TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 345, Number 2, October 1994

A CLASS OF EXCEPTIONAL POLYNOMIALS

STEPHEN D. COHEN AND REX W. MATTHEWS

ABSTRACT. We present a class of indecomposable polynomials of non prime-power degree over the finite field of two elements which are permutation polynomials on infinitely many finite extensions of the field. The associated geometric monodromy groups are the simple groups $PSL_2(2^k)$, where $k \geq 3$ and odd. (The first member of this class was previously found by P. Müller [17]. This realises one of only two possibilities for such a class which remain following deep work of Fried, Guralnick and Saxl [7]. The other is associated with $PSL_2(3^k)$, $k \geq 3$, and odd in fields of characteristic 3.

1. INTRODUCTION

At points in this introduction and throughout we shall refer to various linear groups for which we follow the nomenclature of [18]. (For convenience, their definitions will be summarised in Section 2).

Let $\mathbf{F}_q$ be the finite field of order q, a power of a prime p, and denote by $\overline{\mathbf{F}_q}$ its algebraic closure. A polynomial f $(\neq f_0^p)$ over $\mathbf{F}_q$ is said to be *exceptional* if it is a permutation polynomial on infinitely many finite extensions of $\mathbf{F}_q$. An equivalent definition that has frequently been used (see [13, Chapter 7], [4], and §4 below) is that every factor $\Theta(X, Y)$ (other than $X - Y$) of the difference polynomial

$$\phi_f(X, Y) = f(X) - f(Y) \tag{1.1}$$

which is irreducible over $\mathbf{F}_q$ becomes reducible over $\overline{\mathbf{F}_q}$, i.e., $\Theta(X, Y)$ is not absolutely irreducible.

The notion of an exceptional polynomial is a strong one but it is important as a source of permutation polynomials, (see [11]). Yet in essence, all known examples derive from two types [4]. The first comprises Dickson (Chebyshev) polynomials and incorporates powers X^n as special cases. The other consists of linearized polynomials (additive on $\overline{\mathbf{F}_q}$) and a class of related polynomials (called 'sublinearized' in [4]). More precisely, a linearized polynomial has the

Received by the editors February 25, 1994 and, in revised form, May 4, 1994.
1991 *Mathematics Subject Classification.* Primary 11T06.
Key words and phrases. Exceptional polynomials, permutation polynomials, finite fields.
This work was done while the first author was visiting the University of Tasmania at Hobart. The visit was supported by a University of Tasmania ARC small grant.

shape

$$L(X) = \sum_{i=0}^{k} a_i X^{p^{si}}, \qquad a_0, \ldots, a_k \in \mathbb{F}_q \tag{1.2}$$

(for some $s \geq 1$) and a sublinearized polynomial $M(X)$ satisfies

$$M(X^d) = L^d(X) \tag{1.3}$$

for some linearized polynomial L and some divisor d of $p^s - 1$. Necessarily, M has degree a power of p.

Exceptional polynomials can be composed to yield further exceptional polynomials and, conversely, the composition factors of an exceptional polynomial over $\mathbb{F}_q$ are themselves indecomposable exceptional polynomials [4]. Thus, for existence questions, it suffices to study indecomposable exceptional polynomials alone.

There is an important connection between the theory of exceptional polynomials and Galois theory (see [6, 7]). Let t be transcendental over $\mathbb{F}_q$ and x be a root of $f(X) - t$ in some algebraic closure of $\mathbb{F}_q(t)$. Denote by Ω the normal closure of the extension $\mathbb{F}_q(x)/\mathbb{F}_q(t)$; Ω is a splitting field for $f(X) - t$ over $\mathbb{F}_q(t)$. The group $\hat{G} = \mathrm{Gal}(\Omega/\mathbb{F}_q(t))$ is called the *arithmetic monodromy group* of f and can be regarded as a permutation group on the conjugates of x over $\mathbb{F}_q(t)$. Let $\widehat{\mathbb{F}_q}$ be the algebraic closure of $\mathbb{F}_q$ in Ω. Then the group $G = \mathrm{Gal}(\Omega/\widehat{\mathbb{F}_q}(t)) \cong \mathrm{Gal}(\Omega\overline{\mathbb{F}_q}/\overline{\mathbb{F}_q}(t))$ is a normal transitive subgroup of $\hat{G}$ called the *geometric monodromy group* of f. The quotient $\hat{G}/G$ is canonically isomorphic to $\mathrm{Gal}(\widehat{\mathbb{F}_q}/\mathbb{F}_q)$, a cyclic group.

In the above association of a polynomial f with its monodromy groups, the significance of the assumption that f is indecomposable is that, as a permutation group, $\hat{G}$ is primitive (though G need not be), again see [6, 7]. For instance, if f is an indecomposable Dickson polynomial of degree n, then n is a prime (different from p) and G is cyclic or dihedral of degree n. Further, if f is an indecomposable sublinearized polynomial of degree n, then $n = p^m$ (a power of the characteristic) and G is a semidirect product $\mathbb{F}_p^m \times^s C$, with C a cyclic subgroup of $GL_m(p)$ and G acting naturally on the affine space $\mathbb{F}_p$.

Conversely, recent deep work of Fried, Guralnick and Saxl [7] (dependent amongst other things on detailed consequences of the classification of simple groups) has shown that if f is an indecomposable exceptional polynomial then, with two possible exceptions, G must be an affine group of prime power degree as described above except that C must be allowed to be replaced by a more general subgroup H of $GL_m(p)$.

The exceptions just referred to bring us to the subject of this paper. The theory of [7] left open the possibilities that, for an indecomposable exceptional polynomial f, we could have $p = 2$ or 3, $n = \deg f = p^k(p^k - 1)/2$, with $k \geq 3$ and odd and G a group normalising $PSL_2(p^k)$ in its transitive representation on n points. Clearly, any polynomial like this would be most interesting and would have very special properties but it should be stressed that the group theory is permissive; it is not, in itself, indicative that such polynomials exist.

It was therefore significant when following a thorough search of polynomi-

als of degree 28 over $\mathbf{F}_2$, P. Müller [17] was able to exhibit the exceptional polynomials

$$X^{28} + X^{10} + X = X(X^{27} + X^9 + 1), \tag{1.4}$$

$$X(X^9 + X^3 + 1)^3 \text{ and } X(X^3 + X + 1)^9 \tag{1.5}$$

over $\mathbf{F}_2$ for each of which $\widehat{G} = P\Gamma L_2(8)$, $G = PSL_2(8)$ $(= PGL_2(8))$, so that $\widehat{G}/G$ is cyclic of order 3, i.e., $\widehat{\mathbf{F}_2} = \mathbf{F}_8$. Encouraged by this, we sought a complete family of indecomposable exceptional polynomials over $\mathbf{F}_2$ of degree $2^{k-1}(2^k - 1)$, $k \geq 3$, and odd. In this we were successful and the purpose of this paper is to present these polynomials and verify the exceptionality property.

For any $k \geq 2$ we introduce the polynomial

$$S_k(X) = \sum_{i=0}^{k-1} X^{2^i - 1}. \tag{1.6}$$

Then for any $k \geq 2$ (not necessarily odd), and any divisor d of $2^k + 1$, define

$$f_{k,d}(X) = X\{S_k(X^c)\}^d, \tag{1.7}$$

where $cd = 2^k + 1$. In particular, let $f_k = f_{k,1}$, so that

$$f_k(X) = XS_k(X^{2^k+1}). \tag{1.8}$$

In this notation (1.4) is f_3 and the polynomials in (1.5) are $f_{3,3}$ and $f_{3,9}$. The next examples of (1.8) are

$$f_4(x) = X^{120} + X^{52} + X^{18} + X$$

and

$$f_5(X) = X^{496} + X^{232} + X^{100} + X^{34} + X$$

while

$$f_{5,d} = X(X^{15c} + X^{7c} + X^{3c} + X^c + 1)^d, \qquad cd = 33,$$

illustrates (1.7). We establish the following results.

Theorem 1.1. *For any odd $k \geq 3$, the polynomial f_k is exceptional over $\mathbf{F}_2$, indecomposable over $\overline{\mathbf{F}_2}$ with monodromy groups $\widehat{G} = P\Gamma L_2(2^k)$ and $G = PSL_2(2^k)$. It is a permutation polynomial on $\mathbf{F}_{2^e}$ if and only if $(k, e) = 1$.*

Theorem 1.2. *For any odd $k \geq 3$ and divisor d of $2^k + 1$, $f_{k,d}$ is exceptional over $\mathbf{F}_2$, indecomposable over $\overline{\mathbf{F}_2}$ with monodromy groups $\widehat{G} = P\Gamma L_2(2^k)$ and $G = PSL_2(2^k)$. It is a permutation polynomial on $\mathbf{F}_{2^e}$ if and only if $(k, e) = 1$.*

We have stated these results separately as we will establish Theorem 1.1 initially and later extend the results to Theorem 1.2. The key to Theorem 1.1 is the factorisation of $\phi_{f_k}(X, Y)$ (which we shall hereafter denote by $\phi_k(X, Y)$) over $\mathbf{F}_{2^k}$. The factorisation presented here was arrived at indirectly through connections with projective geometry, difference sets, designs, group theory and

Dickson polynomials. Such aspects largely remain to be explored. In looking for patterns and testing hypotheses we were able to make considerable use of the programmable version of the GALOIS package developed by the second author in recent years. This is an extension of a package developed with R. Lidl for performing calculations in finite fields [10]. Specifically, the direct factorisation of ϕ_4 and the synthesis of the factorisation of ϕ_5 through GALOIS was most helpful for our understanding of the general case. In limited attempts, we have not been able to realise any examples pertaining to $PSL_2(3^k)$ in characteristic 3. There are some resemblances of this topic to the theory of Dickson polynomials of the second kind in which there are known to be special types of permutation polynomials both in characteristic 2 and characteristic 3 (see [8]) which is suggestive but not convincing.

Finally, we believe these new polynomials will have applications to design theory, combinatorics, etc. It was not our plan to develop such here but we do record one immediate application to the construction of permutation polynomial functions on matrices over $\mathbf{F}_2$.

2. Preliminaries

We begin by assembling the definitions of the various linear groups that lie in the background of our work.

$\Gamma L_n(q)$ is the general semilinear group of invertible semilinear transformations on $\mathbf{F}_q^n$.

$Z_n(q)$ is the group of linear transformation of $\mathbf{F}_q^n$ induced by multiplication by a nonzero element of $\mathbf{F}_q$.

$GL_n(q)$ is the general linear group of invertible linear transformations of $\mathbf{F}_q^n$, also representable as the group of $n \times n$ matrices over $\mathbf{F}_q$ with nonzero determinant.

$SL_n(q)$ is the special linear group of invertible $n \times n$ matrices over $\mathbf{F}_q$ with determinant 1.

$P\Gamma L_n(q)$ is the projective semilinear group $\Gamma L_n(q)/Z_n(q)$.

$PGL_n(q)$ is the projective linear group $GL_n(q)/Z_n(q)$.

$PSL_n(q)$ is the projective special linear group $SL_n(q)Z_n(q)/Z_n(q)$.

In the case of characteristic 2, with which we are mainly concerned in this paper, $PGL_n(q)$ and $PSL_n(q)$ are isomorphic. Further [18, p. 227], $P\Gamma L_n(q)/PGL_n(q)$ is isomorphic to $\mathrm{Aut}(\mathbf{F}_q)$, a cyclic group of order k when $q = p^k$.

Next, we clarify the two usages of the term 'exceptional polynomial' and their equivalence. Temporarily, regard the term as referring to polynomials f for which ϕ_f (given by (1.1)) has no absolutely irreducible factors over $\mathbf{F}_q$. (Of course, this ignores the obvious factor $(X - Y)$ but the status of this factor is clear and remarks we make about the factorisation of ϕ_f may be easily qualified to take account of it.) The outcome of our first two lemmas (below) is that the two meanings are equivalent and we can interpret their statements with either sense.

The former of these was first established in full by the first author [3] and applies even when the degree of the polynomial is divisible by the characteristic p, which is particulary relevant here. A more elementary proof has recently been given by D. Wan [19].

Lemma 2.1. *Every exceptional polynomial over* $\mathbf{F}_q$ *is a permutation polynomial on* $\mathbf{F}_q$ *(and so on infinitely many extensions of* $\mathbf{F}_q$*).*

The other is an implication in the opposite direction. In it the bound $q > n^4$ can be extracted from results detailed in [13] as noted in [5]. Its exact nature is immaterial here.

Lemma 2.2. *Suppose that* $q > n^4$ *and* f *is a permutation polynomial of degree* n *over* $\mathbf{F}_q$*. Then* f *is exceptional over* $\mathbf{F}_q$*.*

From now on we take $p = 2$ and work entirely over fields of characteristic 2. For any $k \geq 2$ write

$$T_k(X) = X + X^2 + X^{2^2} + \cdots + X^{2^{k-1}} \tag{2.1}$$

so that (from (1.6)) $T_k(X) = XS_k(X)$. Then T_k is a linearized polynomial which acts as the trace function from $\mathbf{F}_{2^k} \to \mathbf{F}_2$. Observe that, from the definition (1.8), we have

$$f_k(X) = \frac{T_k(X^{2^k+1})}{X^{2^k}} \tag{2.2}$$

where the value of the right side is taken to be 0 when X is specialised to 0. The action of f_k on the field $\mathbf{F}_{2^{2k}}$ is crucial. To this end, define

$$\tau(X) = X + X^{2^k}, \quad \nu(X) = X^{2^k+1}. \tag{2.3}$$

In their action on $\mathbf{F}_{2^{2k}}$, τ and ν represent the trace and norm functions, respectively, from $\mathbf{F}_{2^{2k}}$ to $\mathbf{F}_{2^k}$, in which case we can write (2.3) as

$$\tau(x) = x + \bar{x}, \quad \nu(x) = x\bar{x}, \qquad x \in \mathbf{F}_{2^{2k}}, \tag{2.4}$$

where $\bar{x} = x^{2^k}$, the conjugate of x over $\mathbf{F}_{2^k}$. The lemmas which follow are easy to establish but vital in this context.

Lemma 2.3. *For any* x, y $(\neq 0) \in \mathbf{F}_{2^{2k}}$ *we have*

$$\nu(x+y) = \nu(x) + \nu(y)(1 + \tau(x/y)). \tag{2.5}$$

The next result summarises the action of f_k on $\mathbf{F}_{2^{2k}}$.

Lemma 2.4. *Suppose* $x \in \mathbf{F}_{2^{2k}}$*. Then*

$$f_k(x) = \begin{cases} 0 & \text{if } T_k(\nu(x)) = 0, \\ 1/\bar{x} & \text{if } T_k(\nu(x)) = 1. \end{cases} \tag{2.6}$$

In particular, if $x \in \mathbf{F}_{2^k}$*, then*

$$f_k(x) = \begin{cases} 0 & \text{if } T_k(x) = 0, \\ 1/x & \text{if } T_k(x) = 1. \end{cases} \tag{2.7}$$

Moreover, if $x, y \in \mathbf{F}_{2^{2k}}$*, then* $\phi_k(x, y) = 0$ *if and only if* $x = y$ *or* $f_k(x) = f_k(y) = 0$.

Lemma 2.5. *Let* $U_k(X) = T_k(X) + 1$*. Then*

$$T_k(X)U_k(X) = \tau(X). \tag{2.8}$$

In particular the roots of T_k *comprise those* 2^{k-1} *elements of* $\mathbf{F}_{2^k}$ *(including* 0*) of trace* 0 *and the roots of* U_k *are the* 2^{k-1} *elements of* $\mathbf{F}_{2^k}$ *of trace* 1*. Moreover*

$$T_k(x) \neq 0,\ 1, \quad U_k(x) \neq 0,\ 1, \qquad x \in \mathbf{F}_{2^{2k}} \backslash \mathbf{F}_{2^k}. \tag{2.9}$$

Proof. $T_k(X)U_k(X) = X + X^2 + \cdots + X^{2^{k-1}} + X^2 + \cdots + X^{2^k} = \tau(X)$. The roots of τ are simply the elements of $\mathbf{F}_{2^k}$ (with multiplicity 1). □

Lemma 2.6. *The polynomial* $T_k(\nu(X))$ *(of degree* $2^{k-1}(2^k+1)$*) has* $2^{k-1}(2^k-1)$ *distinct roots all in* $\mathbf{F}_{2^{2k}}$*. Specifically,* 0 *is a root of multiplicity* $Q = 2^k + 1$ *and the remaining roots each have multiplicity* 1*.*

Proof. Obviously, 0 is a root of multiplicity Q. Further by the cyclic nature of the multiplicative group of $\mathbf{F}_{2^{2k}}$, for each nonzero β in $\mathbf{F}_{2^k}$ (and certainly for each such β of trace 0) there are precisely Q elements $\alpha \in \mathbf{F}_{2^{2k}}$ for which $\alpha^Q = \beta$. The result follows. □

3. The factorisation of $f(x) + f(y)$

One of the equivalent definitions of exceptionality mentioned in §1 involved the factorisation of $f(x) + f(y)$ into irreducible factors in $\mathbf{F}_2$ and $\overline{\mathbf{F}_2}$. In this section we establish the factorisation over $\mathbf{F}_{2^k}$. As a consequence of a result in the next section, this factorisation is identical to that over $\overline{\mathbf{F}_2}$. From this, as we have said, we can unravel some of the secrets of these polynomials. The factorisation over $\mathbf{F}_2$ will appear at the end of the next section. It turns out that (in addition to $(X+Y)$) ϕ_k has $2^{k-1}-1$ factors indexed by the nonzero roots of T_k and so by the roots of S_k. We will denote the set of roots of S_k by S, a subset of $\mathbf{F}_{2^k}$ (by Lemma 2.5).

Theorem 3.1. *Over* $\mathbf{F}_{2^k}$

$$\phi_k(X, Y) = (X+Y)\prod_{\alpha \in S} \Theta_\alpha(X, Y)\ , \tag{3.1}$$

where

$$\Theta_\alpha(X, Y) = (X+Y)^{2^k+1} U_k^2(\alpha X/(X+Y)) + \alpha^2\ , \tag{3.2}$$

a polynomial of degree 2^k+1 *in each of* X *and* Y*.*

Proof. We set

$$\phi_k^*(X, Y) = \phi_k(X, X+Y) = f_k(X) + f_k(X+Y)$$

and

$$\Theta_\alpha^*(X, Y) = \Theta_\alpha(X, X+Y) = Y^{2^k+1} U_k^2(\alpha X/Y) + \alpha^2 \tag{3.3}$$

and prove the identity (3.1) in the equivalent form

$$\phi_k^*(X, Y) = Y\prod_{\alpha \in S} \Theta_\alpha^*(X, Y)\ , \tag{3.4}$$

in which both sides have degree $n = 2^{k-1}(2^k-1)$ in Y and $n-1$ in X.

In the first place, regard either side of (3.4) as a polynomial of degree $n-1$ in X with coefficients in $\mathbf{F}_{2^{2k}}[Y]$ (though they are actually in $\mathbf{F}_{2^k}[Y]$). To establish

(3.4) it suffices to show that both sides agree at any n distinct specialisations of X to $\mathbf{F}_{2^k}[Y]$ and we select for this purpose the n distinct roots x in $\mathbf{F}_{2^{2k}}$ of $T_k(\nu(X))$ (see Lemma 2.6). (For justification of this claim, note that from this agreement at n points, the coefficients in $\mathbf{F}_{2^k}[Y]$ of either side can be uniquely recovered from a system of linear equations with a Vandermonde determinant of size n and rows of the form $(1, x, x^2, \ldots, x^{n-1})$ with $T_k(\nu(x)) = 0$).

Next, to show that the polynomials of degree n in Y which emerge from the above process (when X has been specialised to x) are the same on both sides of (3.4), it suffices to show that

(a) the n zeros of the left side of (3.4) are zeros of the right side; and

(b) the coefficient of Y^n on either side is the same.

We can quickly verify (b). The coefficient of Y^n on the left side trivially is 1. On the right side it is

$$\prod_{\alpha \in S} \prod_{U_k(\beta)=0} \beta^2 = \prod_{\alpha \in S} \prod_{U_k(\beta)=0} \beta = 1$$

since $U_k(0) = T_k(0) + 1 = 1$.

A minor contribution to (a) is also immediate. For a given x, $Y = 0$ is obviously a zero of both sides.

By Lemmas 2.4 and 2.6 we can summarise the remaining demands of (a) by saying that we have to show that, whenever x and y $(\neq 0)$ in $\mathbf{F}_{2^{2k}}$ are such that $T_k(\nu(x)) = T_k(\nu(x+y))) = 0$, then the right side of (3.4) (with $X = x$, $Y = y$) is also 0, i.e. $\Theta_\alpha^*(x, y) = 0$, for some $\alpha \in S$. We rewrite this last expression as

$$\nu(y) U_k(\alpha^2 x^2 / y^2) = \alpha^2, \qquad \alpha \in S. \tag{3.5}$$

Suppose, therefore, that $T_k(\nu(x)) = T_k(\nu(x+y))$ where x, y $(\neq 0) \in \mathbf{F}_{2^{2k}}$. With (3.5) in view we shall show that there exists $\alpha \in S$ such that

$$T_k(\alpha^2 x^2 / y^2) = \nu(y) \tau(x^2 / y^2). \tag{3.6}$$

It would then follow from Lemma 2.5 and the fact that τ is $\mathbf{F}_{2^k}$-linear that (3.5) holds unless $T_k(\alpha x / y) = 0$. In the latter situation, by (2.8), $x/y \in \mathbf{F}_{2^k}$ and so $\tau(x/y) = 0$. But specifically, in this case the argument below yields (3.6) with $\alpha^2 = \nu(y)$, whence $U_k(\alpha^2 x^2 / y^2) = 1$ and (3.5) is again valid.

To complete the proof, therefore, we establish (3.6) for some α in S. By Lemma 2.3 and our assumptions, $T_k(\beta) = 0$ for $\beta = \nu(y)(1 + \tau(x/y))$. Set

$$\alpha^2 = \beta^2 + \nu^2(y) + \nu(y) = \nu(y) + \nu^2(y) \tau^2(x/y).$$

Then $\alpha^2 = \nu(y)$ whenever $x/y \in \mathbf{F}_{2^k}$, as required. Thus $T_k(\alpha) = 0$ since $T_k(\beta) = T_k(\beta^2) = 0$ and $T_k(\nu^2(y) + \nu(y)) = 0$ (because $\nu(y) \in \mathbf{F}_{2^k}$). With this choice of α,

$$\begin{aligned} T_k(\alpha^2 x^2 / y^2) &= T_k(\nu(y) x^2 / y^2) + T_k(\nu^2(y) x^4 / y^4) \\ &\quad + T_k(\nu^2(y) \nu^2(x^2 / y^2)) \qquad (3.7) \\ &= \tau(\nu(y) x^2 / y^2) + T_k(\nu^2(x)) \qquad (3.8) \\ &= \nu(y) \tau(x^2 / y^2) + 0 \end{aligned}$$

and (3.6) follows. In the above we have used the facts that $\tau(z) = z + \bar{z}$ (for $z = x/y$) at (3.7) and $T_k(z + z^2) = \tau(z)$ with $z = \nu(y)x^2/y^2$ at (3.8). This completes the proof of Theorem 3.1. □

4. Consequences of the factorisation

Theorem 4.1. *The polynomials* $\Theta_\alpha(X, Y) \in \mathbf{F}_{2^k}[X, Y]$, $\alpha \in S$, *defined by* (3.2) *are absolutely irreducible.*

Proof. Equivalently, we need to show that the polynomials $\Theta_\alpha^*(X, Y)$ displayed at (3.3) are irreducible in $\overline{\mathbf{F}_2}[X, Y]$ for any $\alpha \in S$. Suppose to the contrary that $\Theta_\alpha^*(X, Y)$ is reducible in $\overline{\mathbf{F}_2}[X, Y]$. Observe that $\alpha^2 = \alpha^{2^k+1}$ and set $V = \alpha X/Y$, $W^2 = \alpha/Y$. Then, easily, any nontrivial factor of Θ_α^* in $\overline{\mathbf{F}_2}[X, Y]$ yields a nontrivial factor of

$$W^Q + U_k(V) \tag{4.1}$$

$Q = 2^k + 1$, in $\overline{\mathbf{F}_2}[V, W]$. In particular, (4.1) is reducible as a polynomial in W with coefficients in $\overline{\mathbf{F}_2}[V]$. It is well-known, however, that such a binomial can be reducible only if $U_k(V)$ is identically $Z^d(V)$ for some polynomial Z and some $d > 1$ which divides Q. This is a contradiction because U_k is square-free by Lemma 2.5. □

Theorem 4.2. *For any* $k \geq 2$ *the polynomial* f_k *is indecomposable over* $\overline{\mathbf{F}_2}$.

Proof. Suppose f_k is functionally decomposable over $\overline{\mathbf{F}_2}$. Then, as noted in the proof of Lemma 3.1 of [6], for example (and implicit in our Introduction), simply because f_k is a polynomial, there is a decomposition of the form, $f_k = g(h)$, where g, h are polynomials in $\overline{\mathbf{F}_2}[X]$ and $d = \deg h$ is a divisor of $n = 2^{k-1}(2^k - 1) = \deg f_k$ with $d \neq 1, n$. Moreover, $X + Y$ is a factor of $g(X) + g(Y)$ and so $h(X) + h(Y)$ is a factor of ϕ_k in $\overline{\mathbf{F}_2}[X, Y]$. By Theorem 4.1 it follows that ϕ_h is the product of $X + Y$ and j (say) factors $\Theta_\alpha(X, Y)$, $\alpha \in S$, where $1 \leq j \leq 2^{k-1} - 1$. Hence $\deg h = jQ + 1$ divides $n = (2^{k-1} - 1)Q + 1$ where $Q = 2^k + 1$. Thus

$$(2^{k-1} - 1)Q + 1 = i(jQ + 1) \tag{4.2}$$

for some i, which implies $i \equiv 1 \mod Q$. But $i \neq 1$ (since $j < 2^{k-1} + 1$) and so $i \geq 2^k + 2$. Hence the right side of (4.2) exceeds 2^{2k} which exceeds the left side, a contradiction which yields the result. □

Theorem 4.3. *For any odd* $k \geq 3$, f_k *is an indecomposable exceptional polynomial over* $\mathbf{F}_2$. *It has arithmetic monodromy group* $\hat{G} = P\Gamma L_2(2^k)$ *and geometric monodromy group* $G = PSL_2(2^k)$.

Proof. Granted k is odd, $S_k(1) = 1$ and so the roots S of S_k exclude both members of $\mathbf{F}_2$. Hence none of the factors $\Theta_\alpha(X, Y)$ of ϕ_k lie in $\mathbf{F}_2[X, Y]$ and so f_k is exceptional.

Further, by Theorem 4.2, f_k is indecomposable of degree $2^{k-1}(2^k - 1)$. The

only available conclusion from Theorems 13.4 and 14.1 of [7] is that

$$PSL_2(2^k) \subseteq G \subset \hat{G} \subseteq P\Gamma L_2(2^k)\,. \tag{4.3}$$

We have to show that the outer containments of (4.3) are, in fact, equalities. As mentioned at the beginning of §2, the quotient of the outer groups is cyclic of order k. On the other hand, from the factorisation of ϕ_k, $S \subseteq \widehat{\mathbf{F}_2}$. (For example, regarding x as a root of $f_k(X)+t$ and $\Theta_\alpha(x, Y)$ as a polynomial in Y, its coefficients are contained in Ω and so, easily, $\alpha^2 \in \Omega$.) Moreover $\mathbf{F}_2(S) = \mathbf{F}_{2^k}$ because, for instance, for any primitive root γ of $\mathbf{F}_{2^k}$, either γ or $\gamma+1$ is in S. Hence the cardinality of $\hat{G}/G$ is at least k and the result follows. □

We comment on an analogue of Theorem 4.3 when k is even. In this case, since $S_k(1) = 0$, then $1 \in S$ and so $\Theta_1(X, Y) \in \mathbf{F}_2[X, Y]$ and f_k cannot be exceptional (a fact we knew already from [7]). On the other hand Θ_1 is the only absolutely irreducible factor. We know that Theorem 4.3 remains an accurate description of the monodromy groups of f_k although it does not follow in the same way from [7]. In fact, we can give a verification of these groups (whether k is even or odd) which is independent of the classification of simple groups but will leave the details to a further note. There are some differences between the even and odd cases. For example when $k = 2$ (so that $S_2(X) = X+1$), $\phi_2(X, Y)/(X+Y)$ is absolutely irreducible; yet we know that $\widehat{\mathbf{F}_2} = \mathbf{F}_4$, a fact we shall not verify here.

The next result establishes Theorem 1.1 in full.

Theorem 4.4. *For any odd $k \geq 3$, f_k is a permutation polynomial on $\mathbf{F}_{2^e}$ if and only $(k, e) = 1$.*

Proof. Suppose $(k, e) = 1$. Then $\mathbf{F}_{2^k} \cap \mathbf{F}_{2^e} = \mathbf{F}_2$ and none of the factors $\Theta_\alpha(X, Y)$, $\alpha \in S$, has coefficients in $\mathbf{F}_{2^e}$. Thus f_k is a permutation polynomial on $\mathbf{F}_{2^e}$ by Lemma 2.1.

To prove the converse it suffices to show that if e is a *prime* divisor of k then f_k cannot be a permutation polynomial on $\mathbf{F}_{2^e} \subseteq \mathbf{F}_{2^k}$. Let α $(\neq 0) \in \mathbf{F}_{2^e}$ be such that $T_e(\alpha) = 0$. Then evidently $T_k(\alpha) = 0$ and so $f_k(\alpha) = 0$, by (2.7). □

The factorisation of ϕ_k over $\mathbf{F}_2$ can be obtained from that over $\mathbf{F}_{2^k}$ by combining conjugate factors. This leads to a determination of the factorisation pattern of ϕ_k in terms of parameters which are independent of this problem, namely the number N_d of monic irreducibles of degree d over $\mathbf{F}_2$ and U_d, the number of such irreducibles whose term in $d-1$ is 0. We note that $N_d > 0$ for $d \geq 1$, $U_1 = U_2 = 0$, $U_d > 0$ if $d > 2$, and if d is odd then $U_d = N_d/2$. In the next theorem *degree* refers to the degree in X (or Y, which is the same).

Theorem 4.5. *For each divisor d of k, define V_d to be N_d if k/d is even, and U_d if k/d is odd. Then for each such d there are V_d irreducible factors of*

degree dQ over $\mathbf{F}_2$ dividing $\phi_k(X, Y)$. Explicitly,

$$\phi_k(X, Y) = (X + Y) \prod_{d|k} \prod_{t=1}^{V_d} P_{d,t}(X, Y) ,$$

where $P_{d,t}(X, Y)$ is irreducible over $\mathbf{F}_2$ of degree dQ .

Proof. By Lemma 2.5 the trace function $T_k(X)$ splits into linear factors in $\mathbf{F}_{2^k}$. Hence any given root of $S_k(X)$ belongs to some subfield of $\mathbf{F}_{2^k}$ and so its minimal polynomial over $\mathbf{F}_2$ has degree dividing k. So $S_k(X)$ is a product of irreducibles over $\mathbf{F}_2$ whose degrees divide k. Let $S_{k,d}(X)$ be an irreducible factor of degree d of $S_k(X)$. Then from (3.2) the product of $\Theta_\alpha(X, Y)$, where α runs over the roots of $S_{k,d}(X)$ is defined over $\mathbf{F}_2$. This product is irreducible over $\mathbf{F}_2$, as otherwise there would be a proper subset A of the roots of $S_{k,d}$ such that the corresponding product of the Θ_α lies in $\mathbf{F}_2[X, Y]$. Specialising Y to 0 we would obtain a product of the shape $\prod_{\alpha \in A}(x^{2^k+1} + \alpha) \in \mathbf{F}_2[X]$. This would imply that $\prod_{\alpha \in A}(x + \alpha) \in \mathbf{F}_2[X]$, contradicting the $\mathbf{F}_2$-irreducibility of $S_{k,d}(X)$. From the above we see that to each $\mathbf{F}_2$-irreducible factor of $S_k(X)$ of degree d (where d divides k) there corresponds an $\mathbf{F}_2$-irreducible factor of $f(X) + f(Y)$ of degree dQ. To establish the result it then suffices to examine the factorisation pattern of $S_k(X)$. From the explicit form, $T_k(X)$ can be written as

$$\sum_{i=0}^{k/d-1} \left(\sum_{j=0}^{d-1} x^{2^j} \right)^{2^{di}} .$$

When evaluated on $\mathbf{F}_{2^d}$ the inner sum takes the values 0 or 1 and so $T_k(x)$ takes the same values (if k/d is odd) or is always 0 (if k/d is even). In the former case if $I_d(X)$ is a monic irreducible polynomial in $\mathbf{F}_2$ of degree d which has its term in x^{d-1} equal to 0, then the $\mathbf{F}_{2^d}$-trace of any of its roots is 0, and so $T_k(X)$ vanishes on its roots. Hence $I_d(X)$ divides $S_k(X)$. If k/d is even then a similar argument applies to *any* irreducible monic polynomial of degree d. □

In the final section of this paper we will present examples of factorisations based on Theorem 4.5. In group theoretical terms, the total number of irreducible factors of ϕ_k over $\mathbf{F}_2$ (including $X + Y$) equates to the rank of the primitive group $\widehat{G}$.

5. The extended family

So far we have concentrated on the polynomials f_k given by (1.8). Yet, as reported in Theorem 1.2, exceptionality is a property shared by each $f_{k,d}$ as defined in (1.7) for $k \geq 3$ and odd. We now justify this claim.

In fact we can demonstrate exceptionality through Lemma 2.2 without a discussion of $\phi_{k,d}$ (which has the obvious meaning). As this approach falls just a little short of a full proof of Theorem 1.2 we outline it only.

Choose e large enough and odd so that $2^e > n^4$, where $n = 2^{k-1}(2^k - 1)$. For example, $e = 8k + 1$ would do. Then $(2^k + 1, 2^e - 1) = 1$. (The purpose of insisting that e be odd is to avoid having $3 = (2^k + 1, 2^e - 1)$ when k is

odd and e is even.) Given $f_{k,d}$ with $cd = 2^k + 1$, we have $(d, 2^e - 1) = 1$ and so X^d is a permutation polynomial on $\mathbf{F}_{2^e}$. We deduce from Theorem 1.1 that

$$f_k^d(X) = f_{k,d}(X^d) \tag{5.1}$$

is a permutation polynomial on $\mathbf{F}_{2^e}$ and so, by the same reason, $f_{k,d}$ is a permutation polynomial on $\mathbf{F}_{2^k}$. It follows from Lemma 2.2 that $f_{k,d}$ is exceptional over $\mathbf{F}_{2^e}$ and so over $\mathbf{F}_2$ (over which it is defined). By extending this argument we can show that $f_{k,d}$ is a permutation polynomial over $\mathbf{F}_{2^e}$ whenever $(k, e) = 1$ unless e is even and $3|d$ (because then X^3 is not a permutation polynomial over $\mathbf{F}_{2^e}$).

An attack which deals even with this last situation can be based on that which exploited (1.3) to verify the exceptionality of sublinearized polynomials in [4]. Let ζ be a primitive dth root of unity (in $\mathbf{F}_{2^{2k}}$). Then, with $g = f_k^d$, $f = f_k$,

$$\begin{aligned} \phi_{k,d}(X^d, Y^d) &= \phi_g(X, Y) = \prod_{i=0}^{d-1} \{f(X) + \zeta^i f(Y)\} \\ &= \prod_{i=0}^{d-1} \{f(X) + f(\zeta^i Y)\}, \end{aligned} \tag{5.2}$$

since $\zeta^{2^k+1} = 1$. From (3.1), over $\mathbf{F}_{2^k}$, (5.2) is a product of factors of the form

$$\prod_{i=0}^{d-1} \Theta_\alpha(X, \zeta^i Y), \tag{5.3}$$

which is evidently a polynomial in Y^d and X. Interchanging the roles of X and Y we see that (5.3) can be written as $P_\alpha(X^d, Y^d)$. Hence

$$\phi_{k,d}(X, Y) = (X + Y) \prod_{\alpha \in S} P_\alpha(X, Y) \tag{5.4}$$

Moreover, $P_\alpha(0, 0) = \alpha^{2d}$ and $\mathbf{F}_2(\alpha^{2d}) = \mathbf{F}_2(\alpha)$ since $(d, 2^k - 1) = 1$. Thus the permutation properties of $\phi_{k,d}$ stated in Theorem 1.2 can be deduced from (5.4) analogously to the proof of Theorem 4.4. If any of the factors $P_\alpha(X, Y)$ were reducible then (5.1) would lead to the reducibility of Θ_α. The argument for indecomposability given in Theorem 4.2 is also applicable here.

6. Applications and examples

It was not our intent here to deal with extensive applications but we mention one that is immediate. See [1, 9, 14].

Theorem 6.1. *Let k be an odd prime and set $m = k - 1$. Then f_k regarded as a scalar polynomial function on the ring $(\mathbf{F}_2)_{m\times m}$ of $m \times m$ matrices over $\mathbf{F}_2$ is bijective and so is a permutation polynomial function.*

Proof. By [1], it suffices that to show that f_k is a permutation polynomial of $\mathbf{F}_{2^i}$, $i = 1, \ldots, m$, and that the formal derivative f_k' does not vanish on $\mathbf{F}_{2^i}$, $i = 1, \ldots, m/2$. Since f_k' is identically 1, the second condition is no restriction and the result follows from Theorem 1.1. □

We now consider some examples of the factorisations described above. In each we are factoring $\phi_k(X, Y)$, and $Q = 2^k + 1$.

- $k = 2$. In Theorem 4.5 d can be 1 or 2 and $Q = 5$. If $d = 1$ then k/d is even and there is a single ($N_1 = 1$) factor of degree 5. If $d = 2$ there are no ($U_2 = 0$) factors of degree 10. Over $\mathbf{F}_4$ the single factor remains irreducible. The full factorisation of $\phi_2(X, Y)$ is

$$(X+Y)(Y^5 + XY^4 + X^2Y^3 + X^3Y^2 + X^4Y + X^5 + 1).$$

  The nontrivial factor remains irreducible in $\overline{\mathbf{F}_2}$.
- $k = 3$. Theorem 4.5 predicts that over $\mathbf{F}_2$, $\phi_3(X, Y)$ has a single irreducible factor of degree 27. Over the algebraic closure $\overline{\mathbf{F}_2}$ this splits into three absolutely irreducible factors of degree 9. This is the factorisation obtained by Müller [17].
- $k = 4$. $Q = 17$. Theorem 4.5 predicts one factor each of degrees 17, 34 and 68 over $\mathbf{F}_2$, splitting into 7 factors of degree 17 in $\overline{\mathbf{F}_2}$.
- $k = 6$. $Q = 65$. In this case we have one factor of degree 65, two of degree 195 and four of degree 390, all splitting into factors of degree 65 over $\overline{\mathbf{F}_2}$.
- $k = p$ (p an odd prime). Then in Theorem 4.5 d can only be 1 or p. If $d = 1$ we have k/d is odd and $U_1 = 0$. If $k = p$, k/d is odd and there are $U_p = N_p/2 = (2^{p-1} - 1)/k$ factors of degree Qp, where $Q = 2^p + 1$. For example if $k = 5$ there are 3 factors of degree 165 over $\mathbf{F}_2$, each splitting into a product of factors of degree 33 over $\overline{\mathbf{F}_2}$.
- $k = p^t$ (p an odd prime, $t > 1$). Then d is p^l, $0 \le l \le t$. There are $U_{p^l} = (2^{p^l} - 2^{p^{l-1}})/2p^l$ factors of degree Qp^l, for $1 \le l \le t$, where $Q = 2^{p^l} + 1$.

References

1. J. V. Brawley, L. Carlitz and J. Levine, *Scalar polynomial functions on the $n \times n$ matrices over a finite field*, Linear Algebra Appl. **10** (1975), 199–217.
2. L. Carlitz, *On factorable polynomials in several indeterminates*, Duke Math. J. **2** (1936), 660–670.
3. S. D. Cohen, *The distribution of polynomials over finite fields*, Acta Arith. **17** (1970), 255–271.
4. ———, *Exceptional polynomials and the reducibility of substitution polynomials*, Enseign. Math. **36** (1990), 53–65.
5. ———, *Proof of a conjecture of Chowla and Zassenhaus on permutation polynomials*, Canad. Math. Bull. **33** (1990), 230–234.
6. ———, *Permutation polynomials and primitive permutation groups*, Arch. Math. (Basel) **57** (1991), 417–423.
7. M. D. Fried, R. Guralnick and J. Saxl, *Schur covers and Carlitz's conjecture*, Israel J. Math. **82** (1993), 157–225.
8. M. Henderson and R. Matthews, *Permutation properties of Chebyshev polynomials of the second kind over a finite field*, Finite Fields and Their Applications (to appear).
9. N. S. James and R. Lidl, *Permutation polynomials on matrices*, Linear Algebra Appl. **6** (1987), 181–190.
10. R. Lidl and R. Matthews, GALOIS: *A microcomputer algebra package*, Congr. Numer. **66** (1988), 145–156.
11. 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.

12. R. Lidl, G. L. Mullen and G. Turnwald, *Dickson polynomials*, Pitman Monographs and Surveys in Pure and Appl. Math., 65, Longman Scientific and Technical, Essex, England, 1993.

13. R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia Math. Appl., 20, Addison-Wesley, Reading, MA, 1983, now distributed by Cambridge University Press.

14. R. W. Matthews, *Permutation polynomials in one and several variables*, PhD. Thesis, Univ. of Tasmania, Hobart, 1982.

15. W. H. Mills, *The degrees of the factors of certain polynomials over finite fields*, Proc. Amer. Math. Soc. **25** (1970), 860–863.

16. G. L. Mullen, *Permutation polynomials over finite fields*, Finite Fields, Coding Theory and Advances in Communications and Computing, (G.L. Mullen and P.J. Shiue, eds.), Lecture Notes in Pure and Appl. Math., 141, Marcel Dekker, 1993, pp. 131–151.

17. P. Müller, *New examples of exceptional polynomials* Finite Fields: Theory, Applications and Algorithms, (G. L. Mullen and P. J. Shiue, eds.), Contemp. Math., vol. 168, Amer. Math. Soc., Providence, RI, 1994, pp. 245–249.

18. T. Tsuzuku, *Finite groups and finite geometries*, Cambridge Univ. Press, Cambridge, 1982.

19. D. Wan, *A p-adic lifting lemma and its applications to permutation polynomials*, Finite Fields, Coding Theory and Advances in Communications and Computing, (G. L. Mullen and P. J. Shiue, eds.), Lecture Notes in Pure and Appl. Math., 141, Marcel Dekker, 1993, pp. 209–216.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF GLASGOW, GLASGOW G12 8QW, SCOTLAND
E-mail address: sdc@maths.glasgow.ac.uk

DEPARTMENT OF COMPUTER SCIENCE, THE UNIVERSITY OF QUEENSLAND, QUEENSLAND 4072, AUSTRALIA
E-mail address: rex@cs.uq.oz.au