. Thus $\bar{e}_1$ and $\bar{e}_2$ are orthogonal idempotents in $E(\mathfrak{S}f)$. As well, $h_1 + h_2 = 1$, so $\bar{e}_1 + \bar{e}_2 = 1 \in E(\mathfrak{S}f)$. □

4. FACTORING MODULAR ORE POLYNOMIALS

Theorem 3.6 effectively reduces the problem of factoring in $\mathfrak{S}$ to finding zero divisors in a finite dimensional associative algebra over the field of constants K in both the difference and differential case. To find such zero divisors quickly we use the algorithm of Ivanyos et al. [1994]. For any finite-dimensional associative algebra over $\mathbb{F}_q(T)$, their algorithm finds the Jacobson radical if it exists, and, for a semi-simple algebra, finds a system of primitive orthogonal idempotents. Otherwise it reports that $\mathfrak{A}$ is a division algebra. In either case, the output immediately yields zero divisors or states that non-exists. The algebra is presented to the zero-divisor finding algorithm as a basis of generating matrices over $\mathbb{F}_q(T)$ (also known as the *structure constants* for the algebra). The algorithm of Ivanyos et al. [1994] runs in time polynomial in the dimension of the algebra and the height (degree in T) of the structure constants (entries in the basis). Computing a basis for the eigenring $\mathfrak{A} \cong E(\mathfrak{S}f)$ has been discussed in the previous section.

The cost of their algorithm is polynomial in the dimension of the algebra, the maximum degree of the entries of the generating matrices, and $\log q$.

Again, we let $\mathfrak{S} = \mathbb{F}_q(t)[\mathcal{D}; \sigma, \delta]$, transformed to a pure differential or automorphism ring as in Section 2.

```
Algorithm: Factorization
Input:    ▸ $f \in \mathfrak{S}$ of degree $n$;
Output:   ▸ $g, h \in \mathfrak{S}$, or a message that $f$ is irreducible;
(1) Compute a basis $A_1, \ldots, A_m \subseteq \mathsf{K}^{n\nu \times n\nu}$ for $\mathfrak{A} \cong E(\mathfrak{S}f)$ as in Subsection 3.3;
(2) If $\mathfrak{A}$ is a division ring then report "$f$ is irreducible"
    Else
(3)     Find a non-trivial left zero divisor $u \in \mathfrak{A}$;
        Compute $h := \operatorname{gcrd}(f, u)$ and $g \in \mathfrak{S}$ with $f = gh$;
(5)     Return $g, h$;
```

THEOREM 4.1. *The above algorithm works as specified. It runs in time polynomial in $\deg_{\mathcal{D}}(f)$, $\deg_t(f)$ and q.*

PROOF. Correctness when f is irreducible follows from Theorem 3.6, as does the existence of u when f is irreducible. Suppose that $v \in \mathfrak{A}\backslash\{0\}$ is such that $uv = 0$. To see that $\operatorname{gcrd}(f, u)$ is a non-trivial factor of f, assume to the contrary that $\operatorname{gcrd}(f, u) = 1$. Then there exist $s, t \in \mathfrak{S}$ such that $sf + tu = 1$ and $sfv + tuv = v$. But

$fv \in \mathfrak{S}f$ and $uv \in \mathfrak{S}f$, so $v \in \mathfrak{S}f$, a contradiction to v being non-trivial in $\mathfrak{A}$ (which is defined modulo f).

The costs are dominated by finding a basis for the eigenring (see Theorem 3.5) and finding the zero-divisors in $\mathfrak{A}$ (see Ivanyos et al. [1994]), all of which are polynomial in $\deg_{\mathcal{D}}(f)$, $\deg_t(f)$ and q. □

5. COMPUTING A COMPLETE LCLM DECOMPOSITION

In this section we present a method for the LCLM-decomposition of a polynomial $f \in \mathbb{F}_q(t)[\mathcal{D};\sigma,\delta]$. Again, we let $\mathfrak{S} = \mathbb{F}_q(t)[\mathcal{D};\sigma,\delta]$, transformed to a pure differential or automorphism ring as in Section 2.

Using the relationship between the existence of an LCLM-decomposition and the existence of non-trivial, orthogonal idempotents in $\mathsf{E}(\mathfrak{S}f)$ summing to 1 developed in Theorems 3.7 and 3.8 of the previous section, we reduce the problem to finding such idempotents.

We need to be able to find a pair of orthogonal idempotents in $\mathfrak{A}$ which sum to the identity. We again employ the algorithm of Ivanyos et al. [1994], this time to compute $\mathrm{Rad}(\mathfrak{A})$ and an idempotent in $\mathfrak{A}$ mod $\mathrm{Rad}(\mathfrak{A})$. We use this to construct an idempotent in $\mathfrak{A}$ as follows.

```
Algorithm: Orthogonal-Idempotents
Input:   ▸ a basis $\mathfrak{A}_1,\ldots,\mathfrak{A}_m \in \mathsf{K}^{r\times r}$ for an associative algebra (containing the identity).
           Here $\mathsf{K} = \mathbb{F}_q(T)$ for an indeterminate $T$, and $q$ some power of a prime $q$.
Output:  ▸ non-trivial orthogonal idempotents $e_1, e_2 \in \mathfrak{A}$ such that $e_1 + e_2 = 1$.
(1) Compute $\mathrm{Rad}(\mathfrak{A})$, and assume $\mathrm{Rad}(\mathfrak{A})^\eta = 0$, using the algorithm of Ivanyos et al. [1994].
(2) If $\mathfrak{A}/\mathrm{Rad}(\mathfrak{A})$ is a division algebra;
(3)     Then output "$\mathfrak{A}$ has no non-trivial idempotents";
(3) Else
(4)     Let $\bar{e} \in \mathfrak{A}$ be such that $\bar{e}$ mod $\mathrm{Rad}(\mathfrak{A})$ is a non-trivial idempotent in $\mathfrak{A}/\mathrm{Rad}(\mathfrak{A})$, using the algorithm of Ivanyos et al. [1994].
(5)     Compute $u \in \mathsf{K}[x]$: $u \equiv 1 \bmod x^\eta$, $u \equiv 0 \bmod (x-1)^\eta$;
                    $v \in \mathsf{K}[x]$: $v \equiv 0 \bmod x^\eta$, $v \equiv 1 \bmod (x-1)^\eta$;
(6)     Output $e_1 := u(\bar{e})$, $e_2 = v(\bar{e})$;
```

Theorem 5.1. *Orthogonal-Idempotents works as specified. The time require is polynomial in r and the maximum degree of any entry in $\mathfrak{A}_i$ for $1 \le i \le m$.*

Proof. We need to show that e_1, e_2 are orthogonal idempotents in $\mathfrak{A}$. First, note that $\bar{e}^2 - \bar{e} \in \mathrm{Rad}(\mathfrak{A})$, so $(\bar{e}^2-\bar{e})^\eta = 0$. Thus, the minimal polynomial in $\mathsf{K}[x]$ of $\bar{e}$ divides $(x^2-x)^\eta = x^\eta(x-1)^\eta$. With u, v as in step (5), we know

$$\begin{aligned} u(x) &= q_1(x)x^\eta + 1 \qquad & u(x) &= q_2(x)(x-1)^\eta \\ v(x) &= r_1(x)x^\eta \qquad & v(x) &= r_2(x)(x-1)^\eta + 1 \end{aligned}$$

for some $q_1, q_2, r_1, r_2 \in \mathsf{K}[x]$. Now

$$\begin{aligned} e_1^2 - e_1 = e_1(e_1-1) &= q_2(\bar{e})(\bar{e}-1)^\eta q_1(\bar{e})\bar{e}^\eta \\ &= \bar{e}^\eta(\bar{e}-1)^\eta q_1(\bar{e})q_2(\bar{e}) = 0, \\ e_2^2 - e_2 = e_2(e_2-1) &= r_2(\bar{e})(\bar{e}-1)^\eta r_1(\bar{e})\bar{e}^\eta \\ &= \bar{e}^\eta(\bar{e}-1)^\eta r_1(\bar{e})r_2(\bar{e}) = 0, \\ e_2e_1 = e_1e_2 &= q_1(\bar{e})(\bar{e}-1)^\eta r_1(\bar{e})\bar{e}^\eta \\ &= \bar{e}^\eta(\bar{e}-1)^\eta q_1(\bar{e})r_1(\bar{e}) = 0. \end{aligned}$$

Finally $e_1 + e_2 = u(\bar{e}) + v(\bar{e}) = (u+v)(\bar{e})$. But $u + v \equiv 1 \bmod x^\eta(x-1)^\eta$ by construction, so $e_1 + e_2 = 1$.

That the algorithm runs in polynomial in the dimension r and the maximum degree of a structure constant follows immediately from Ivanyos et al. [1994]. □

We can now present our algorithm to compute an LCLM-decomposition.

```
Algorithm: LCLM-Decomposition
Input:   ▸ $f \in \mathfrak{S}$ of degree $n$;
Output:  ▸ $g, h \in \mathfrak{S}$ with $f = \mathrm{lclm}(g,h)$ and $\mathrm{gcrd}(g,h) = 1$ for $1 \le i \le k$;
(1) Compute a basis $A_1,\ldots,A_m \subseteq \mathsf{K}^{n\nu\times n\nu}$ for $\mathfrak{A} \cong E(\mathfrak{S}f)$ as in Section 3;
(2) Using Orthogonal-Idempotents, attempt to find a pair of orthogonal idempotents $e_1, e_2 \in \mathfrak{A}$ such that $e_1 + e_2 = 1 \in \mathfrak{A}$;
(3) If no such idempotents exist, report "$f$ is indecomposable";
    Else
(4)     Let $g, h \in \mathfrak{S}$ each be of minimal degree such that $ge_1 \in \mathfrak{S}f$, and $he_2 \in \mathfrak{S}f$;
(5)     Return $g, h$;
```

Theorem 5.2. *The above algorithm works as specified. It runs in time polynomial in $\deg_{\mathcal{D}}(f)$, $\deg_t(f)$ and p.*

Proof. Correctness of Step (3) follows from Theorem 3.8, and that of Step (5) follows from Theorem 3.7.

The dominant cost in this algorithm is computing the orthogonal idempotents with `Orthogonal-Idempotents`, which can be done in time polynomial in the dimension and degree of entries in the basis for $\mathfrak{A}$, i.e., polynomial in n, $\deg_t(f)$ and p. As well, we must compute g and h in step (4), but this is simply linear algebra in W (see Subsection 3.3). □

6. CONCLUSION

Given $f \in \mathbb{F}_q(t)[\mathcal{D};\sigma,\delta]$, we have considered the problems of computing factorizations $f = gh$ for $g, h \in \mathbb{F}_q(t)[\mathcal{D};\sigma,\delta]$, and LCLM-decompositions $f = \mathrm{lclm}(g,h)$ for relatively (right) prime g, h. The algorithms presented require time polynomial in $\deg_{\mathcal{D}} f$, $\deg_t f$ and q. Our main idea was to work by decomposing the eigenring, and use the correspondence between these decompositions and factorizations to split f.

Many important questions remain to be considered. We have shown here how to split and LCLM-decompose polynomials into two factors, and can iterate the algorithm on these factors until a complete factorization or complete LCLM-decomposition is obtained. However, we must be careful to manage the growth in the degree of t in the factors. We can also ask if there are any factors of a specific given degree s. For this an analogue to the method of Giesbrecht [1998] should apply.

As noted earlier, one of the main goals was to apply this work to factoring in $\mathbb{Q}(t)[\mathcal{D};\sigma,\delta]$. The problems of lifting and factor reconstruction are considerably more difficult in the non-commutative case. Interesting mathematical questions also arise in understanding the factorization pattern under modular reduction, which could greatly affect the complexity of algorithms for these problems.

7. ACKNOWLEDGEMENT

The authors are grateful to the anonymous referees for pointing out the important unpublished works of van der Put [1997], and to their author for allowing access to them. We are also grateful to Jacques-Arthur Weil, Thomas Cluzeau, Ziming Li, and Anne Fredet for their correspondence.

The first author acknowledges the support of NSERC, ORDCF, and Waterloo Maple Incorporated.

References

S. A. Amitsur. Derivations in simple rings. *Proc. London Mathematical Society*, VII, 3rd series:87–112, 1957.

E. Beke. Die irreducibilität der homogenen linearen differentialgleichungen. *Math. Annalen*, 45:278–300, 1894.

J. Bergen and S. Montgomery. Smash products and outer derivations. *Israel Journal of Mathematics*, 53 (1):321–345, 1986.

M. Bronstein and M. Petkovšek. On Ore rings, linear operators and factorisation. *Programmirovanie*, 20: 27–45, 1994.

M. Bronstein and M. Petkovšek. An introduction to pseudo-linear algebra. *Theoretical Computer Science*, 157:3–33, 1996.

T. Cluzeau. Factorization of differential systems in characteristic p. These proceedings. 2003.

P. Cohn. *Free Rings and their Relations*. Academic Press, London, 1985.

P. Cohn. *Skew Fields: Theory of General Division Rings*. Cambridge, London, 1995.

M. Giesbrecht. Some results on the functional decomposition of polynomials. Master's thesis, University of Toronto, 1988. Also available as University of Toronto Technical Report 209/88.

M. Giesbrecht. Factoring in skew-polynomial rings. In *Proceedings of Latin American Theoretical INformatics Conference (LATIN)*, pages 191–203, Sao Paulo, Brasil, 1992.

M. Giesbrecht. Factoring in skew-polynomial rings over finite fields. *J. of Symbolic Computation*, 24(5):463–486, 1998.

M. van Hoeij. Rational solutions of the mixed differential equation and its application to factorization of differential operators. In *Proc. ISSAC'96*, pages 219–225, 1996.

M. van Hoeij. Factorization of differential operators with rational functions coefficients. *J. Symb. Comp.*, 24:537–561, 1997.

J. van der Hoeven. FFT-like multiplication of linear differential operators. *J. Symb. Comp.*, 33(1):123–127, 2002.

G. Ivanyos, L. Rónyai, and A. Szántó. Decomposition of algebras over $\mathbb{F}_q(x_1,\ldots,x_m)$. *Applicable Algebra in Engineering, Communication and Computing*, 5: 71–90, 1994.

N. Jacobson. *The Theory of Rings*. American Math. Soc., New York, 1943.

N. Jacobson. *Finite-Dimensional Division Algebras over Fields*. Springer-Verlag, 1996.

Z. Li. A subresultant theory for ore polynomials with applications. In *Proc. ISSAC 1998*, pages 132–139, 1998.

Z. Li. Some bounds for skew polynomials, 2002. Preprint.

S. Montgomery. *Fixed rings of finite automorphism groups of associative rings*, volume 818 of *Lecture Notes in Mathematics*. Springer-Verlag, 1980.

O. Ore. Formale Theorie der linearen Differentialgleichungen. *J. reine angew. Math.*, 168:233–252, 1932.

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

O. Ore. Theory of non-commutative polynomials. *Annals of Mathematics*, 34(22):480–508, 1933b.

O. Ore. Contributions to the theory of finite fields. *Trans. Amer. Math. Soc.*, 36:243–274, 1934.

M. van der Put. Differential equations in characteristic p. *Compositio Mathematica*, 97:227–251, 1995.

M. van der Put. Reduction modulo p of differential equations. *Indag. Mathem.*, 7(3):367–387, 1996.

M. van der Put. Modular methods for factoring differential operators. Unpublished manuscript, 34 pp., 1997.

M. van der Put and M.F. Singer. *Galois Theory of Difference Equations*. LNM 1666. Springer, 1997.

M. F. Singer. Testing reducibility of linear differential operators: A group theoretic perspective. *Applicable Algebra in Engineering, Communication and Computing*, 7(2):77–104, 1996.