FINITE FIELDS AND THEIR APPLICATIONS 1, 261–277 (1995)

Exceptional Polynomials over Finite Fields

STEPHEN D. COHEN

Department of Mathematics, University of Glasgow, Glasgow G12 8QW, Scotland
E-mail: sdc@maths.gla.ac.uk

AND

REX W. MATTHEWS

Department of Computer Science, The University of Queensland, Brisbane 4072, Australia
E-mail: rex@cs.uq.oz.au

Communicated by the Editors

Received September 6, 1994; revised May 25, 1995

DEDICATED TO LEONARD CARLITZ WITH OUR GRATITUDE AND APPRECIATION

A recently discovered family of indecomposable polynomials of nonprime power degree over $\mathbb{F}_2$ (which include a class of exceptional polynomials) is set against the background of the classical families and their monodromy groups are obtained without recourse to the classification of finite simple groups.

1. INTRODUCTION

Let $\mathbb{F}_q$ be the finite field of order q, a power of a prime p. All polynomials f over $\mathbb{F}_q$ will be assumed to be separable, i.e. $f \neq f_1^p$. For q prime at least the notion of an *exceptional polynomial* (EP) f over $\mathbb{F}_q$ was first isolated in 1963 by Davenport and Lewis [6], who had to exclude such from general results related to the nature of the set of values of a polynomial f of given degree n (≥ 2) over a finite field of large size (compared to n). Though their definition was in terms of the reducibility of the polynomial $f(X) - f(Y)$ rather than the permutation properties of f, it turned out that a property of an EP on $\mathbb{F}_q$ that can be used as a defining one is that f is a *permutation polynomial* (PP) on $\mathbb{F}_{q^r}$ (i.e., as a function, permutes $\mathbb{F}_{q^r}$) for

1071-5797/95 $12.00

infinitely many values of e (and so, in particular, is a PP on $\mathbb{F}_q$). In fact, Davenport and Lewis recognized that an EP is "close" to being a PP and conjectured that an EP must actually be a PP. Of course, the connection with PPs renders it transparent why EPs are exceptional to the estimates of [6].

The condition for a polynomial to be an EP is stringent but there are some basic examples that (essentially) flow from classical investigations of Dickson around 1900 (e.g., [7]). Indeed, these constitute core items in the (small) stock of known, easily describable families of PPs over $\mathbb{F}_q$ (see [16]). In brief, for appropriate q, these comprise *cyclic polynomials* X^n $(p \nmid n)$, *Dickson* (or *Chebyshev*) polynomials $D_n(X, a)$, $(a \in \mathbb{F}_q, p \nmid n)$, which satisfy the identity

$$D_n(X + (a/X), a) = X^n + (a/X)^n \tag{1.1}$$

and reduce to cyclic polynomials when $a = 0$, and *linearized (additive) polynomials* $L(X)$, where L has the form

$$L(X) = \sum_{i=0}^{m} a_i X^{p^i}, \qquad a_0(\neq 0), a_1, \ldots, a_m(\neq 0) \in \mathbb{F}_q. \tag{1.2}$$

Then, in 1990, Cohen [3] (using the Davenport-Lewis "reducibility" definition) discovered there are EPs among the members of a "neo-classical" family, called *sublinearized polynomials*. These are related to (and incorporate) linearized polynomials and like the latter all have degree a power of p. In the simplest case of degree p, the corresponding polynomials had been recognized as permutation polynomials by Dickson, who conjectured that all PPs whose degree equalled the field characteristic were of this type. In [11] this was established for EPs and in [10] this was extended to PPs with $q > p^3$.

Now, composites of EPs over $\mathbb{F}_q$ (and of linear polynomials) are also EPs and, until very recently, all known EPs were formed in this way from the basic classical examples. Conversely, any EP over $\mathbb{F}_q$ can be decomposed over $\mathbb{F}_q$ to be a composition of indecomposable EPs and linear polynomials. In particular, an indecomposable cyclic or Dickson polynomial has degree n, a prime $(\neq p)$. Thus, all classical indecomposable EPs have degree a prime or a prime power. Moreover, without detracting from their significance or usefulness, when examined in the right way, there is a relatively simple "explanation" for the exceptional nature of each.

By contrast, starting from a set of three related polynomials of degree 28 over $\mathbb{F}_2$ found by Müller [20], the authors [5] have discovered, for each $k \geq 2$, a set of related indecomposable polynomials $\{f_{k,d}: d \mid 2^k + 1\}$ of degree $n = n_k = 2^{k-1}(2^k - 1)$ with remarkable reducibility and permutation properties; in particular, those with odd k are EPs over $\mathbb{F}_2$. Thus, Müller's

examples (those with $k = 3$) are the first nonclassical EPs. They were found by means of a computer search (facilitated by some group theory) using the permutation property and verified (also by computation) to satisfy the reducibility definition of an EP. For the rest, a whole new theory had to be developed in [5] (though computation had played a part in its formulation).

Specifically, the polynomials $f_{k,d}$ are defined as follows. Let

$$S_k(X) = \sum_{i=0}^{k-1} X^{2^i-1}, \qquad k \geq 2.$$

Then, with $cd = 2^k + 1$, set

$$f_{k,d}(X) = X\{S_k(X^c)\}^d, \qquad k \geq 2. \tag{1.3}$$

In particular, abbreviate $f_{k,1}$ to f_k. Their properties are evidently deeper than those of the classical families, yet there are connections (albeit subtle) with the latter. In fact, the interplay between these families is involved in the establishment of the properties which was achieved ultimately by direct means working with the fields and polynomials alone.

Nevertheless, the motivation for he discovery of the $f_{k,d}$ and direction for the theory was provided by the known connection between indecomposable EPs and the theory of primitive permutation groups which was first observed by Fried [8] in 1970 and subsequently involved in other papers, such as those of Klyachko [14] and Cohen [4]. Other papers also considered the "monodromy groups" of EPs as permutation groups without exploiting primitivity [2, 9]. The climax was the work of Fried *et al.* [11], which employed the classification of finite simple groups (CSG) and covering theory in prime characteristic to eliminate all but a few candidates for the monodromy groups of an indecomposable EP. They concluded that, over $\mathbb{F}_q$, q even ($p = 2$), the only possible non-prime power degrees for an indecomposable EP were members of the sequence $\{n_k, k (\geq 3) \text{ odd}\}$ of the degrees of the $f_{k,d}$. There is a similar sequence of possible degrees over fields $\mathbb{F}_q$ of characteristic 3 but, in fields of characteristic exceeding 3, all indecomposable EPs (other than Dickson and cyclic ones) must have degree a power of the characteristic p. These findings were the motivation for Müller's search and the eventual discovery by the authors of the polynomials $f_{k,d}$. Further, although all necessary reducibility and permutation properties of the $f_{k,d}$ were established independently of this theory in [5] and it was clear that their monodromy groups ought to be those permitted by [11], formal verification of their identity had been made only for odd values of k, by elimination, from [11] and therefore was dependent on CSG.

In this paper we remedy this deficiency and confirm the monodromy

group of all polynomials $f_{k,d}$ ($k \geq 2$) (independently of CSG) by further direct analysis of the polynomails plus a key characterization of the linear groups $PSL_2(2^k)$ of McDermott [19]. We also set the new polynomials against the classical scheme.

In 1966 Leonard Carlitz, in a conjecture that has driven much of the work on EPs, asserted that, over a sufficiently large finite field of odd order, there is no PP of given even degree. The immediate subsequent activity clarified the equivalent formulation in terms of the non-existence of an EP of even degree over a field of odd order [13]. Then there was a period in which little seemed to be happening in the theory of EPs, but it coincided with one in which CSG was developed, a process that is generally accepted as complete but that lacks a cohesive treatment. Eventually, the weight of this machinery sufficed to settle the conjecture affirmatively in [11] and, in attacking it, even more general results on EPs were obtained. We believe that Carlitz would be satisfied that his insight into the nature of PPs has had such deep consequences and also that he would appreciate the particular structure of the $f_{k,d}$.

2. Preliminary Results

The Dickson polynomial $D_n(X, a)$ satisfies (1.1) and is given explicitly by

$$D_n(X, a) = \sum_{i=0}^{[n/2]} \frac{n}{n-i} \binom{n-i}{i} (-a)^i X^{n-2i}.$$

When q is prime or $a \in \mathbb{F}_p$, $D_n(X, a)$ may be regarded as a polynomial in $\mathbb{Z}[X]$ interpreted as one in $\mathbb{F}_q[X]$. (See [16] for a book devoted to these and related polynomials.) We note that in characteristic 2 there are relationships between certain Dickson polynomials and the linearized polynomial

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

We also define

$$U_k(X) = T_k(X) + 1, \tag{2.2}$$

and set $D_n(X) = D_n(X, 1)$.

Lemma 2.1. *For any $k \geq 1$,*

(i) $D_{2^k-1}(X) = X^{2^k+1} T_k^2(1/X)$,

(ii) $D_{2^k+1}(X) = X^{2^k+1} U_k^2(1/X)$.

Proof. By induction on k. For $k = 1$,

$$D_1(X) = X,\ D_3(X) = X^3 + X = X^3(X^{-2} + 1).$$

(i) By [16, p. 11],

$$\begin{aligned} D_{2^{k+1}-1}(X) &= D_{2^k-1}(X)D_{2^k}(X) + X \\ &= X^{2^k}(X^{2^k+1}T_k(1/X)) + X, \end{aligned}$$

and the result follows since

$$\frac{T_k^2(Y)}{Y^{2^{k+1}+1}} + \frac{1}{Y} = \frac{(T_k(Y) + Y^{2^k})^2}{Y^{2^{k+1}+1}} = \frac{T_{k+1}^2(Y)}{Y^{2^{k+1}+1}}.$$

(ii) Similarly, using

$$D_{2^{k+1}+1}(X) = D_{2^k}(X)D_{2^k+1}(X) + X. \quad \blacksquare$$

Given f, let $\phi_f(X, Y) = (f(X) - f(Y))/(X - Y) \in \mathbb{F}_q[X, Y]$ and denote the algebraic closure of $\mathbb{F}_q$ by $\overline{\mathbb{F}}_q$ ($= \overline{\mathbb{F}}_p$). Then ϕ_f factorizes as a product of distinct irreducible factors in $\mathbb{F}_q[X, Y]$. If such an irreducible factor remains irreducible in $\overline{\mathbb{F}}_q[X, Y]$, then it is said to be *absolutely irreducible*. Let $\mathbb{F}_q' = \mathbb{F}_{q^l}$ for some $l \geq 1$ be the finite extension of $\mathbb{F}_q$ obtained by adjoining all the constant coefficients of all the irreducible factors of ϕ_f over $\overline{\mathbb{F}}_q$ to $\mathbb{F}_q$. Then a factor of ϕ_f over $\mathbb{F}_q$ is absolutely irreducible if and only if it is irreducible over $\mathbb{F}_q'$. Then f is *exceptional on* $\mathbb{F}_q$ if ϕ_f has no absolutely irreducible factors, i.e., every irreducible factor over $\mathbb{F}_q$ is reducible in some extension such as $\mathbb{F}_q'$.

Let z be an indeterminate and L the splitting field of the (separable) polynomial $f(X) - z$ over $\mathbb{F}_q(z)$. Further let $\Omega = \{Y = Y_1, \ldots, Y_n\} \subset L$ be the roots of $f(X) - z$. The *arithmetic monodromy group* G of f (over $\mathbb{F}_q$) is the Galois group of the irreducible polynomial $f(X) - z$ over $\mathbb{F}_q(z)$, regarded as a (transitive) group on Ω. The subgroup $\overline{G} = \mathrm{Gal}(f(X) - z, \overline{\mathbb{F}}_q(z))$ is the *geometric monodromy group of* f. Indeed, if $\widehat{\mathbb{F}}_q = \mathbb{F}_{q^k}$, say, is the algebraic closure of $\mathbb{F}_q$ in L, then $\overline{G} \cong \mathrm{Gal}(f(X) - z, \widehat{\mathbb{F}}_q)$ and $G/\overline{G} \cong \mathrm{Gal}(\widehat{\mathbb{F}}_q/\mathbb{F}_q)$, a cyclic group of order k. We also write G_Y and $\overline{G}_Y$ for the stabilizers of Y (in G and $\overline{G}$, respectively) acting either on Ω or on $\Omega\backslash\{Y\}$. Thus G_Y is the Galois group of $f(X) - f(Y)$ (or of $\phi_f(X, Y)$) over $\mathbb{F}_q(Y)$. Since $\mathbb{F}_{q^k}(z)$ is a normal extension of $\mathbb{F}_q(z)$ it follows immediately that $\overline{G}$ is a normal subgroup of G and $G/\overline{G} \cong C_k$. The groups all act as permutation groups on the roots of $f(X) - z$. The critical property relating to EPs lies in the subgroup $\overline{G}_Y = \overline{G} \cap G_Y$. The property of f being exceptional trans-

lates into the statement that *every orbit of G_Y (other than Y) splits into strictly smaller orbits under $\overline{G}_Y$*. Since $\mathbb{F}_{q^\ell}(z)$ is a normal extension of $\mathbb{F}_q(z)$ there is a homomorphism θ: $G \to C_k$ with kernel $\overline{G}$. We denote by G^* the union of the cosets which generate C_k. Consequently $|G^*| = \phi(k)|\overline{G}| = (\phi(k)/k)\,|G|$, where ϕ is the Euler ϕ-function. G^* may be characterized as those $g \in G$ which, in their action on $\mathbb{F}_{q^\ell}$, fix only $\mathbb{F}_q$.

Exceptional polynomials can also be characterized as those polynomials which permute infinitely many extensions of $\mathbb{F}_q$. In fact the following result holds [11].

LEMMA 2.2. *If f is an EP on $\mathbb{F}_q$ then there exists $\ell > 1$ such that, if $(e, \ell) = 1$, then f is a PP on $\mathbb{F}_{q^e}$.*

We enlarge on the factorization of ϕ_{D_n}, where $D_n(X) = D_n(X, 1)$. We state the result in arbitary characteristic p but use it only when $p = 2$. From [16, Theorem 3.12] (taken from [23] when q is odd), ϕ_{D_n} factorizes into absolutely irreducible quadratic factors over $\mathbb{F}_{q^\ell}$ (ℓ as above) as follows. Let ζ be a primitive nth root of unity (in $\mathbb{F}_{q^\ell}$) and set

$$\beta_1 = \zeta^i + \zeta^{-i}, \qquad \gamma_i = \zeta^i - \zeta^{-i}, \qquad i = 1, 2, 3, \ldots .$$

Then, with $f(X) = D_n(X, a)$, over $\mathbb{F}_{q^\ell}$,

$$\phi_f(X, Y) = \prod_{i=1}^{(n-1)/2} (X^2 - \beta_i XY + Y^2 + \gamma_i^2 a), \qquad n \text{ odd}, \tag{2.3}$$

$$\phi_f(X, Y) = (X + Y) \prod_{i=1}^{(n-2)/2} (X^2 - \beta_i XY + Y^2 + \gamma_i^2 a), \qquad n \text{ even}. \tag{2.4}$$

Although ϕ_{D_n} factorizes over $\mathbb{F}_{q^\ell}$ into irreducible quadratics it is easy to see [3] that $X^n Y^n D_n(X + (a/X), Y + (a/Y))$ splits completely into factors over $\mathbb{F}_{q^\ell}$ linear in X (say). Note also that, from (1.1), $D_{mn}(X, a) = D_m(D_n(X, a), a^n)$ and so $D_n(X, a)$ is indecomposable over $\mathbb{F}_q$ if and only if n is a prime ($\neq p$).

LEMMA 2.3. *Suppose n is odd and $p \nmid n$. Let z be an indeterminate. Then $D_n(X) - z^n$ is irreducible over $\overline{\mathbb{F}}_q(z)$. Indeed, if $n \mid q - 1$, then the Galois group of $D_n(X) - z^n$ over $\mathbb{F}_q(z)$ is the dihedral group of order $2n$.*

Proof. If $D_n(X) - z^n$ is reducible as a polynomial in X, it is reducible as a polynomial in z and so, by a well-known fact (independent of the nature of D_n), $D_n(X) = g^d(X)$ for some d (>1) dividing n and polynomial g, which is false since D_n is square-free (when $p \nmid n$).

Assume next $n \mid q - 1$ so that $\mathbb{F}_q$ contains ζ, a primitive nth root of unity. Let Y be a root of the polynomial and U be such that $Y = U + (1/U)$. By

(1.1), $U^n = V$ (say), where $V + 1/V = z^n$. The n roots of the polynomial are $\zeta^i U + (1/\zeta^i U)$, $i = 0, \ldots, n-1$, and $\mathbb{F}_q(z, U)$ is a splitting field over $\mathbb{F}_q(z)$, which by the first part has degree n or $2n$ over $\mathbb{F}_q(z)$. If the degree is n, then $V \in \mathbb{F}_q(z)$, i.e. there are co-prime polynomials V_1, V_2 with (identically)

$$\frac{V_1^2(z) + V_2^2(z)}{V_1(z)V_2(z)} = z^n,$$

which is obviously false.

Finally, generators of the cyclic groups $\mathrm{Gal}(\mathbb{F}_q(z, U), \mathbb{F}_q(z, V))$ and $\mathrm{Gal}(\mathbb{F}_q(z, U), \mathbb{F}_q(z, Y))$ (or order n and 2, respectively) together generate the dihedral group of order $2n$. ∎

A major advance in the classification of exceptional polynomials was achieved in [11]. In this paper the possible arithmetic/geometric monodromy groups which can be assumed by an indecomposable exceptional polynomial are reduced to a small number of classes. If the degree n of f is not divisble by the characteristic p of $\mathbb{F}_q$ then f is a cyclic or Dickson polynomial, with G being cyclic or dihedral. If $n = p^m$, a power of p, then G is an "affine group," i.e., a semi-direct product $G = V \times {}^{\cdot}H$, acting on affine space V, where V is an $\mathbb{F}_p$-vector space of dimension m, $H = G_Y \subseteq GL_m(p)$ acts irreducibly on V via invertible linear transformations, and V acts by translation. In particular, G is a subgroup of the whole linear affine group $AGL_m(p)$. (Of course, $\overline{H} = \overline{G}_Y \subseteq H$ need not act irreducibly because $\overline{G}$ need not be primitive.) Now, in fact, all the classical indecomposable EPs (except for the cyclic and Dickson polynomials) have affine monodromy groups. Conversely, [11, Corollary 11.2] shows, via ramification, that if it is known that H is cyclic, then an indecomposable EP of prime power degree must be classical. But, there could well be other such EPs with prime power degree (without $\overline{H}$ being cyclic) and any examples of these would be most interesting.

The main bulk of the effort of [11] was in treating the other general possibility permitted by the Aschbacher–O'Nan–Scott theorem. This is that the *generalized Fitting subgroup* of G (which for G primitive, is the direct product of the minimal normal subgroups), or *socle* of G, is a direct product of, say, r (≥ 1) isomorphic non-abelian simple groups H, with $n = |H|^r$, or $r \geq 2$ and $n = |H|^{r-1}$. In fact, the theorem implies much more (see [12, Proposition 2.1]), but certainly we can see that n cannot be a prime power. From this, mostly by the exceptionality condition and CSG, it is deduced in [11] that actually G must be "almost simple," i.e., $r = 1$ and $H \subseteq \overline{G} \subseteq G \subseteq N = \mathrm{Aut}\, H$, the normalizer of H in S_n. Further, for G primitive, the polynomial condition implies that there is a "factorization" $G = G_Y \overline{G}_\infty$ (a set-theoretic product), where G_Y is maximal in G and $\overline{G}_\infty$ is

transitive. Now, a paper of Liebeck *et al.* [17] (using CSG) had listed all possible factorizations of almost simple groups where both factors are maximal and neither factor contains the (unique) normal simple group. This does not quite apply as $\overline{G}_\infty$ need not be maximal, but with some additional effort along the same kind of lines using CSG, it is shown in [11] that there are only two possibilities for H, both involving $PSL_2(q)$, the projective special linear group of 2×2 matrices over $\mathbb{F}_q$ of determinant 1 and its automorphism group $P\Gamma L_2(q)$, the projective semi-linear group of invertible semi-linear transformations of $\mathbb{F}_q^2$ (modulo its centre), see [21]. Briefly, the conclusion is that, necessarily,

$$p = 2 \text{ or } 3, \qquad n = p^k(p^k - 1)/2, \text{ where } k \geq 3 \text{ odd}, \tag{2.5}$$

and

$$H = PSL_2(p^k) \subseteq \overline{G} \subseteq G \subseteq N = P\Gamma L_2(p^k). \tag{2.6}$$

The action is on the cosets of the appropriate maximal subgroup of index n (i.e., for G, on the cosets of G_Y). If p is odd then $P\Gamma L_2(p^k)/PSL_2(p^k) \cong \mathrm{Gal}(\mathbb{F}_{p^{2k}}/\mathbb{F}_p)$, a cyclic group of order $2k$, so we must have $\widehat{\mathbb{F}_q} \subseteq \mathbb{F}_{p^{2k}}$. If $p = 2$ we conclude similarly that $\widehat{\mathbb{F}_q} \subseteq \mathbb{F}_{p^k}$. In fact, a careful reading of the proof of [11, Theorem 14.1] and the reformulation of that result as [10, Theorem 2.4] indicate that necessarily $H = \overline{G}$ and $N = G$ in (2.6). (See also Theorem 3.12 below.)

This theory directed Müller [20] to search for EPs among all polynomials of degree 28 over $\mathbb{F}_2$ (the case $p = 2$, $k = 3$ of (2.5)). He used GAP with some group theory and exceptionality (for fields $\mathbb{F}_{2^e}$, $e \leq 7$) to find the examples $f_{3,d}$, $d = 1, 3, 9$. This opened up the way for the discovery of the full class of polynomials $f_{k,d}$ by the authors [5] and we go on to discuss their properties in the next section.

3. The Polynomials $f_{k,d}$

From now on we suppose $p = 2$ and consider the polynomials $f_{k,d}$ defined by (1.3) for all $k \geq 2$ (and not just odd $k \geq 3$ as in [5]).

We recall (1.3). For any $d \mid 2^k + 1$, let $cd = 2^k + 1$ and set

$$f_{k,d}(X) = X\{S_k(X^c)\}^d, \tag{3.1}$$

where

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

a linearized polynomial. Then also

$$f_{k,d}(X) = \frac{T_k^d(X^c)}{X^{2^k}}. \tag{3.2}$$

Thus, bearing in mind Lemma 2.1(i), we see that the $f_{k,d}$ involve cyclic, linearized and Dickson polynomials and, for given k, the set $\{f_{k,d} : d \mid 2^k + 1\}$, is somewhat analogous to the set of sub-linearized polynomials L_d associated with a fixed linearized polynomial L. In fact, it was this last feature which was instrumental in the postulation of the $f_{k,d}$ as candidates for EPs (from Müller's single set of examples).

The major effort of [5] was the explicit factorization of ϕ_{f_k} (which will be abbreviated to ϕ_k) over $\mathbb{F}_{2^k}$. We had quickly checked, for a few odd values of k, that the f_k permuted a number of fields (and so seemed certain to be exceptional) but it seemed hopeless to establish exceptionality in this fashion directly and therefore factorization of ϕ_k was sought as the means of proving exceptionality. This was difficult to accomplish as, unlike the classical EPs, the nature of the factorization would not be simple and the available clues were very limited—the data from Müller's examples, the general shape of the polynomials and their connections with the classical families (as outlined earlier in this section), and some rough ideas of the likely factorization pattern of ϕ_k from the nature of the group $P\Gamma L_2(2^k)$. Our understanding of the general situation was therefore greatly aided by means of interactive sessions—involving theory and experiment—with the package GALOIS, developed specifically for finite field computation by Matthews from an original version of Lidl and Matthews ([15], cf. the comment on [1, p. 56]). In particular, ϕ_4 was factorized, its shape analyzed, and that of ϕ_5 synthesized by an algorithm involving subgroups of the additive group of roots of the linearized polynomial T_5. (It should be said that factorization of ϕ_4 by pure computation would be a challenge and that of ϕ_5 probably infeasible.) Motivated by the success of this algorithm for ϕ_5, we reformulated the result it produced as a conjectural explicit factorization of ϕ_k, valid for all $k \geq 2$. To justify the formula theoretically was not easy. We achieved it through a number of lemmas (stated below). In fact, the form of the factorization that we give (Theorem 3.6) represents an advance on that of [5, Theorem 3.1], in that from it we can identify the monodromy groups of $f_{k,d}$ for all k, d, without assuming CSG.

In the following lemmas, the role of the field $\mathbb{F}_{2^{2k}}$ is seen to be vital. We write

$$\tau(X) = X^{2^k} + X, \qquad \nu(X) = X^{2^k+1},$$

so that, on $\mathbb{F}_{2^{2k}}$, if $\bar{x} = x^{2^k}$ denotes the conjugate of $x \in \mathbb{F}_{2^{2k}}$ over $\mathbb{F}_{2^k}$, then $\tau(x) = x + \bar{x}$, $\nu(x) = x\bar{x}$ are the trace and norm functions, respectively, from $\mathbb{F}_{2^{2k}}$ to $\mathbb{F}_{2^k}$. We refer to [5] for proofs.

LEMMA 3.1. *For any $x, y\ (\neq 0) \in \mathbb{F}_{2^{2k}}$, we have*

$$\nu(x + y) = \nu(x) + \nu(y)(1 + \tau(x/y)).$$

LEMMA 3.2. *Suppose $x \in \mathbb{F}_{2^{2k}}$. Then*

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

Thus, on $\mathbb{F}_{2^{2k}}$, f_k is not a PP but has the following curious property.

LEMMA 3.3. *Suppose $x, y \in \mathbb{F}_{2^{2k}}$. Then*

$$f_k(x) = f_k(y) \Rightarrow x = y \quad \text{or} \quad f_k(x) = f_k(y) = 0.$$

Hence

$$\phi_k(x, y) = 0 \Rightarrow f_k(x) = f_k(y) = 0.$$

For the last part of Lemma 3.3, note that $f_k'(x)\ (= 1) \neq 0$ for all $x \in \bar{\mathbb{F}}_q$.

LEMMA 3.4. *Let $U_k(X) = T_k(X) + 1$. Then $T_k(X)U_k(X) = \tau(X)$.*

LEMMA 3.5. *The polynomial $T_k(\nu(X))$ has $n = n_k = 2^{k-1}(2^k - 1)$ distinct roots, all in $\mathbb{F}_{2^{2k}}$. Specifically, 0 is a root of multiplicity $2^k + 1$ and the remaining $n_k - 1$ roots each have multiplicity 1.*

Let S_k be the set of roots of $S_k(X)$ (all of which are in $\mathbb{F}_{2^k}$, by Lemma 3.4) and set $D_n(X) = D_n(X, 1)$.

THEOREM 3.6. *For any $k \geq 2$, over $\mathbb{F}_{2^{2k}}$,*

$$\phi_k(X, Y) = \prod_{\alpha \in S_k} E_\alpha(X, Y), \tag{3.3}$$

where, with $K = 2^k + 1$,

$$E_\alpha(X, Y) = X^K D_K\left(\frac{X + Y}{\alpha X}\right) + 1 \tag{3.4}$$

$$= Y^K D_K\left(\frac{X + Y}{\alpha Y}\right) + 1. \tag{3.5}$$

Proof. It suffices to prove (3.3), with E_α given by (3.4). Note that, by Lemma 2.1(ii) and the fact that $\Pi_{\alpha \in S_k} \alpha^2 = 1$ (since $S_k \subseteq \mathbb{F}_{2^k}$), this follows from the factorization (shown in [5, Theorem 3.1])

$$\phi_k(X, Y) = \prod_{\alpha \in S} \Theta_\alpha(X, Y), \tag{3.6}$$

where

$$\Theta_\alpha(X, Y) = (X + Y)^K U_k^2(\alpha X/(X + Y)) + \alpha^2.$$

We sketch the proof of (3.6) by showing the equivalent identity

$$f_k(X) + f_k(X + Y) = Y \prod \Theta_\alpha^*(X, Y), \tag{3.7}$$

where

$$\Theta_\alpha^*(X, Y) = Y^K U_k^2(\alpha X/Y) + \alpha^2. \tag{3.8}$$

Both sides of (3.8) have degree n_k in Y and $n_k - 1$ in X. From (3.2), note that $f_k(X) = T_k(\nu(X))/X^{2^k}$. From Lemmas 3.2 and 3.3, the zeros of the left side of (3.8) at points $(x, y) \in \mathbb{F}_{2^k}^2$ occur when $\nu(x) = \nu(x + y) = 0$. By elementary degree and polynomial considerations using Lemma 3.5 it suffices to show that for any such pair (x, y) (with $y \neq 0$), there exists $\alpha \in S_k$ with $\Theta_\alpha^*(x, y) = 0$. Choose α by

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

and it follows, by means of Lemma 3.1, that

$$T_k(\alpha^2 x^2/y^2) = \nu(y)\tau(x^2/y^2),$$

and hence, by Lemma 3.4, that $\nu(y)U_k(\alpha^2 x^2/y^2) = \alpha^2$, whence $\Theta_\alpha^*(x, y) = 0$. ∎

The next result follows quickly from (3.5) by using Lemma 2.3 (which was the purpose of the latter).

LEMMA 3.7. *For each $\alpha \in S_k$, the factor $E_\alpha(X, Y)$ in (3.3) is absolutely irreducible over $\mathbb{F}_{2^k}(Y)$ and its Galois group over $\mathbb{F}_{2^k}(Y)$ is dihedral of order $2(2^k + 1)$. Moreover the constant coefficients of $E_\alpha(X, Y)$ generate $\mathbb{F}_2(\alpha)$ over $\mathbb{F}_2$.*

Proof. The first sentence follows from Lemma 2.3 since $K = 2^k + 1$ divides $2^{2k} - 1$. (In fact, $E_\alpha(X, Y)$ has the same Galois group over $\mathbb{F}_{2^k}(Y)$ as we shall later see.) The last part is easier to deduce from (3.8) since

$$\Theta_\alpha^*(X, Y) = (Y^K + \alpha X Y^{K-1} + \cdots) + \alpha^2. \quad \blacksquare$$

LEMMA 3.8. *For $k \geq 2$, f_k is indecomposable over $\bar{\mathbb{F}}_2$.*

Proof. (Taken from [5, Theorem 4.2]). Suppose there is a non-trivial decomposition $f_k = g(h)$ over $\bar{\mathbb{F}}_2$. Then $d = \deg h$ is a divisor of n_k (with $d \neq 1, n_k$). Since $h(X) + h(Y)$ is a factor of $f_k(X) + f_k(Y)$, by the absolute irreducibility of the E_α (Lemma 3.7), ϕ_h is a product of J of them, where $1 \leq J \leq 2^{k-1} - 1$. Hence $d = JK + 1$ ($\equiv 1 \pmod K$) divides $n_k = 2^{k-1}(2^k - 1) \equiv 1 \pmod K$. It follows that $n_k = Id_k$, where $I \equiv 1 \bmod K$) ($I > 1$) and so $n_k \geq (K + 1)^2$, which is false. $\blacksquare$

LEMMA 3.9. *For the polynomial f_k ($k > 2$), $\bar{G}_Y$, the one point stabilizer of the geometric monodromy group is dihedral of order $2(2^k + 1)$.*

Proof. Let L be the splitting field of $D_K(Z) + (1/Y^K)$ over $\bar{\mathbb{F}}_2(Y)$ (where $f_k(Y) = z$). Then $\mathrm{Gal}(L/\bar{\mathbb{F}}_2(Y))$ is dihedral of order $2K$ by Lemma 2.3. For any $\alpha \in S_k$, a root Z^* of $D_K(Z) + (1/Y^K)$ over $\mathbb{F}_{2^k}(Y)$ is linked to one X^* of $D_K((X + Y)/\alpha X) + 1/Y^K$ by $X^* = Y(\alpha Z^* + 1)$; hence L is also the splitting field of the latter. Since this is true for every $\alpha \in S_k$, L is also the splitting field of $f_k(X) + z$ over $\bar{\mathbb{F}}_2(z)$ and so of $\phi_k(X, Y)$ over $\bar{\mathbb{F}}_2(Y)$. $\blacksquare$

LEMMA 3.10. *If $k \geq 3$, then $\mathbb{F}_2(S_k) = \mathbb{F}_{2^k}$.*

Proof. If k is odd, then, for any $\beta \in \mathbb{F}_{2^k}$, $T_k(\alpha) = 0$ for exactly one member of $\{\beta, \beta + 1\}$ (since $T_k(\beta + 1) = T_k(\beta) + 1$) and we may take β to be a primitive root of $\mathbb{F}_{2^k}$ to yield a non-zero member $\alpha \in S_k$ for which $\mathbb{F}_2(\alpha) = \mathbb{F}_{2^k}$.

Suppose k (>2) is even and that every member of $\mathbb{F}_{2^k}$ that is not in a proper subfield has trace 1 (over $\mathbb{F}_2$). Then,

$$2^k - \sum_{\substack{\ell \mid k \\ \ell \text{ prime}}} 2^{k/\ell} \leq 2^{k-1},$$

and so, easily,

$$2^{k-1} \leq 2^{k/2} + (k - 3)2^{k/2},$$

which is impossible. $\blacksquare$

We remark that Lemma 3.10 fails when $k = 2$ because $S_2 = \{1\}$ and so $\mathbb{F}_2(S_2) = \mathbb{F}_2$. In fact by Lemma 3.10 and the last part of Lemma 3.7 we have the following result.

LEMMA 3.11. *Given f_k ($k \geq 2$), let $\mathbb{F}_2'$ be the constant field extension associated with ϕ_k (as in Section 2). Then*

$$\mathbb{F}_2' = \begin{cases} \mathbb{F}_2, & \text{if } k = 2, \\ \mathbb{F}_{2^k}, & \text{if } k \geq 3. \end{cases}$$

In group-theoretical terms, the fact that all the irreducible factors E_α in (3.3) have the same degree $(2^k + 1)$ in X is equivalent to the fact that the (primitive) geometric monodromy group $\overline{G}$ is $\frac{3}{2}$-transitive; i.e., all the non-trivial "sub-degrees" (sizes of orbits) are the same. (Incidentally, the equality of (3.4) and (3.5) yields that all the orbits are "self-paired" too.) Indeed, by Lemmas 3.7 and 3.9, any two point stabilizer $\overline{G}_{Y_1Y_2}$ of $\overline{G}$ has order 2. Moreover, since $\overline{G}$ is primitive of non-prime power degree, it cannot contain a regular elementary abelian normal subgroup [22, Theorem 11.5]. A most convenient theorem of McDermott [19] reveals that the above features precisely characterize $PSL_2(2^k)$ in its representation of degree n_k. We are grateful to Saxl for drawing our attention to McDermott's work, specifically, a related paper [18] from which our result could also be deduced.

THEOREM 3.12. *For any $k \geq 2$, the arithmetic monodromy group G of f_k is $P\Gamma L_2(2^k)$ and its geometric monodromy group $\overline{G}$ is $PSL_2(2^k)$. Moreover $\widehat{\mathbb{F}_2} = \mathbb{F}_{2^k}$.*

Proof. By the preceding remarks, $\overline{G} = PSL_2(2^k)$. Hence, by the basic theory of primitive groups, (2.6) holds; i.e., $G \subseteq P\Gamma L_2(2^k)$ and so $\widehat{\mathbb{F}_2} \subseteq \mathbb{F}_{2^k}$. On the other hand, evidently $\mathbb{F}_2' \subseteq \widehat{\mathbb{F}_2}$ and so, provided $k \geq 3$, $\widehat{\mathbb{F}_2} = \mathbb{F}_{2^k}$, which implies that $G = P\Gamma L_2(2^k)$, $k \geq 3$. Suppose therefore that $k = 2$ and Y, Y^* are distinct roots in Ω. Then, by (2.3),

$$\begin{aligned} Y^{-5}\phi_2(X, Y) &= D_5\left(\frac{X + Y}{Y}\right) + \frac{1}{Y^5} \\ &= D_5\left(\frac{X + Y}{Y}\right) + D_5\left(\frac{Y^* + Y}{Y}\right) \\ &= (Z_1^2 + \beta Z_1 Z_2 + Z_2^2 + \beta^2) \\ &\quad \times (Z_1^2 + (\beta + 1)Z_1 Z_2 + Z_2^2 + (\beta + 1)^2), \end{aligned}$$

where $Z_1 = (X + Y)/Y$, $Z_2 = (Y^* + Y)/Y$, and $\beta^2 + \beta = 1$ so that $\mathbb{F}_2(\beta) = \mathbb{F}_4$. Hence $\widehat{\mathbb{F}_2} = \mathbb{F}_4$ in this case and it follows that $G = P\Gamma L_2(4)$. ∎

It follows incidentally from Theorem 3.12 that the Galois group of f_k over $\mathbb{F}_{2^k}(Y)$ is dihedral of order $2(2^k + 1)$ (cf. Lemma 3.9 and the remark in the proof of Lemma 3.7).

We now deduce the corresponding result (to Theorem 3.12) for an arbitrary polynmial $f_{k,d}$, $d \mid 2^k + 1$. We write $\phi_{k,d}$ for $f_{f_{k,d}}$.

LEMMA 3.13. (i) *For any $k \geq 2$, $d \mid 2^k + 1$, $\phi_{k,d}$ splits into a product of factors $\Pi_{\alpha \in S_k} P_\alpha(X, Y)$, where each P_α is defined and absolutely irreducible over $\mathbb{F}_{2^k}$ and has degree $2^k + 1$ in X and in Y.*

(ii) *The constant coefficients of $P_\alpha(X, Y)$ generate $\mathbb{F}_2(\alpha)$ over $\mathbb{F}_2$.*

(iii) *$f_{k,d}$ is indecomposable over $\mathbb{F}_2$.*

Proof. (i) This is essentially in [5]. We summarize it here. Denote a primitive dth root of unity by ζ ($\in \mathbb{F}_{2^{2k}}$). Since

$$f_{k,d}(X^d) = f_k^d(X), \tag{3.9}$$

then

$$\begin{aligned} f_{k,d}(X^d) + f_{k,d}(Y^d) &= \prod_{i=0}^{d-1} \{f_k(X) + \zeta^i f_k(Y)\} \\ &= \prod_{i=0}^{d-1} \{f_k(X) + f_k(\zeta^i Y)\} \\ &= (X^d + Y^d) \prod_{\alpha \in S_k} \prod_{i=0}^{d-1} E_\alpha(X, \zeta^i Y), \end{aligned}$$

and the *polynomial* $P_\alpha(X, Y)$ can be defined by

$$P_\alpha(X^d, Y^d) = \prod_{i=0}^{d-1} E_\alpha(X, \zeta^i Y), \tag{3.10}$$

where $\deg P_\alpha = 2^k + 1$. Suppose P_α has a non-trivial factorization $P_\alpha = Q_1 Q_2$ over $\mathbb{F}_{2^k}$. Then the absolutely irreducible polynomial $E_\alpha(X, Y)$ divides $Q_1(X^d, Y^d)$, say, and so, since the latter is invariant under $Y \to \zeta Y$, $P_\alpha(X^d, Y^d)$, divides it, a contradiction. Hence P_α is absolutely irreducible over $\mathbb{F}_{2^k}$.

(ii) By (3.10) and (3.5),

$$P_\alpha(0, Y) = (D_K(1/\alpha) Y^K + 1)^d.$$

But, by Lemma 2.1(ii), $D_K(1/\alpha) = U_k^2(\alpha)/\alpha^K = 1/\alpha^2$ (since $T_k(\alpha) = 0$), and so

$$P_\alpha(0, Y) = 1 + (1/\alpha^2)Y + \cdots.$$

(iii) This is proved exactly as in Lemma 3.8. ■

We now generalize Theorem 3.12.

THEOREM 3.14. *For any $k \geq 2$, $d \mid 2^k + 1$, the monodromy groups of $f_{k,d}$ are given by $G = P\Gamma L_2(2^k)$, $\bar{G} = PSL_2(2^k)$, and $\hat{\mathbb{F}}_2 = \mathbb{F}_{2^k}$.*

Proof. Let $g(X)$ be the polynomial (3.9) and M be the splitting field of $g(X) + z$ over $\mathbb{F}_{2^{2k}}(z)$. Then M is also the splitting field of $f_d(X) + U$ over $\mathbb{F}_{2^{2k}}(U)$, where $U^d = z$ and $\mathbb{F}_{2^{2k}}(U)/\mathbb{F}_{2^{2k}}(z)$ is a normal (cyclic) extension of degree d (since $\mathbb{F}_{2^{2k}}$ contains all dth roots of unity). Now let M_0 be the splitting field of $f_{k,d}(X) + z$ over $\mathbb{F}_{2^{2k}}(z)$. Then M_0 is also a normal extension of $\mathbb{F}_{2^{2k}}(z)$ contained in M. By Galois theory and Theorem 3.12,

$$\begin{aligned} PSL_2(2^k) &= \mathrm{Gal}(f_k(X) + z, \mathbb{F}_{2^{2k}}(U)) \\ &\cong \mathrm{Gal}(f_{k,d}(X) + z, \mathbb{F}_{2^{2k}}(U) \cap M_0), \end{aligned}$$

which is a normal subgroup of $\mathrm{Gal}(f_{k,d}(X) + z, \mathbb{F}_2(z)) = G$. Hence the Fitting subgroup of the primitive group G is $PSL_2(2^k)$ and so (2.6) holds. But, by an argument similar to that given above,

$$\begin{aligned} P\Gamma L_2(2^k) &= \mathrm{Gal}(f_k(X) + z, \mathbb{F}_2(U)) \\ &\cong \mathrm{Gal}(f_k(X) + z, \mathbb{F}_2(U) \cap M_1) \subseteq G, \end{aligned}$$

where M_1 is the splitting field of $f_{k,d}(X) + z$ over $\mathbb{F}_2(z)$.

Hence, in fact, $G = P\Gamma L_2(2^k)$. ■

THEOREM 3.15. *For all odd $k \geq 3$ and all divisors d of $2^k + 1$, $f_{k,d}$ is a PP on $\mathbb{F}_{2^e}$ if and only if $(k, e) = 1$.*

Proof. By the factorizations we can take $\ell = k$ in Lemma 2.2.

Conversely, let e be a prime divisor of k and α ($\neq 0$) $\in \mathbb{F}_{2^e}$ be such that $T_k(\alpha) = 0$. If $cd = 2^k + 1$, then $(c, 2^k - 1) = 1$ and so $(c, 2^e - 1) = 1$. Hence $\alpha = \beta^c$ for some β ($\neq 0$) $\in \mathbb{F}_{2^e}$, which implies that $f_{k,d}(\beta) = T_k^d(\alpha)/\beta^{2^k} = 0$ (by (3.2)). So $f_{k,d}$ is not a PP of $\mathbb{F}_{2^e}$ and this suffices to prove the result. ■

We conclude this section with some comments on f_2, which, by Lemma 3.11, is slightly anomalous, as $\mathbb{F}_2' = \mathbb{F}_2$, yet $\hat{\mathbb{F}}_2 = \mathbb{F}_4$.

We have $f_2(X) = X^6 + X, f_2'(X) = 1$ so that $f_2(X) + \alpha$ is square-free for all α in $\overline{\mathbb{F}}_2$. Further, [21], $G = P\Gamma L_2(4) \cong S_5$, $\overline{G} = PSL_2(4) \cong A_5$, the symmetric and alternating groups of degree 5. Using this association (or by direct consideration of the action of G and $\overline{G}$ on G_Y and $\overline{G}_Y$) we can calculate the number of elements in $\overline{G}$ and G^* (where G is the disjoint union $\overline{G}$ and G^*, with G^* defined in Section 2) as in the following table.

Cycle pattern		No. elements
$(1, 5)$	$\overline{G}$	24
(3^2)		20
$(1^2, 2^2)$		15
(1^6)		1
(6)	G^*	20
(2^3)		10
$(1^2, 4)$		30

The Galois group of $f_2(X) + z$ over $\mathbb{F}_{2^e}(z)$, e even, is $\overline{G}$ and so does not contain a 6-cycle. So $f_2(X) + \alpha$ ($\alpha \in \mathbb{F}_{2^e}$, e even) cannot be irreducible. Indeed, by [2, Theorem 1], as $e \to \infty$, the proportion of $\alpha \in \mathbb{F}_{2^e}$ for which $f_2(X) + \alpha$ has the indicated factor patterns approaches $\frac{2}{5}, \frac{1}{3}, \frac{1}{4}, \frac{1}{60}$, respectively, and the number of distinct values attained by the polynomial f_2 in $\mathbb{F}_{2^e}$ tends to $\frac{2}{5}$.

When e is odd, $f_2(X) + z$ has Galois group G over $\mathbb{F}_{2^e}(z)$, the relevant part (as far as the factor patterns of $f_2(X) + \alpha$, $\alpha \in \mathbb{F}_{2^e}$, are concerned) being G^*. Hence, for large e, the proportion of α in $\mathbb{F}_{2^e}$ for which $f_2(X) + a$ is irreducible, or has factor patterns (2^3) or $(1^2, 4)$, is $\frac{1}{3}, \frac{1}{6}, \frac{1}{2}$, respectively. In particular, for arbitrary odd e (not necessarily large), every value in $\mathbb{F}_{2^e}$ attained by $f_2(X)$ is attained at precisely two points and so the number of distinct values of f_2 in $\mathbb{F}_{2^e}$ is *exactly* 2^{e-1}.

For $k \geq 3$, as Saxl pointed out to us, no member of $P\Gamma L_2(2^k)$ (in its representation of degree n_k) can be n_k-cycle; thus $f_{k,d}(X) + \alpha$ is reducible over $\mathbb{F}_2(\alpha)$ for every $\alpha \in \overline{\mathbb{F}}_2$. More detailed work on cycle patterns, etc., should yield further interesting facts about factorization.

References

1. S. S. Abhyankar, Galois theory on the line in nonzero characteristic, *Bull. Amer. Math. Soc.* **27** No. 1 (1992), 68–133.
2. S. D. Cohen, The distribution of polynomials over finite fields, *Acta Arith.* **17** (1970), 255–271.
3. S. D. Cohen, Exceptional polynomials and the reducibility of substitution polynomials, *Enseign. Math.* **36** (1990), 53–65.
4. S. D. Cohen, Permutation polynomials and primitive permutation groups, *Arch. Math. (Basel)* **57** (1991), 417–423.

5. S. D. Cohen and R. W. Matthews, A class of exceptional polynomials, *Trans. Amer. Math. Soc.* **345** No. 2 (1994), 897–909.
6. H. Davenport and D. J. Lewis, Notes on congruences, I, *Quart. J. Math. Oxford Ser.* (2) **14** (1963), 51–60.
7. 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. Math.* **11** (1897), 65–120, 161–183.
8. M. Fried, On a conjecture of Schur, *Michigan Math. J.* **17** (1970), 41–55.
9. M. Fried, Arithmetical properties of function fields. II. The generalized Schur problem, *Acta Arith.* **25** (1974), 225–258.
10. M. Fried, Global construction of general exceptional covers, *in* "Finite Fields: Theory, Applications and Algorithms" G. L. Mullen and P. J.-S. Shiue, Eds.), pp. 69–100, Contemporary Mathematics, Vol. 168, Am. Math. Soc., Providence, RI, 1994.
11. M. D. Fried, R. Guralnick, and J. Saxl, Schur covers and Carlitz's conjecture, *Israel J. Math.* **82** (1993), 157–225.
12. R. M. Guralnick and J. Saxl, Monodromy groups of polynomials. preprint.
13. D. R. Hayes, A geometric approach to permutation polynomials over a finite field, *Duke Math. J.* **34** (1967), 293–305.
14. A. A. Klyachko, Monodromy groups of polynomial mappings. *Studies in Number Theory* **6** (1975), 82–91. [in Russian]
15. R. Lidl and R. Matthews, GALOIS: A microcomputer algebra package, *Congr. Numer.* **66** (1988), 145–156.
16. R. Lidl, G. L. Mullen, and G. Turnwald, "Dickson Polynomials," Pitman Monographs and Surveys in Pure and Applied Mathematics, Vol 65. Longman, Essex, England, 1993.
17. M. W. Liebeck, C. E. Praeger, and J. Saxl, The maximal factorisations of the finite simple groups and their automorphism groups, *Mem. Amer. Math. Soc.* (1990), 432.
18. J. P. J. McDermott, Characterisations of some $\frac{3}{2}$-transitive groups, *Math. Z.* **120** (1971), 204–210.
19. J. P. J. McDermott, Transitive permutation groups with 2-point stabilisers of order 2, *Math. Z.* **157** (1977), 37–41.
20. P. Müller, New examples of exceptional polynomials, *in* "Finite Fields: Theory, Applications and Algorithms" (G. L. Mullen and P. J.-S. Shiue, Eds.), pp. 245–250, Contemporary Mathematics, Vol. 168, Am. Math. Soc., Providence, RI, 1994.
21. T. Tsuzuku, "Finite Groups and Finite Geometries," Cambridge Univ. Press, Cambridge, UK, 1982.
22. H. Wielandt, "Finite Permutation Groups," Academic Press, New York, 1964.
23. K. S. Williams, Note on Dickson's permutation polynomials, *Duke Math. J.* **38** (1971), 659–665.