J. Austral. Math. Soc. (*Series A*) **49** (1990), 309–318

THE FACTORABLE CORE OF POLYNOMIALS OVER FINITE FIELDS

S. D. COHEN

(Received 16 May 1989; revised 2 October 1989)

Communicated by R. Lidl

Abstract

For a polynomial $f(x)$ over a finite field $\mathbf{F}_q$, denote the polynomial $f(y)-f(x)$ by $\varphi_f(x, y)$. The polynomial φ_f has frequently been used in questions on the values of f. The existence is proved here of a polynomial F over $\mathbf{F}_q$ of the form $F = L^r$, where L is an affine linearized polynomial over $\mathbf{F}_q$, such that $f = g(F)$ for some polynomial g and the part of φ_f which splits completely into linear factors over the algebraic closure of $\mathbf{F}_q$ is exactly φ_F. This illuminates an aspect of work of D. R. Hayes and Daqing Wan on the existence of permutation polynomials of even degree. Related results on value sets, including the exhibition of a class of permutation polynomials, are also mentioned.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*) (1985 *Revision*): 11 T 06.

1. Introduction

Let $f(x)$ be a monic polynomial in $\mathbf{F}_q[x]$, where $\mathbf{F}_q$ is the finite field of prime power order $q = p^m$. (Without loss, we shall assume throughout that f is separable, that is, $f(x) \notin \mathbf{F}_q[x^p]$.) Questions relating to the value set of f in $\mathbf{F}_q$ (for example, whether f is a permuation polynomial on $\mathbf{F}_q$) have frequently been tackled by consideration of the polynomial $\varphi_f(x, y)$ defined by $\varphi_f(x, y) = f(y) - f(x)$, its factorization over $\mathbf{F}_q$ and any further reducibility over the algebraic closure $\overline{\mathbf{F}}_q$ of $\mathbf{F}_q$ (see [15], Chapter 7, Section 4 and references on pages 379–381, [4], [11], [19], [20], for example).

Of course, $\varphi_f(x, y)$ has the trivial factor $y - x$ and, more generally, if $f = g(h)$, a composition of polynomials in $\mathbf{F}_q[x]$, then, in $\mathbf{F}_q[x, y]$, φ_f is divisible by φ_h. Such factorization aside, the most conspicuous possibility for factors of φ_f in $\overline{\mathbf{F}}_q[x, y]$ are linear ones $y - \zeta x - \alpha$ $(\zeta, \alpha \in \overline{\mathbf{F}}_q)$. Denote by $\lambda_f(x, y)$ the factor of $\varphi_f(x, y)$ (monic in y, say) that is the product of all linear factors in $\overline{\mathbf{F}}_q[x, y]$. Employing some old terminology of Carlitz [3], [16], we say that f or φ_f is *factorable* if $\lambda_f = \varphi_f$, that is, φ_f splits completely into linear factors in $\overline{\mathbf{F}}_q[x, y]$. More generally, we refer to λ_f (actually in $\mathbf{F}_q[x, y]$ by Corollary 2.2 below) as the *factorable part* of φ_f.

Preliminary studies on polynomials f with non-trivial factorable part (that is, having $\deg \lambda_f > 1$) have been undertaken by Hayes [13] and Daqing Wan [20]; see also [11]. Here we describe λ_f for arbitrary f and, in particular, identify all factorable polynomials. In summary, f always possesses a "factorable core", namely a factorable polynomial $F(x)$ in $\mathbf{F}_q[x]$ for which $f = g(F)$ (for some $g(x)$ in $\mathbf{F}_q[x]$) and $\lambda_f = \lambda_F = \varphi_F$. In turn, F is a "cyclic extension of a linearized core" as we proceed now to describe.

To do this, we modify slightly the standard terminology for linearized polynomials—also known as p^s-polynomials, [15, Section 3.4]. For any $s \geq 1$, define a *p^s-polynomial* (over $\mathbf{F}_q$) as one of the form

$$L(x) = \sum_{i=0}^{k} a_i x^{p^{si}} \qquad (a_0, \dots, a_k \in \overline{\mathbf{F}}_p). \tag{1.1}$$

where we note that $\overline{\mathbf{F}}_p = \overline{\mathbf{F}}_q$ and the reference to $\mathbf{F}_q$ is appropriate if the coefficients actually belong to the subfield $\mathbf{F}_q$ of $\overline{\mathbf{F}}_q$. In extension of this, an *affine p^s-polynomial* (over $\mathbf{F}_q$), by definition, is one of the form $L(x) + \alpha$, where L is a p^s-polynomial (over $\mathbf{F}_q$) and $\alpha \in \overline{\mathbf{F}}_p$ (or $\mathbf{F}_q$). Clearly, a p^s-polynomial L is a linear transformation of $\overline{\mathbf{F}}_p$ as an $\mathbf{F}_{p^s}$-vector space. Moreover, if $\zeta \in \mathbf{F}_{p^s}$ and $\alpha \in \overline{\mathbf{F}}_p$, then, identically,

$$L(\zeta x + \alpha) = \zeta L(x) + L(\alpha), \qquad \zeta \in \mathbf{F}_{p^s}, \alpha \in \overline{\mathbf{F}}_p. \tag{1.2}$$

To introduce cyclic extensions, given an affine p^s-polynomial $L(x) + \alpha$, and $r \geq 1$, set $F(x) = (L(x) + \alpha)^r$, and let ζ be a primitive rth root of unity in $\overline{\mathbf{F}}_p$. Then, provided $r \mid (p^s - 1)$ if $\deg L > 1$ (so that $\zeta \in \mathbf{F}_{p^s}$), it follows from (1.2) that

$$\begin{aligned}\varphi_F(x, y) &= \prod_{i=0}^{r-1} \{(L(y) + \alpha) - \zeta^i (L(x) + \alpha)\} \\ &= \prod_{i=0}^{r-1} \{L(y - \zeta^i x) + \alpha(1 - \zeta^i)\} = \prod_{i=0}^{r-1} \prod_{\gamma_i} (y - \zeta^i x - \gamma_i),\end{aligned} \tag{1.3}$$

https://doi.org/10.1017/S1446788700030585 Published online by Cambridge University Press

where the inner product in (1.3) is over all roots γ_i of $L(x)+\alpha(1-\zeta^i)=0$. Thus F is factorable. The two theorems we now state and are to prove demonstrate that, in fact, the factorable parts of all polynomials are accounted for by the above.

THEOREM 1.1. *A separable monic polynomial $F(x)$ in $\mathbf{F}_q[x]$ is factorable if and only if $F(x)=L^r(x)+\delta$ where $\delta\in\mathbf{F}_q$ and L is an affine p-polynomial over $\mathbf{F}_q$, with $r\,|\,(p^s-1)$ if L is actually an affine p^s-polynomial of degree exceeding* 1.

THEOREM 1.2. *Let $f(x)$ be a separable monic polynomial in $\mathbf{F}_q[x]$. Then there exists a monic polynomial $g(x)$ and a monic factorable polynomial $F(x)$ in $\mathbf{F}_q[x]$ such that $f=g(F)$ and $\lambda_f=\lambda_F=\varphi_F$.*

In Theorem 1.2 the factorable core F can be specified uniquely with $\delta=0$ in Theorem 1.1 and, additionally, with L a p-polynomial, not affine, if $r=1$.

It was the Carlitz conjecture (see [14]) on the non-existence of permutation polynomials of even degree n over $\mathbf{F}_q$ (q odd) which motivated the present treatment. A proof appears to be difficult when $p\,|\,n$ but, partly aided by consideration of the factorable part, it has been accomplished for $n\leq 16$ by Dickson [9], Hayes [13] and Daqing Wan [20]. In fact, application of our theorems would significantly simplify their arguments and, in principle, allow further cases $n=18, 20, 22, \ldots$ to be solved (notably the case $n=18$, $p=3$, in which $p^2\,|\,n$). We do not, however, incorporate such applications here because there is an alternative viewpoint (that of primitive permutation groups) which has an important bearing on the problem; a further paper is planned with this stance. Nonetheless we shall include some comments on the value sets of factorable polynomials and, in particular, exhibit what seems to be a new class of permutation polynomials.

When f is separable, φ_f is a product of *distinct*, irreducible polynomials in $\overline{\mathbf{F}}_q[x, y]$. If f is inseparable, then $f(x)=f_1(x^{p^b})=f_2^{p^b}(x)$ for some separable $f_1(x)$, $f_2(x)$ in $\mathbf{F}_q[x]$ and evidently we may treat f_2 in place of f. For convenience, therefore, we shall assume that all polynomials in $\overline{\mathbf{F}}_q[x]$ are monic and separable and all polynomials in $\overline{\mathbf{F}}_q[x, y]$ are monic in y.

2. The linearized core

We begin with some generalities. Given an irreducible (for example, linear) polynomial $\rho(x, y)$ in $\overline{\mathbf{F}}_q[x, y]$, let the field obtained by adjoining the

https://doi.org/10.1017/S1446788700030585 Published online by Cambridge University Press

coefficients of ρ to $\mathbf{F}_q$ be $\mathbf{F}_{q^t}$. Define

$$\overline{\rho}(x,y)=\prod_{i=0}^{t-1}\rho(x^{1/q^i},y^{1/q^i})^{q^i}.$$

The following basic result is evident from [3].

LEMMA 2.1. *Let $\rho(x,y)$ be an irreducible polynomial in $\overline{\mathbf{F}}_q[x,y]$ as above. Then $\overline{\rho}(x,y)$ is in $\mathbf{F}_q[x,y]$. Further, if $\rho(x,y)$ is a factor of $\theta(x,y)\in\mathbf{F}_q[x,y]$, then $\overline{\rho}(x,y)$ divides $\theta(x,y)$.*

COROLLARY 2.2. *Given $f(x)\in\mathbf{F}_q[x]$, then $\lambda_f(x,y)\in\mathbf{F}_q[x,y]$. Further, if $\mu_f(x,y)$ is the product of all linear factors of $\lambda_f(x,y)$ of the form $y-x-\alpha$ $(\alpha\in\overline{\mathbf{F}}_q)$, then $\mu_f(x,y)\in\mathbf{F}_q[x,y]$.*

PROOF. Since λ_f and μ_f divide φ_f in $\mathbf{F}_q[x,y]$, Lemma 2.1 can be applied to all their linear factors (in $\overline{\mathbf{F}}_q[x,y]$) and the result follows.

The next crucial fact follows from [10], especially Theorems 2.3 and 4.2, and is a polynomial version of [6, Lemma 4]. In its statement, f, f^*, F, etc., are all monic separable polynomials in $\mathbf{F}_q[x]$.

LEMMA 2.3. *Suppose $\rho(x,y)\in\mathbf{F}_q[x,y]$ divides $\varphi_{f^*}(x,y)$ for some f^*. Then there exists $F(x)$ in $\mathbf{F}_q[x]$ such that, for any f, $\rho(x,y)$ divides $\varphi_f(x,y)$ if and only if $f=h(F)$ for some $h(x)\in\mathbf{F}_q[x]$.*

Linearized polynomials come to the fore in the next lemma ([7, Lemma 4]).

LEMMA 2.4. *Suppose the p-polynomial L over $\mathbf{F}_q$ decomposes functionally over $\mathbf{F}_q$ as $L=L_1(L_2)$. Then $L=L_1^*(L_2^*)$, where $L_1^*(x)=L_1(x+L_2(0))$, $L_2^*(x)=L_2(x)-L_2(0)$ are p-polynomials over $\mathbf{F}_q$.*

With the above preparations, we now demonstrate the existence of a linearized core.

LEMMA 2.5. *Given $f(x)$ in $\mathbf{F}_q[x]$, there exists a p-polynomial $L(x)$ and a polynomial $h(x)$ in $\mathbf{F}_q[x]$ such that $f=h(L)$ and $\mu_f=\mu_L=\lambda_L=\varphi_L$.*

PROOF. By Corollary 2.2 we may take $\rho(x,y)=\mu_f(x,y)$ in Lemma 2.3. Then certainly $\mu_f\mid\varphi_f$. But, also, writing $\mu_f(x,y)=\prod_{i=1}^{j}(y-x-\alpha_i)$, say, and $F_{q^t}=F_q(\alpha_1,\dots,\alpha_j)$ we see that μ_f divides $(y-x)^{q^t}-(y-x)=$

$\varphi_{L^*}(x, y)$, where $L^*(x) = x^{q^t} - x$. It follows from Lemma 2.3 that for some $L(x)$, $L_0(x)$ and $h(x)$ in $\mathbf{F}_q[x]$ with φ_L divisible by μ_f, $f = h(L)$ and $L^* = L_0(L)$. Additionally, by Lemma 2.4, L (as well as L_0) can be assumed to be p-polynomials. From the definition of μ_f and (1.3) (with $r = 1$) we see that $\mu_f = \varphi_L$. This finishes the proof.

3. The cyclic extension

Given r with $p \nmid r$, we now suppose that ζ is a primitive rth root of unity in $\overline{\mathbf{F}}_p$ (a field which we can equally well visualise as $\overline{\mathbf{F}}_q$).

LEMMA 3.1. *Given $f(x)$ in $\mathbf{F}_q[x]$, suppose that $r > 1$ and $y - \zeta x - \alpha$ (where $\alpha \in \overline{\mathbf{F}}_q$) divides φ_f. Then, for each $i = 0, \dots, r-1$, $y - \zeta^i x - \beta(1 - \zeta^i) = y - \beta - \zeta^i(x - \beta)$ divides φ_f, where $\beta = \alpha/(1-\zeta)$. Moreover, for some $g(x)$ in $\overline{\mathbf{F}}_q[x]$, $f(x) = g((x-\beta)^r)$.*

PROOF. The first part is [13, Theorem 5.1]. A simple application of Lemma 2.3 with $\rho(x, y) = \varphi_F(x, y)$, where $F(x) = (x - \beta)^r$, yields the rest.

The vital fact that, in Theorem 1.1, $r \mid (p^s - 1)$ is decided in the next lemma. We continue to work in $\overline{\mathbf{F}}_p[x]$, the argument employed being relevant in the sequel too.

LEMMA 3.2. *Let $f(x)$ be a separable monic polynomial in $\mathbf{F}_q[x]$ whose linearized core $L(x)$ in $\mathbf{F}_q[x]$ has degree greater than 1. Let s be the maximal integer such that L is a p^s-polynomial over $\mathbf{F}_q$. Then the maximal integer r with $p \nmid r$ such that $y - \zeta x - \alpha$ divides φ_f for some primitive rth root of unity ζ in $\overline{\mathbf{F}}_p$, and α in $\overline{\mathbf{F}}_p$ satisfies $r \mid (p^s - 1)$.*

PROOF. We can assume $r > 1$. Suppose that $y - \zeta x - \alpha = y - \beta - \zeta(x - \beta)$, where $\beta = \alpha/(1-\zeta)$, is a factor of φ_f. By Lemma 3.1, $f(x) = g((x-\beta)^r)$, where $g(x) \in \overline{\mathbf{F}}_p[x]$, and, in fact, $y - \beta - \zeta(x - \beta)$ is a factor of φ_f for $i = 0, \dots, r-1$.

As in [20, Lemma 3.1], for instance, we enlist the aid of some $\overline{\mathbf{F}}_p(z)$-automorphisms of $\overline{\mathbf{F}}_p(x)$, where $f(x) = z$, an indeterminate. In the first place, for each $i = 0, \dots, r-1$, there is an automorphism σ_i which maps $x \mapsto \zeta^i(x - \beta) + \beta$ (all these being roots of $f(y) - z$). There are also automorphisms permuting the zeros of μ_f (as a polynomial in y) defined by

https://doi.org/10.1017/S1446788700030585 Published online by Cambridge University Press

$x \mapsto x+\gamma$ for any γ with $L(\gamma)=0$. Application of these maps demonstrates that (independently of i) the number of factors of λ_f of the form $y-\zeta^i x-\alpha$, $i=0,\dots,r-1$, is the same (namely, $\deg L$). Further, operating on the factor $L(y)-L(x)=L(y-x)$ of λ_f with each σ_i in turn, we obtain

$$\lambda_f(x,y)=(L(y)-L(x))\prod_{i=1}^{r-1}L(y-\beta-\zeta^i(x-\beta))$$

$$(3.1)\qquad =(L(y)-L(x))\prod_{i=1}^{r-1}(L(y-\beta)-L(\zeta^i(x-\beta)))$$

$$(3.2)\qquad =\prod_{L(\gamma)=0}\prod_{i=0}^{r-1}(y-\beta-\zeta^i(x-\beta)-\gamma)$$

$$(3.3)\qquad =(L(y)-L(x))\prod_{L(\gamma)=0}\prod_{i=1}^{r-1}\left\{\left(y-\beta-\frac{\gamma}{1-\zeta^i}\right)\right. \left.-\zeta^i\left(x-\beta-\frac{\gamma}{1-\zeta^i}\right)\right\}.$$

Suppose that γ is any root of $L(x)$ (in $\overline{\mathbf{F}}_p$). By (3.3) and Lemma 3.1, for any $i=1,\dots,r-1$, because $(y-\beta-\gamma/(1-\zeta^i))-\zeta^i(x-\beta-\gamma/(1-\zeta^i))$ is a factor of λ_f so also is $(y-\beta-\gamma/(1-\zeta^i))-\zeta^{2i}(x-\beta-\gamma/(1-\zeta^i))$ (where the case $i=r/2$ when r is even needs some special consideration). From (3.2), however, every factor of λ_f of the form $y-\zeta^{2i}x-\alpha$ has the explicit shape $y-\beta-\zeta^{2i}(x-\beta)-\gamma_1$, where $L(\gamma_1)=0$. Consequently, $\gamma_1=(1-\zeta^{2i})\gamma/(1-\zeta^i)=(1+\zeta^i)\gamma$, that is, $L((1+\zeta^i)\gamma)=0$. Hence $L(\zeta^i\gamma)=L((1+\zeta^i)\gamma)-L(\gamma)=0$. Thus, apart from the zero root, whenever γ is a root of L, γ, $\zeta\gamma,\dots,\zeta^{r-1}\gamma$ are all distinct roots of L. Since f is separable the important conclusion that $L(x)/x\in\mathbf{F}_q[x^r]$ results.

To complete the proof suppose L is given by (1.1) with $k\geq 1$ and $a_0a_k\neq 0$ and set $I=\{i\colon 0\leq i\leq k,\, a_i\neq 0\}$. We deduce from the above that $r\,|\,p^{si}-1$ for all $i\in I$. In other words $w\,|\,si$ for all $i\in I$, where w denotes the order of p modulo r. By the definition of I, the highest common factor of the members of I is 1, which implies the fact, equivalent to the stated result, that $w\,|\,s$.

We are now ready to finish the proofs of Theorems 1.1 and 1.2. Let L be the linearized core of f and r be as in Lemma 3.2. We are done if $r=1$; so assume $r>1$. Let $y-\beta-\zeta(x-\beta)$ be a factor of φ_f (as in Lemma 3.1). We assert that actually $L(\beta)\in\mathbf{F}_q$.

To justify this, observe from Lemma 2.1 that $y-\beta^q-\zeta^q(x-\beta^q)$ is also

https://doi.org/10.1017/S1446788700030585 Published online by Cambridge University Press

a factor of φ_f. In turn, Lemma 3.1 yields $y - \beta^q - \zeta(x - \beta^q)$ as another factor (because ζ^q is also a primitive rth root of unity). We therefore have, by (3.2), that $(1 - \zeta)\beta^q = (1 - \zeta)\beta + \gamma$, where $L(\gamma) = 0$. Hence $L((1-\zeta)\beta^q) = L((1-\zeta)\beta) + L(\gamma)$ which implies that $L(\beta^q) = L(\beta)$. Because $L(x) \in \mathbf{F}_q[x]$ then, in fact, $L(\beta^q) = L^q(\beta)$ and our claim is proved.

When $\deg L = 1$ the results are evident from Lemma 3.1. Assume therefore that $\deg L > 1$. The import of Lemma 3.2 is that, for $i = 0, \dots, r-1$, $L(\zeta^i x) = \zeta^i L(x)$ and (3.1) can be written

$$\begin{aligned}\lambda_f(x, y) &= (L(y) - L(x)) \prod_{i=1}^{r-1} (L(y - \beta) - \zeta^i L(x - \beta)) \\ &= L^r(y - \beta) - L^r(x - \beta) = \varphi_F(x, y).\end{aligned}$$

where $F(x) = L^r(x - \beta) = (L(x) - L(\beta))^r$, which proves the results (recall that $L(\beta) \in \mathbf{F}_q$).

4. Further results and remarks

The observations to be made here will not be worked out exhaustively and details of the proofs will largely be left to the reader. The notation and conventions will be as before except that later the prime power q will be redefined.

Suppose that f is a separable monic polynomial of degree exceeding 1 over $\mathbf{F}_q$. By definition [15, Chapter 7, Section 4], f is called *exceptional* over $\mathbf{F}_q$ if every irreducible factor (other than $y - x$) of φ_f in $\mathbf{F}_q[x, y]$ factorises further in $\overline{\mathbf{F}}_q[x, y]$, that is, no irreducible factor in $\mathbf{F}_q[x, y]$ (other than $y - x$) is absolutely irreducible. Every exceptional polynomial over $\mathbf{F}_q$ is a permutation polynomial over $\mathbf{F}_q$ (by [5, Theorem 5], for example), and conversely (at least for large q as a function of $\deg f$) [20, Theorem 2.4].

For the conjecture of Carlitz referred to in the introduction, it suffices to show that, for q odd, there are no exceptional polynomials of even degree. Now a composition $f = g(h)$ of polynomials over $\mathbf{F}_q$ is exceptional (or a permutation polynomial) if and only if both g and h are also exceptional (or permuation polynomials). Thus, for many purposes, the study of exceptional (or permutation) polynomials can be restricted to indecomposable polynomials. As the nature of factorable polynomials in this context is not difficult to determine (see below), it may also be presumed that f has trivial factorable core. In particular, for example, for such an exceptional polynomial of even degree, over $\overline{\mathbf{F}}_q[x, y]$ φ_f must have an odd number (> 1) of factors of some odd degree (> 1). This immediately disposes of the possibility of

https://doi.org/10.1017/S1446788700030585 Published online by Cambridge University Press

exceptional polynomials of degree 12, for instance, (compare [20]) and the principle has potential application to polynomials of higher degree. Nevertheless, for the reason stated in the introduction, we defer further discussion on this specific topic. On the other hand, we now describe all factorable exceptional polynomials. To do this, we set $d = (s, m)$, $s = td$, $m = nd$, and re-define q as p^d.

THEOREM 4.1. *Let t, n be relatively prime integers and $L(x)$ be a separable q^t-polynomial of degree exceeding* 1 *over $\mathbf{F}_{q^n}$ with no non-zero roots in $\mathbf{F}_{q^n}$. Let r be an integer such that $r \mid (q^t - 1)$ but $(r, q-1) = 1$. Then, for any α in $\mathbf{F}_{q^n}$, $(L(x)-\alpha)^r$ is an exceptional and so a permutation polynomial over $\mathbf{F}_{q^n}$.*

In Theorem 4.1, note that the conditions on r imply that $(r, q^n - 1) = 1$. As an interesting corollary we deduce the following class of permutation polynomials over $\mathbf{F}_{q^n}$, which, from [14], seem to be new (at least when $k > 1$).

COROLLARY 4.2. *Let t, n be relatively prime integers and r an integer such that $r \mid (q^t - 1)$ but $(r, q-1) = 1$. Suppose that*

$$M(x) = x^{(q^{tk}-1)/r} + \sum_{i=0}^{k-1} a_i x^{(q^{ti}-1)/r}, \qquad k \geq 1, a_0 \neq 0,$$

is a polynomial in $\mathbf{F}_{q^n}[x]$ with no roots in $\mathbf{F}_{q^n}$. Then $f(x) = xM^r(x)$ is an exceptional and a permutation polynomial over $\mathbf{F}_{q^n}$.

We remark that, for $r > 1$, the polynomial f, though exceptional, is not factorable; the irreducible factors of φ_f in $\overline{\mathbf{F}}_q[x, y]$ (other than $y - x$) all have degree r (from (3.2)). Further (as we hope to discuss fully elsewhere), while not evident from Theorem 4.1, the condition $(r, q-1) = 1$ is not required for Corollary 4.2.

EXAMPLE 1. Take $q = t = 2$, $r = 3$. Define $\mathbf{F}_8$ as $\mathbf{F}_2(\theta)$, where $\theta^3 = \theta + 1$. Put $M(x) = x^5 + (\theta^2 + \theta + 1)x + \theta + 1$ in $\mathbf{F}_8[x]$. Then, over F_8, $M(x) = (x^2 + x + \theta + 1)(x^3 + x^2 + \theta x + 1)$, where the factors are irreducible. It follows from Corollary 4.2 that $xM^3(x)$ is a permutation polynomial over $\mathbf{F}_{2^{3n}}$ for all integers n with $(n, 6) = 1$.

EXAMPLE 2. Take $q = t = 3$, $r = 13$. Put $M(x) = x^{56} - x^2 - 1$. By theoretical reasoning (or calculation) over F_3, M factorises into a product of three irreducible polynomials, namely two of degree 24 and one of degree 8. (In any case [8, Example 2] shows that $x^{28} - x - 1$ is a product of seven irreducible quartics over $\mathbf{F}_{27}$.) It follows that $xM^{13}(x)$ is a permutation polynomial over $\mathbf{F}_{3^n}$ for all n such that $3 \nmid n$ and $8 \nmid n$. (In fact, as noted above, the same conclusion can be drawn when $3 \mid n$ but $8 \nmid n$.)

We note that in this context, as well as the general criterion for a linearized polynomial to be a permutation on pages 361–362 of [15], results such as those in [18], [8], [1] and [2] may also be useful.

At the other extreme from permutation polynomials (as far as the size of the value set is concerned), factorable polynomials F can also be ones whose value set in $\mathbf{F}_q$ has minimal size of approximately $q/\deg f$ (see [17], [19], [12]). This occurs whenever $\varphi_F = \lambda_F$ splits completely into linear factors over $\mathbf{F}_q[x, y]$ itself. In the final result, q denotes what was formerly q^s.

THEOREM 4.3. *Let $L(x)$ be a separable q-polynomial of degree q^k (> 1) over $\mathbf{F}_{q^n}$ and $\alpha \in \mathbf{F}_{q^n}$ be such that $L(x) - \alpha$ splits completely in $\mathbf{F}_{q^n}[x]$. Then, for any divisor r of $q - 1$, the number of distinct values taken by $F(x) = (L(x) - \alpha)^r$ in $\mathbf{F}_{q^n}$ is $((q^{n-k} - 1)/r) + 1$.*

In Theorem 4.3, the “monodromy group of F over $\mathbf{F}_q$”, that is, the Galois group of $F(x) - z$ over $\mathbf{F}_q(z)$, z an indeterminate, is regular as a permutation group on the roots. As hinted at earlier, there clearly could be merit in studying the monodromy group in the general case from the point of view of permutation group theory. There is obviously also scope for further work on the value sets of polynomials encompassing Theorems 4.1 and 4.3 and extended possibly to compositions of factorable polynomials.

References

[1] S. Agou, ‘Sur l’irréductibilité des trinômes $X^{p^r+1} - aX - b$ sur les corps finis $\mathbf{F}_{p^s}$’, *Acta Arith.* **44** (1984), 343–355.

[2] S. Agou, ‘Sur la factorisation des polynòmes $X^{p^{2r}+p^r+1} - aX^{p^r+1} - bX - c$ sur les corps finis $\mathbf{F}_{p^s}$’, *Manuscripta Math.* **58** (1987), 141–154.

[3] L. Carlitz, ‘On factorable polynomials in several indeterminates’, *Duke Math. J.* **2** (1936), 660–670.

[4] L. Carlitz, ‘On the number of distinct values of a polynomial with coefficients in a finite field’, *Proc. Japan Acad.* **31** (1955), 119–120.

[5] S. D. Cohen, ‘The distribution of polynomials over finite fields’, *Acta Arith.* **17** (1970), 255–271.

[6] S. D. Cohen, ‘Uniform distribution of polynomials over finite fields’, *J. London Math. Soc.* (2) **6** (1972), 93–102.

[7] S. D. Cohen, ‘The irreducibility of compositions of linear polynomials over a finite field’, *Compositio Math.* **47** (1982), 149–152.

https://doi.org/10.1017/S1446788700030585 Published online by Cambridge University Press

[8] S. D. Cohen, 'Reducibility of sub-linear polynomials over a finite field', *Bull. Korean Math. Soc.* **22** (1985), 53–56.

[9] L. E. Dickson, 'The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group', *Ann. of Math.* **11** (1897), 65–120 and 161–183.

[10] M. D. Fried and R. E. MacRae, 'On curves with separated variables', *Math. Ann.* **180** (1969), 220–226.

[11] J. Gomez-Calderon and D. J. Madden, 'Polynomials with small value set over finite fields', *J. Number Theory* **28** (1988), 167–188.

[12] J. Gomez-Calderon, 'A note on polynomials with minimal value set over finite fields', *Mathematika* **35** (1988), 144–148.

[13] D. R. Hayes, 'A geometric approach to permutation polynomials over a finite field', *Duke Math. J.* **34** (1967), 293–305.

[14] R. Lidl and G. L. Mullen, 'When does a polynomial over a finite field permute the elements of the field?', *Amer. Math. Monthly* **95** (1988), 243–246.

[15] R. Lidl and H. Niederreiter, *Finite Fields*, (Addision-Wesley, Reading, Massachusetts, 1983). (Now distributed by Cambridge University Press, Cambridge.)

[16] A. F. Long, 'Some theorems on factorable irreducible polynomials', *Duke Math. J.* **34** (1967), 281–291.

[17] W. H. Mills, 'Polynomials with minimal value sets', *Pacific J. Math.* **14** (1964), 225–241.

[18] W. H. Mills, 'The degree of factors of certain polynomials over finite fields', *Proc. Amer. Math. Soc.* **25** (1970), 860–863.

[19] D. A. Mit′kin, 'Polynomials with a minimal value set of values and the equation $f(x) = f(y)$ in a finite prime field', (Russian), *Mat. Zametki* **38** (1985), 3–14, 168.

[20] Daqing Wan, 'On a conjecture of Carlitz', *J. Austral. Math. Soc. Ser. A* **43** (1987), 375–384.

Department of Mathematics
University of Glasgow
University Gardens
Glasgow, G12, 8QW
Scotland

https://doi.org/10.1017/S1446788700030585 Published online by Cambridge University Press