ON DECOMPOSITION OF SUB-LINEARISED POLYNOMIALS

ROBERT S. COULTER, GEORGE HAVAS and MARIE HENDERSON

(Submitted 19 August 2002; revised 3 March 2003)

Abstract

We give a detailed exposition of the theory of decompositions of linearised polynomials, using a well known connection with skew-polynomial rings with zero derivative. It is known that there is a one-to-one correspondence between decompositions of linearised polynomials and sub-linearised polynomials. This correspondence leads to a formula for the number of indecomposable sub-linearised polynomials of given degree over a finite field. We also show how to extend existing factorisation algorithms over skew-polynomial rings to decompose sub-linearised polynomials without asymptotic cost.

1. Introduction

Let F be a field with $F[X]$ the ring of polynomials with coefficients from F in the indeterminate X. For polynomials $f, f_1, f_2 \in F[X]$, let $\deg(f)$ be the degree of f and $f_1 \circ f_2$ denote the composition $f_1(f_2)$. Note that $\deg(f_1 \circ f_2) = \deg(f_1)\deg(f_2)$. A polynomial f is called *indecomposable* if for all $f_1, f_2 \in F[X]$ satisfying $f = f_1 \circ f_2$, then either $\deg(f_1) = 1$ or $\deg(f_2) = 1$. A *complete* decomposition of $f \in F[X]$ is any decomposition of f into indecomposable factors. The problem of polynomial decomposition has been well studied with [20] providing a survey of results. Generally, decomposition behaviour can been split into two cases: the characteristic of F is zero or the degree of the polynomial is not divisible by the characteristic of F; or F is a finite field and the degree of the polynomial is divisible by the characteristic of the field. In this article we consider two classes of polynomials over a finite field with degree divisible by the characteristic. Determining results on decomposition behaviour for such polynomials is, in general, less tractable.

Let $\mathbb{F}_q$ be the finite field of order $q = p^e$ for a prime p and $\mathbb{F}_q^*$ be the set of non-zero elements of $\mathbb{F}_q$. Polynomials of $\mathbb{F}_q[X]$ with degree divisible by the characteristic p are called *wild polynomials*

This research was funded by the Australian Research Council

and those with degree not divisible by p are called *tame polynomials*, see [8, 9]. For a positive integer s, a *p^s-polynomial* $L \in \mathbb{F}_q[X]$ with $\deg(L) = p^{st}$ is a polynomial of the shape

$$L(X) = \sum_{i=0}^{t} a_i X^{p^{si}} \tag{1}$$

where $a_i \in \mathbb{F}_q$ and $a_t \in \mathbb{F}_q^*$. For $s = 1$ these polynomials are known as *linearised polynomials* and are precisely the linear transformations of $\mathbb{F}_q$, see [14, Chapter 3]. Note that p^s-polynomials are, in a sense, the wildest polynomials, as the exponent of each term is a power of the characteristic. Even more important here, the class of all p^s-polynomials over $\mathbb{F}_q$ is closed under composition.

Let $L \in \mathbb{F}_q[X]$ be a p^s-polynomial and d be a divisor of $p^s - 1$. Then $L(X) = XM(X^d)$ for some $M \in \mathbb{F}_q[X]$. The polynomial $S(X) = XM^d(X)$ is called a *sub-linearised polynomial*, or, more precisely, a *(p^s, d)-polynomial* and is said to be *associated* with L (simply, the polynomials L and S are associated if and only if $L^d(X) = S(X^d)$). Note that p^s-polynomials are $(p^s, 1)$-polynomials but the distinction is important when one considers the additional properties satisfied by p^s-polynomials. However, a result of Henderson and Matthews [11] shows that the compositional behaviour of (p^s, d)-polynomials is in one-to-one correspondence with the compositional behaviour of p^s-polynomials. It follows that any results concerning the theory of decompositions of p^s-polynomials as p^s-polynomials is relevant to (p^s, d)-polynomials. Given our aim is to determine the number of indecomposable (p^s, d)-polynomials the distinction between p-polynomials and p^s-polynomials will be key in what follows. Results and further references on (p^s, d)-polynomials can be found in [11].

Section 2 gives an in-depth discussion of compositions of p^s-polynomials, and hence (p^s, d)-polynomials. Utilising earlier work of Odoni [15], we then determine a formula for the number of indecomposable p^s-polynomials, and hence (p^s, d)-polynomials, of given arbitrary degree. In the final section, we consider Ritt's Theorem and show how to extend current decomposition algorithms to provide decompositions of (p^s, d)-polynomials for no asymptotic cost.

2. The ring A_s and its properties

The following result connects the compositional behaviour of the two classes of polynomials considered in this article.

Theorem 2.1 ([11, Theorem 4.1]). *Let L be a p^s-polynomial with associated (p^s, d)-polynomial S. The polynomial $L = L_1(L_2)$ for p^r-polynomials $L_1, L_2 \in \mathbb{F}_q[X]$ where r divides s and d divides $p^r - 1$ if and only if $S = S_1(S_2)$ for (p^r, d)-polynomials S_1, S_2 where $L_i^d(X) = S_i(X^d)$, $i = 1, 2$. Also, $L_1^d(L_2(X)) = S_1(S_2(X^d))$.*

By appealing to this theorem, our results can be determined by simply considering p^s-polynomials. However, there is one distinction in the decomposition behaviour of p^s-polynomials and (p^s, d)-polynomials important to our task: a p^s-polynomial may be indecomposable as a p^s-polynomial, but still be decomposable as a p^r-polynomial for some integer r dividing s. This can not be true for the associated (p^s, d)-polynomial unless d divides $p^r - 1$. We will return to this point later but for now it is enough to realise that we need to consider the indecomposable p^s-polynomials where

J. Austral. Math. Soc. 76 (2004), 317-328

the decomposition factors are restricted to the same set (in other words they are p^s-polynomials themselves).

Let A_s be the set of all p^s-polynomials over $\mathbb{F}_q$. It is easily seen that A_s is closed under addition and composition of polynomials and that the triple $(A_s, +, \circ)$ forms a non-commutative ring. Throughout we use A_s to denote the ring $(A_s, +, \circ)$. It is possible to relate decompositions in A_s to factorisations in a non-commutative polynomial ring, known as a skew-polynomial ring. This connection has been used elsewhere (e.g. [10]). Let σ be an automorphism of $\mathbb{F}_q$. Then we must have $\sigma(a) = \sigma_s(a) = a^{p^s}$ for some integer s. Construct the skew-polynomial ring $\mathbb{F}_q[X; \sigma_s]$ consisting of polynomials in the indeterminate X where for $f, g \in \mathbb{F}_q[X; \sigma_s]$ given by $f(X) = \sum_{i=0}^{t_1} \alpha_i X^i$, $g(X) = \sum_{i=0}^{t_2} \beta_i X^i$ their addition is performed in the usual way, and their multiplication is given by

$$f(X)g(X) = \sum_{i=0}^{t_1+t_2} h_i X^i$$

where $h_i = \sum_{j+k=i} \alpha_j \sigma_s^j(\beta_k)$. It is easily seen that the mapping $\Phi_s : A_s \to \mathbb{F}_q[X, \sigma_s]$ given by

$$\Phi_s(L(X)) = \Phi_s\left(\sum_{i=0}^{t} a_i X^{p^{si}}\right) = \sum_{i=0}^{t} a_i X^i$$

is a ring isomorphism. In [16, 17] Ore considers more general skew polynomial rings than the one described here and notes in [17] that A_1 is isomorphic to $\mathbb{F}_q[X, \sigma_1]$.

We give an exposition of the properties of A_s in terms of composition, as this enables direct interpretation of compositional behaviour. We loosely follow the discussion given in [15] for A_1, as later we shall be interested in generalising a result from there. It should be noted that, ignoring context, the general content of this section is not new and can be found in a number of texts covering skew-polynomial rings, such as [12, Chapter 1].

The ring A_s has no zero divisors; if $f \circ g = 0$ for $f, g \in A_s$, then at least one of f or g must be identically zero. With respect to composition, the identity element is X and the units (invertible elements) are aX where $a \in \mathbb{F}_q^*$. As A_s is a non-commutative ring we distinguish between right and left ideals (it is easily seen that the right and left ideals of A_s are generally distinct). In [17] a version of Euclid's division algorithm is given that holds for a general skew-polynomial ring, and so for A_s as well. Precisely, for $L_1, L_2 \in A_s$ there exist $f, g \in A_s$ where $L_1(X) = f(X) \circ L_2(X) + g(X)$ and $\deg(g) < \deg(L_2)$. It follows that A_s is a left Principal Ideal Domain (PID). We will mainly consider left ideals of A_s but note that as σ_s is an automorphism of $\mathbb{F}_q$, A_s is also a right PID [12, Proposition 1.1.14], and so our statements shall also hold for right ideals of A_s. Throughout, an ideal is a left ideal unless otherwise stated.

We represent left ideals in A_s with angle brackets as follows:

$$\langle L \rangle = A_s \circ L = \{f \circ L \,:\, f \in A_s\}.$$

The ideal $\langle L \rangle$ is a maximal left ideal of A_s if and only if $L \in A_s$ is indecomposable (in this case there is also a maximal right ideal of A_s generated by L). Set $k = \gcd(s, e)$, and $m = \mathrm{lcm}(s, e) = se/k$. It is readily seen that the centre, C_s, of the ring A_s consists of polynomials of the shape

$$f(X) = \sum_{i=0}^{n} a_i X^{p^{mi}}$$

J. Austral. Math. Soc. 76 (2004), 317-328

where $a_i \in \mathbb{F}_{p^k}$. In fact, under the isomorphism Φ_s we see that C_s is indeed isomorphic to the centre of $\mathbb{F}_q[X, \sigma_s]$, namely $\mathbb{F}_{p^k}[X^{m/s}, \sigma_s]$. The ring $\mathbb{F}_{p^k}[X^{m/s}, \sigma_s]$ is in turn isomorphic to the ordinary multiplicative polynomial ring $\mathbb{F}_{p^k}[Y]$ ($Y = X^{m/s}$). So C_s is a commutative PID whose maximal ideals coincide with the irreducible polynomials of $\mathbb{F}_{p^k}[Y]$. From [14, Theorem 3.25], the number of monic irreducibles of degree d in $\mathbb{F}_{p^k}[Y]$ is given by

$$N_{p^k}(d) = \frac{1}{d} \sum_{i|d} \mu(d/i)(p^k)^i \tag{2}$$

where $\mu : \mathbb{N} \mapsto \mathbb{N}$ is the Moebius function. Thus $N_{p^k}(d)$ is the number of indecomposables of degree p^{md} in C_s. This formula will be useful when determining the number of indecomposables in A_s of given degree.

Next we consider the division rings constructed from A_s and C_s. We show that we have a special case: the division ring constructed from A_s is a finite dimensional vector space over its centre, and this centre is the division ring constructed from C_s. These constructions are considered elsewhere [12] but are included here for the convenience of the reader and because we work with the ring A_s (rather than $\mathbb{F}_q[X, \sigma_s]$).

As C_s is an integral domain, the smallest field containing C_s is the field of fractions:

$$F = \{g^{-1} \circ f \mid f, g \in C_s, g \neq 0\}. \tag{3}$$

The addition of two elements of F is calculated in the normal way and as F is an ordinary (commutative) field of fractions $g^{-1} \circ f = f \circ g^{-1}$ (which is determined using the Euclidean algorithm).

Embeddings of non-commutative rings into division rings do not always exist but we are fortunate as for A_s this can be done. For any two non-zero elements $f, g \in A_s$, the intersection of the ideals they generate, $\langle f \rangle \cap \langle g \rangle$, is non-empty as the existence of a left least common composition (analogous to the least common multiple) for f and g is guaranteed by the left Euclidean algorithm for A_s. Suppose $h \in A_s$ is the unique monic polynomial of least degree satisfying $h = f_1 \circ f = g_1 \circ g$ for $f_1, g_1 \in A_s$. It follows that $g \circ f^{-1} = g_1^{-1} \circ f_1$ (in this case A_s is said to satisfy the Ore condition). Thus, as A_s has no zero divisors, we have satisfied the conditions of [2, Theorem 1.2.2] and can construct the ring of fractions, D of A_s, given by

$$D = \{g^{-1} \circ f \mid f, g \in A_s, g \neq 0\}. \tag{4}$$

For $g^{-1} \circ f, g_1^{-1} \circ f_1 \in D$, in the standard way

$$g^{-1} \circ f + g_1^{-1} \circ f_1 = h^{-1} \circ (h_1 \circ f + h_2 \circ f_1)$$

where $h = h_1 \circ g = h_2 \circ g_1$ for some $h_1, h_2 \in A_s$, and their composition is given by

$$(g^{-1} \circ f) \circ (g_1^{-1} \circ f_1) = (m \circ g)^{-1} \circ (m_1 \circ f_1) \tag{5}$$

where $m \circ f = m_1 \circ g_1$ for some $m, m_1 \in A_s$. From this point, it is readily shown that these operations are well defined.

We will need the following properties of D, F, A_s and C_s in Section 3. As we will be using results from [18], we follow the definitions given therein.

J. Austral. Math. Soc. 76 (2004), 317-328

Lemma 2.2. *Let F be the field of fractions of C_s (given by (3)) and D be the ring of fractions of A_s (given by (4)). The following conditions hold for F, D, C_s and A_s.*
(i) F is a global field and C_s a Dedekind domain.
(ii) D is a simple central F-algebra of dimension $(e/k)^2$.
(iii) A_s is a maximal C_s-order in D.

Proof. (i) As F is isomorphic to $\mathbb{F}_{p^k}(T)$, from [18, Section 4e] F is a global field. As C_s is isomorphic to $\mathbb{F}_{p^k}[X]$ (a commutative PID), from [18, Section 4a] C_s is a Dedekind domain.

(ii) Following [18, Section 7b] we must show that D is a simple finite dimensional F-algebra where F is the centre of D. We first show that F is the centre of D. Recall $g^{-1} \circ f = f \circ g^{-1}$ for $f, g \in C_s$. For each $h \in A_s$, there exists $h_1 \in A_s$ such that $h \circ h_1 \in C_s$. Then for $g \in C_s$, $g^{-1} \circ (h \circ h_1) = (h \circ h_1) \circ g^{-1}$. Composing on the right with g and using the fact $g \in C_s$ we obtain

$$\begin{aligned} h \circ h_1 &= g^{-1} \circ (h \circ h_1) \circ g \\ &= (g^{-1} \circ h) \circ (g \circ h_1). \end{aligned}$$

Now composing on the right with $(g \circ h_1)^{-1}$ we have $h \circ g^{-1} = g^{-1} \circ h$, and its inverse $g \circ h^{-1} = h^{-1} \circ g$, for all $g \in C_s$ and $h \in A_s$. From these identities and the multiplication rule for D (5) it follows that F is the centre of D.

It is a simple matter to show that D is a left and right F-module. Also, from (5), $a \circ (b \circ c) = (a \circ b) \circ c = b \circ (a \circ c)$ for all $a \in F$ and $b, c \in D$. Therefore D is a F-algebra. As D is a division ring it only contains trivial ideals and so D is a simple F-algebra.

We now proceed to show that D is a F-vector space of dimension $(e/k)^2$. As we have noted above, for every $h \in A_s$ there exists $h_1 \in A_s$ such that $h \circ h_1 \in C_s$. So the elements of D may be written as $g^{-1} \circ f$ where $g \in C_s$. It follows that the number of elements in a basis for D over F is equal to the number of elements in a basis for A_s over C_s. Set $\delta = e/k$. Take the normal basis for $\mathbb{F}_q$ over $\mathbb{F}_{p^k}$ generated by the element $\alpha \in \mathbb{F}_q$, namely $(\alpha, \alpha^{p^k}, \dots, \alpha^{p^{(\delta-1)k}})$. Then every element $\beta \in \mathbb{F}_q$ has a unique representation

$$\beta = b_0\alpha + \cdots + b_{\delta-1}\alpha^{p^{(\delta-1)k}}$$

with $b_0, \dots, b_{\delta-1} \in \mathbb{F}_{p^k}$. Let S be the set

$$S = \{\alpha_i X^{p^{sj}} \mid 0 \le i < \delta,\ 0 \le j < \delta\}.$$

Each element $f \in A_s$ can be uniquely written as

$$f(X) = g_0(X) \circ \alpha_0 X + \cdots + g_{\delta-1}(X) \circ \alpha_{\delta-1} X^{p^{(\delta-1)k}}$$

where $g_0, \dots, g_{\delta-1} \in C_s$. Thus A_s is a free C_s-module with basis S containing $\delta^2 = (e/k)^2$ elements.

(iii) Following the definition given in [18, Section 8] A_s is a C_s-order in the F-algebra D as A_s is a finitely generated C_s-module such that $D = F \cdot A_s$. Note that every element in D can be written as $(g_1^{-1} \circ f_1) \circ f$ where $f \in A_s$ and $f_1, g_1 \in C_s$. It is now not difficult to see that A_s is the integral closure of C_s in D and so is the unique maximal C_s-order in D (see [18, page 110]). $\square$

Note that in the above proof our methods have differed somewhat from those used in [15].

3. Counting indecomposable sub-linearised polynomials

In [15] a formula is given for the number of indecomposable p-polynomials of given degree over $\mathbb{F}_q$. By extending these results to cover p^s-polynomials we can apply Theorem 2.1 to give a formula for the number of indecomposable (p^s, d)-polynomials of given degree over $\mathbb{F}_q$ where s is the least positive integer such that d divides $p^s - 1$ (we can say this without loss of generality as in the cases where d does divide $p^r - 1$ for a proper divisor r of s we can instead consider S to be a (p^r, d)-polynomial). We remind the reader that we are concerned with the ring A_s and when we say $L \in A_s$ is indecomposable we mean L is indecomposable over A_s.

Theorem 3.1. *Let $\mathbb{F}_q$ be a finite field of order $q = p^e$, $k = (e, s)$, and*

$$\mathcal{N}_t = \#\{L \in A_s : \deg(L) = p^{st} \text{ and } L \text{ is indecomposable in } A_s\}.$$

Then $\mathcal{N}_1 = q(q-1)$ and for $t \geq 2$,

$$\mathcal{N}_t = \frac{(q-1)(q^t-1)}{t(p^{tk}-1)} \sum_{i|t} \mu(t/i)(p^k)^i.$$

Further, if s is the least positive integer such that d divides $p^s - 1$, then the number of indecomposable (p^s, d)-polynomials of degree p^{st} is given by $\mathcal{N}_t$.

Proof. If $t = 1$, then for all $a_0 \in \mathbb{F}_q$ and for all $a_1 \in \mathbb{F}_q^*$, $L(X) = a_1 X^{p^s} + a_0 X$ is obviously indecomposable (as p^s-polynomials) so $\mathcal{N}_1 = q(q-1)$. For the remainder of the proof we assume $t \geq 2$. Let $L \in A_s$ be indecomposable with degree p^{st}. Let $f \in A_s$ be the unique monic polynomial of least degree such that $h = f \circ L \in C_s$. Then h is indecomposable over C_s (as otherwise we would contradict our assumption that L is indecomposable and f has least degree). So to count the number of indecomposables $L \in A_s$ of degree p^{st}, we can count the number of indecomposables $h \in C_s$ generated in this way (which in turn shall mean determining their degrees) and the number of distinct $L \in A_s$ that generate the same polynomial h. To do this we use properties of certain ideals of A_s and C_s generated from an indecomposable $L \in A_s$.

As $L \in A_s$ is indecomposable, $\langle L \rangle$ is a maximal left ideal of A_s. The elements of the quotient ring $A_s / \langle L \rangle$ are

$$f(Z) = \sum_{i=0}^{t-1} b_i Z^{p^{si}}$$

where $b_i \in \mathbb{F}_q$ and the degree of f is less than the degree of L. Therefore, $A_s/\langle L \rangle$ is a $\mathbb{F}_q$-vector space of dimension t with q^t elements.

Put $\mathfrak{p} = \langle L \rangle \cap C_s$. Then $\mathfrak{p}$ is a maximal ideal of C_s containing polynomials $f \circ L$ for $f \in A_s$ such that $f \circ L \in C_s$. Let $h \in A_s$ be the unique monic polynomial of least degree such that $h \in \mathfrak{p}$. Then $A_s \mathfrak{p} = \mathfrak{p} A_s = \langle h \rangle$. The elements of the annihilator, $\mathfrak{P} = \operatorname{ann}_{A_s}(A_s/\langle L \rangle)$, of the A_s-module $A_s/\langle L \rangle$, are given by

$$\mathfrak{P} = \{f \circ g \,:\, f \in A_s, g \in C_s, \text{ where } g = g_1 \circ L \text{ for } g_1 \in A_s\}.$$

It follows that $\mathfrak{P}$ is a two-sided maximal ideal of A_s contained in $\langle L \rangle$. Note also $\mathfrak{p} = \mathfrak{P} \cap C_s$ and $\mathfrak{P} = \mathfrak{p} A_s = \langle h \rangle$. By [18, Theorem 22.15] and Lemma 2.2 above, each maximal left ideal of A_s

determines a unique (two-sided) prime ideal $\mathfrak{P}$ and vice versa (as A_s is a PID, its prime ideals and maximal ideals coincide).

It is established in the proof of [18, Theorem 22.15] that $A_s/\mathfrak{P}$ is a simple artinian ring. In our case it is also finite. From [18, Theorem 7.4,7.24] it follows that $A_s/\mathfrak{P}$ is isomorphic to an algebra of $\kappa \times \kappa$ matrices over the finite field $\mathbb{F}_Q$ of Q elements, $M_\kappa(\mathbb{F}_Q)$ (here κ is the capacity of $\mathfrak{P}$ as defined on page 213 of [18]). On the other hand, $A_s/\mathfrak{P}$ is isomorphic to $(A_s/\langle L\rangle)^\kappa$ (see the proof of [18, Corollary 24.8]). As $A_s/\langle L\rangle$ has q^t elements, we have

$$(A_s : \mathfrak{P}) = (A_s : \langle L\rangle)^\kappa = (q^t)^\kappa = Q^{\kappa^2}$$

where $(G : H)$ denotes the index of a subgroup H of an additive abelian group G where G/H is finite. From pages 212 and 213 of [18] the inertial degree of $\mathfrak{P}$ is the integer $\mathfrak{f}$ satisfying

$$(A_s : \mathfrak{P}) = (C_s : \mathfrak{p})^{\mathfrak{f}}.$$

From page 215 of [18] $\mathfrak{f} = \kappa e/k$ and it now follows $(C_s : \mathfrak{p}) = p^{tk}$. Put $\delta = e/k$. From the proof of part (ii) of Lemma 2.2, A_s is a free C_s-module of rank δ^2 so that $(A_s : \mathfrak{p}\, A_s) = (C_s : \mathfrak{p})^{\delta^2}$. Since $\mathfrak{p}\, A_s = \mathfrak{P}$ we have

$$(A_s : \mathfrak{P}) = (C_s : \mathfrak{p})^{\delta^2}.$$

Therefore $\mathfrak{f} = \delta^2$, $\kappa = \delta$ and $Q = p^{tk}$. Now everything is in place to complete the proof.

By inspection of the above arguments we see that

$$\mathcal{N}_t = \sum_{(C_s:\mathfrak{p})=p^{kt}} \mathcal{N}_{(t,k,\mathfrak{p})}$$

where $\mathcal{N}_{(t,k,\mathfrak{p})}$ is the number of indecomposables $L \in A_s$ such that $\deg(L) = p^{st}$ $(t > 1)$ and $C_s \cap \langle L\rangle = \mathfrak{p}$. Recall $\mathfrak{p}$ generates the unique maximal two-sided ideal of A_s, namely $\mathfrak{P} = \mathfrak{p}A_s$. Since maximal two-sided ideals $\mathfrak{P}$ in A_s correspond to maximal left ideals in $A_s/\mathfrak{P}$ and units are not counted in $A_s/\mathfrak{P}$, we obtain

$$\mathcal{N}_{(t,k,\mathfrak{p})} = (q-1)\#\{\text{maximal left ideals in } M_\kappa(\mathbb{F}_{p^{kt}})\}.$$

Since $\mathcal{N}_{(t,k,\mathfrak{p})}$ does not depend on the choice of $\mathfrak{p}$, we can consider instead $\mathcal{N}_t = (q-1)G_tM_t$ where

$$G_t = \#\{\text{maximal ideals } \mathfrak{p} \subset C_s \text{ where } (C_s : \mathfrak{p}) = p^{kt}\}$$

and

$$M_t = \#\{\text{maximal left ideals in } M_\kappa(\mathbb{F}_{p^{kt}})\}.$$

Since G_t is the number of indecomposables $g \in C_s$ of degree p^{mt} it can be determined using Equation (2) (it is easily seen that if $g \in C_s$ with $\deg(g) = p^{mt}$, then there are $(p^k)^t$ elements in the factor ring $C_s/\langle g\rangle$). Put $\Lambda = M_\kappa(\mathbb{F}_{p^{kt}})$. Then Λ is a simple central $\mathbb{F}_{p^{kt}}$-algebra. The maximal ideals of Λ are generated by $M \in \Lambda$ with $\mathrm{rank}(M) = (\kappa - 1)$ or, equivalently, the $(\kappa-1)$-dimensional subspaces of the vector space $(\mathbb{F}_{p^{kt}})^\kappa$. It follows that $M_t = (p^{tk\kappa} - 1)/(p^{tk} - 1)$. The value of $\mathcal{N}_t$ is now determined. That the number of indecomposable (p^s, d)-polynomials of degree p^{st} is given by $\mathcal{N}_t$ follows from Theorem 2.1. □

It is easily checked that for p-polynomials this result coincides with [15, Theorem 1]. We have confirmed the result for small values of p, e, s and t through direct computation using the algebra package MAGMA [1].

J. Austral. Math. Soc. 76 (2004), 317-328

4. Tame behaviour of two wild classes

For the field of complex numbers, Ritt [19] has shown that the complete decomposition of a polynomial is unique in the following sense: if we have two complete decompositions of a polynomial f

$$
\begin{aligned}
f &= f_1 \circ \cdots \circ f_m \\
&= g_1 \circ \cdots \circ g_n,
\end{aligned}
$$

then $m = n$ and $\deg(f_i) = \deg(g_{\pi(i)})$ for some permutation π of $\{1, \ldots, m\}$. Engstrom [6] and Levi [13] extended this to any field of characteristic zero. The behaviour for polynomials over a finite field is less simple and has generally been split into two cases. Fried and MacRae [7] established that Ritt's Theorem holds for tame polynomials over a finite field $\mathbb{F}_q$. By giving an example, Dorey and Whaples [5] established that Ritt's Theorem does not hold for wild polynomials (the example used a class of wild polynomials not considered here).

While it is true that Ritt's Theorem does not hold for wild polynomials in general, the two classes considered in this article, p^s-polynomials and (p^s, d)-polynomials, do satisfy Ritt's Theorem. It is implicit in the work of Ore [16, 17] that A_s satisfies Ritt's Theorem (as Ore shows that A_s is a PID). Now Theorem 2.1 tells us that (p^s, d)-polynomials must also satisfy Ritt's Theorem. It is conceivable that no other classes of wild polynomials not contained in these classes satisfy Ritt's Theorem.

The polynomial decomposition problem introduced by Ritt now receives attention mainly through the development of efficient decomposition algorithms. Algorithms for decomposing p^s-polynomials and (p^s, d)-polynomials can be developed by extending existing algorithms. We end the article by outlining how this may be achieved without asymptotic cost. We consider the following two decomposition problems from [3].

The complete decomposition problem: given a $f \in \mathbb{F}_q[X]$, find indecomposable $f_1, \ldots, f_m \in \mathbb{F}_q[X]$ such that $f = f_1 \circ \cdots \circ f_m$.

The bi-decomposition problem: given a $f \in \mathbb{F}_q[X]$ and $n \in \mathbb{N}$ where $n < \deg(f)$, determine if there exist $f_1, f_2 \in \mathbb{F}_q[X]$ such that $f = f_1 \circ f_2$ and $\deg(f_2) = n$, and if so, find f_1, f_2.

An algorithm for the complete factorisation of $f \in \mathbb{F}_q[X, \sigma_s]$ is given in [10, Section 3] and an algorithm for the bi-factorisation of $f \in \mathbb{F}_q[X, \sigma_s]$ is given in [10, Section 4]. In [3] it is shown how these results can be extended to (p, d)-polynomials using Theorem 2.1. Given the isomorphism between A_s and $\mathbb{F}_q[X, \sigma_s]$, it is clear that the scope of Giesbrecht's algorithms can be extended to decompose p^s-polynomials and (p^s, d)-polynomials. We give simple descriptions of algorithms for our decomposition problems in the case of (p^s, d)-polynomials.

Algorithm 1: Complete decomposition
Input: A (p^s, d)-polynomial $S \in \mathbb{F}_q[X]$ and the integers s and d.
Output: Indecomposable (p^r, d)-polynomials $S_1, \ldots, S_k \in \mathbb{F}_q[X]$ where r divides s and $S = S_1 \circ \cdots \circ S_k$.

1. Determine the least positive integer r such that r divides s and d divides $p^r - 1$.
2. Convert S to a p^r-polynomial L.

3. Convert L to a polynomial $f \in \mathbb{F}_q[X, \sigma_r]$ using the isomorphism Φ_r.
4. Find irreducibles $f_1, \ldots, f_k \in \mathbb{F}_q[y, \sigma_r]$ satisfying $f = f_1 \cdots f_k$ using the algorithm from Section 3 of [10].
5. Convert each $f_i \in \mathbb{F}_q[y, \sigma_r]$ into a p^r-polynomial using Φ_r^{-1}.
6. Convert each p^r-polynomial into a (p^r, d)-polynomial.

Algorithm 2: Bi-decomposition
Input: A (p^s, d)-polynomial $S \in \mathbb{F}_q[X]$, say $S(X) = X(\sum_{i=0}^{m} a_i X^{(p^s i-1)})^d$, the integers s and d, and an integer $n = p^t$.
Output: A pair of (p^k, d)-polynomials $S_1, S_2 \in \mathbb{F}_q[X]$ where k divides s, d divides $p^k - 1$ and $S = S_1 \circ S_2$, or a message that no such bi-decomposition exists.

1. Determine the integer $k = \gcd(sm, t)$. If d does not divide $p^k - 1$, then return "S has no such bi-decomposition".
2. Convert S to a p^k-polynomial L.
3. Convert L to a polynomial $f \in \mathbb{F}_q[y, \sigma_k]$ using the isomorphism Φ_k.
4. Use the bi-factorisation algorithm from Section 4 of [10] to determine if there exist $f_1, f_2 \in \mathbb{F}_q[X, \sigma_k]$ satisfying $f = f_1 f_2$ and $\deg(f_2) = t$. If no suitable polynomials exist, then return "S has no such bi-decomposition".
5. Convert $f_1, f_2 \in \mathbb{F}_q[X, \sigma_k]$ to p^k-polynomials L_1, L_2 using Φ_k^{-1}.
6. Convert L_1, L_2 to (p^k, d)-polynomials S_1, S_2. Return S_1, S_2.

The conversion algorithms from a (p^s, d)-polynomials to a p^s-polynomial and the reverse are found in [3]. The conversion algorithm from a p^s-polynomial L to a polynomial $f \in \mathbb{F}_q[X, \sigma_s]$ is $O(m)$ where $\deg(L) = p^{ms}$ (i.e. L has m terms). The reverse conversion has the same cost. We note that step 1 in the first algorithm and steps 1 and 2 in the second algorithm are the only additional steps required which affect the complexity analysis from [3]. Step 1 (Algorithm 1) has cost $O(s \log s)$ while step 1 (Algorithm 2) has cost bounded by $O(\text{Cost for} \gcd(sm, t))$. Combining our arguments with those of [3] shows that the extension of the deterministic algorithms for factorisation in skew polynomial rings $\mathbb{F}_q[X, \sigma_s]$ from [10] to (p^s, d)-polynomials is asymptotically free. As reported in [4], these algorithms have been successfully implemented.

References

[1] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. **24** (1997), 235–265.

[2] P.M. Cohn, *Skew Field Constructions*, London Mathematical Society Lecture Note Series, vol. 27, Cambridge University Press, 1977.

[3] R.S. Coulter, G. Havas, and M. Henderson, *Functional decomposition of a class of wild polynomials*, J. Combin. Math. Combin. Comput. **28** (1998), 87–94.

[4] ———, *Giesbrecht's algorithm, the HFE cryptosystem and Ore's p^s-polynomials*, Computer Mathematics: Proceedings of the Fifth Asian Symposium (ASCM 2001) (K. Shirayanagi and K. Yokoyama, eds.), Lecture Notes Series on Computing, vol. 9, World Scientific, 2001, pp. 36–45.

[5] F. Dorey and G. Whaples, *Prime and composite polynomials*, J. Algebra **28** (1974), 88–101.

[6] H.T. Engstrom, *Polynomial substitutions*, Amer. J. Math. **63** (1941), 249–255.

[7] M.D. Fried and R.E. MacRae, *On the invariance of chains of fields*, Illinois J. Math. **13** (1969), 165–171.

[8] J. von zur Gathen, *Functional decomposition of polynomials: the tame case*, J. Symbolic Computation **9** (1990), 281–299.

[9] ———, *Functional decomposition of polynomials: the wild case*, J. Symbolic Computation **10** (1990), 437–452.

[10] M. Giesbrecht, *Factoring in skew-polynomial rings over finite fields*, J. Symbolic Comput. **26** (1998), 463–486.

[11] M. Henderson and R. Matthews, *Composition behaviour of sub-linearised polynomials over a finite field*, Finite Fields: Theory, Applications and Algorithms (R.C. Mullin and G.L. Mullen, eds.), Contemporary Mathematics, vol. 225, American Mathematical Society, 1999, pp. 67–75.

[12] N. Jacobson, *Finite-dimensional division algebras over fields*, Springer, Berlin, New York, 1996.

[13] H. Levi, *Composite polynomials with coefficients in an arbitrary field of characteristic zero*, Amer. J. Math. **64** (1942), 389–400.

[14] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl., vol. 20, Addison-Wesley, Reading, 1983, (now distributed by Cambridge University Press).

[15] R.W.K. Odoni, *On additive polynomials over a finite field*, Proc. Edinburgh Math. Soc. **42** (1999), 1–16.

[16] O. Ore, *On a special class of polynomials*, Trans. Amer. Math. Soc. **35** (1933), 559–584, Errata, *ibid.* **36**, 275 (1934).

[17] ———, *Theory of non-commutative polynomials*, Annals of Math. **34** (1933), 480–508.

[18] I. Reiner, *Maximal Orders*, London Mathematical Society Monographs, vol. 5, Academic Press, 1975.

[19] J.F. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc. **23** (1922), 51–66.

[20] A. Schinzel, *Polynomials with Special Regard to Reducibility*, Encyclopedia of Mathematics and Its Applications, vol. 77, Cambridge University Press, 2000.

Department of Mathematical Sciences
University of Delaware
Newark, DE 19716-2553
Australia
e-mail: coulter@math.udel.edu
marie@math.udel.edu

Centre for Discrete Mathematics
and Computing
School of Information Technology
and Electrical Engineering
The University of Queensland
Qld 4072
Australia
e-mail: havas@itee.uq.edu.au

J. Austral. Math. Soc. 76 (2004), 317-328