Proceedings of the Edinburgh Mathematical Society (1995) **38**, 133–149 ©

THE NUMBER OF PERMUTATION POLYNOMIALS OF THE FORM $f(x)$ cx OVER A FINITE FIELD

by DAQING WAN*, GARY L. MULLEN** and PETER JAU-SHYONG SHIUE*

(Received 17th June 1993)

Let F_q be the finite field of q elements. Let $f(x)$ be a polynomial of degree d over F_q and let r be the least non-negative residue of $q-1$ modulo d. Under a mild assumption, we show that there are at most r values of $c\in F_q$ such that $f(x)+cx$ is a permutation polynomial over F_q. This indicates that the number of permutation polynomials of the form $f(x)+cx$ depends on the residue class of $q-1$ modulo d.

As an application we apply our results to the construction of various maximal sets of mutually orthogonal latin squares. In particular for odd $q=p^n$ if $\tau(n)$ denotes the number of positive divisors of n, we show how to construct $\tau(n)$ nonisomorphic complete sets of orthogonal squares of order q, and hence $\tau(n)$ nonisomorphic projective planes of order q. We also provide a construction for translation planes of order q without the use of a right quasifield.

1991 *Mathematics subject classification:* primary 11T06, 05B15.

1. Introduction

Let F_q be the finite field of q elements with characteristic p. Let $f(x)$ be a polynomial over F_q of degree $d(1<d<q)$. If $f(x)$ induces a one–one map of F_q to itself, then $f(x)$ is called a permutation polynomial (PP). Motivated by various combinatorial applications, it is of interest to study the number $C(f)$ of PPs of the form $f(x)+cx$, where $f(x)$ is fixed and c varies in F_q, (see [**6–8, 13–14, 16–17**]). Several bounds are currently known. Using Fried's characterization of PPs as in his proof of the Schur conjecture in [**10**], Cohen [**3**] proved the Chowla–Zassenhaus conjecture that $C(f)\leqq 1$ if d is not divisible by p and q is sufficiently large compared to d. This result was recently generalized to PPs of the form $f(x)+cg(x)$ by Cohen, Mullen and Shiue [**4**] where $g(x)$ is a polynomial over F_q.

In his thesis [**1**], Chou showed that

$$C(f)\leqq q-1-d. \tag{1.1}$$

If $C(f)\geqq 2$ it was proved in [**17**] for odd q and in [**20**] for even q that $d\leqq q-3$. A

*These authors would like to thank UNLV for partial support by the University Research Grants and Fellowship Committee. The first author would also like to thank the Institute for Advanced Study for its hospitality, and the National Science Foundation and the UNLV Faculty Development Leave Committee for partial support.

**This author would like to thank the National Security Agency for partial support under grant agreement #MDA904-92-H-3044.

https://doi.org/10.1017/S001309150000626X Published online by Cambridge University Press

generalization of Chou's bound for prime q was obtained by Stothers [19]. The following bound was given by Evans, Greene and Niederreiter [8]:

$$C(f) \leqq q - \frac{q-1}{d-1}. \tag{1.2}$$

In the case that q is an odd prime, they showed that

$$C(f) \leqq (q-3)/2. \tag{1.3}$$

But (1.1) and (1.3) are best possible for polynomials of the form $x^{(q+1)/2} + cx$.

In this paper, we give a new bound which shows that $C(f)$ depends on the residue class of $q-1$ modulo d. Namely, we have:

Theorem 1.1. *Let $q-1 = \lfloor \frac{q-1}{d} \rfloor d + r$ and $J = \lfloor \frac{q-1}{d} \rfloor + r$. Assume that $1 < d < q$ and that the binomial coefficient $\binom{J}{r}$ is not divisible by pJ as a p-adic integer (that is, the power of p dividing $\binom{J}{r}$ is at most equal to the power of p dividing J). Then,*

$$C(f) \leqq r. \tag{1.4}$$

In the case that $q-1$ is divisible by $d > 1$ (i.e., $r = 0$), Theorem 1.1 reduces to the well known result that there are no PPs of degree $d > 1$, see [13, Cor. 7.5]. In the case that $q-2$ is divisible by d (i.e., $r = 1$), Theorem 1.1 shows that there is at most one PP of the form $f(x) + cx$. If d divides $q-2$, the monomial x^d is a PP. Thus, Theorem 1.1 is best possible in this case. If d divides $q-2$ and $(d, 3) = 1$, the following shows that Theorem 1.1 is also best possible for a more general class of polynomials, the so-called Dickson polynomials of degree d defined for the parameter $a \in F_q$ by

$$D_d(x, a) = \sum_{i=0}^{\lfloor d/2 \rfloor} \frac{d}{d-i} \binom{d-i}{i} (-a)^i x^{d-2i},$$

where $\lfloor d/2 \rfloor$ denotes the largest integer $\leqq d/2$. It is known from [13, Thm. 7.16] that for $a \neq 0$, $D_d(x, a)$ induces a PP on F_q if and only if $(d, q^2 - 1) = 1$. In Section 3, we shall compare the bound in Theorem 1.1. with the true value of $C(f)$ in the case that $f(x)$ is of the form $x^{1+(q-1)/k} + ax$.

The assumption in Theorem 1.1 is automatically satisfied if q is a prime. In general, the assumption in Theorem 1.1 cannot be removed. For example, let us consider the p-linearized polynomial $f_a(x) = x^p - ax$. It is well known that $f_a(x)$ is a PP over F_q if and only if a is not a non-zero $(p-1)$th power in F_q. This implies that $C(x^p) = q - \frac{q-1}{p-1}$. On the other hand, the residue class r of $q-1$ modulo the degree p is seen to be $p-1$. If q is not p and $p > 2$, then $p - 1 < q - \frac{q-1}{p-1}$. This shows that the assumption in Theorem 1.1 cannot be removed. We are indebted to W.-S. Chou for providing the following example which shows that the condition in Theorem 1.1 cannot be replaced by the condition that d is not divisible by p: Let $q=25$ and $f_c(x)=x^7+cx$. One checks that $f_c(x)$ is a PP over F_{25} for exactly 9 values of c and thus, $C(f)=9$.

Note that Theorem 1.1 is also best possible for polynomials of the form $x^{(q+1)/2}+cx$. In this case, it is well known that $C(f)=(q-3)/2$, see Niederreiter and Robinson [**17**]. One checks that $d=(q+1)/2$, $r=(q-3)/2$ and $J=(q-1)/2$. Thus, the binomial coefficient $\binom{J}{r}=(q-1)/2$ is not divisible by p and Theorem 1.1 applies.

Theorem 1.1 can be generalized as follows:

Theorem 1.2. *Let $f(x)$ be a polynomial of degree d over F_q and let $q-1=kd+r$, with $0<r<d$. If for some j, $0\leqq j<k$,*

$$\binom{k+r+j(d-1)}{k-j}\not\equiv 0 \bmod (p(k+r+j(d-1))) \tag{1.5}$$

in the ring of p-adic integers, then

$$C(f)\leqq r+jd. \tag{1.6}$$

We note that if $j=0$, Theorem 1.2 reduces to Theorem 1.1 and if $j=k-1$, Theorem 1.2 reduces to Chou's bound (1.1). An alternate form of Theorem 1.2 is the following.

Theorem 1.3. *If m is a positive integer such that $m\leqq k$ and p does not divide $\frac{1}{m}\binom{md}{m-1}$, then $C(f)\leqq q-1-md$.*

Proof. Taking $j=k-m$, one computes that $k+r+j(d-1)=q-1-m(d-1)$. Thus the combinatorial number

$$\frac{1}{k+r+j(d-1)}\binom{k+r+j(d-1)}{k-j}=\frac{1}{m}\binom{q-2-m(d-1)}{m-1}$$

$$\equiv(-1)^{m-1}\frac{1}{m}\binom{md}{m-1}(\bmod p).$$

The theorem now follows from Theorem 1.2.

Theorem 1.1 can also be generalized as follows: Let $f(x)$ and $g(x)$ be two polynomials over F_q of degrees d_f and d_g, where $d_f>d_g\geqq 1$. Let $C(f,g)$ be the number of PPs of the form $f(x)+cg(x)$ as c runs through the elements of F_q.

Theorem 1.4. *Assume that we can write $q-1=sd_f+rd_g$, where r and s are non-negative integers with r minimal. Assume that the binomial coefficient $\binom{r+s}{r}$ is not divisible by $p(r+s)$ as a p-adic integer. Then,*

https://doi.org/10.1017/S001309150000626X Published online by Cambridge University Press

$$C(f,g)\leqq r.$$

In the case $d_g=1$, Theorem 1.4 reduces to Theorem 1.1. If (d_f,d_g) divides $q-1$ and

$$q>\left(\frac{d_f}{(d_f,d_g)}-1\right)\left(\frac{d_g}{(d_f,d_g)}-1\right),$$

the theory of linear diophantine equations shows that we can always write $q-1=sd_f+rd_g$, where r and s are non-negative integers.

We note that the generalized Carlitz conjecture [21] also indicates that the distribution of PPs depends on the residue class of $q-1$ modulo the degree d. The generalized Carlitz conjecture postulates that if $q>d^4$, then $C(f,g)=0$ if $(d,q-1)>1$. The generalized Carlitz conjecture is now known to be true in most cases in view of the recent work by Fried, Guralnick, and Saxl [11].

2. Proof of Theorems 1.2 and 1.4

Let Q_p be the field of p-adic rational numbers and let K be the unique unramified extension of Q_p with residue field F_p. Let T_q be the set of Teichmüller liftings of F_q in K, that is, T_q is the set of all $b\in K$ satisfying $b^q=b$. Let $F(x)$ be a lifting of $f(x)$ to $K[x]$.

Define $U_q(f)$ to be the smallest positive integer t such that

$$\sum_{x\in T_q} F(x)^t \not\equiv 0 \pmod{pt}. \tag{2.1}$$

One checks that $U_q(f)$ is independent of the choice of the lifting $F(x)$. Furthermore, the number $U_q(f)$ is invariant under linear transformations, in fact, invariant under substitutions of PPs. Note that $U_q(f)\leqq q-1$, (see [23]). Furthermore, $f(x)$ is a PP if and only if $U_q(f)=q-1$. In [23], it was shown that $f(x)$ takes at most $q-U_q(f)$ different values as x runs through F_q provided that $f(x)$ is not a PP. The following lemma shows that the number $U_q(f)$ can also be used to bound $C(f,g)$, which is our main concern here.

Lemma 2.1. *The following inequality holds:*

$$C(f,g)\leqq\frac{U_q(f)d_f-(q-1)}{d_f-d_g}. \tag{2.2}$$

Proof. To simplify notations, we assume that $f(x)$ and $g(x)$ are already lifted to be polynomials of degrees d_f and d_g over K. Let $U=U_q(f)$. If $U=q-1$, then (2.2) is trivial. In the following, we assume that $1\leqq U\leqq q-2$. Then

$$G(c)=\sum_{x\in T_q}(f(x)+cg(x))^U$$

https://doi.org/10.1017/S001309150000626X Published online by Cambridge University Press

$$=\sum_{i=0}^{U}\binom{U}{i}c^i\sum_{x\in T_q}g(x)^i f(x)^{U-i} \tag{2.3}$$

is a polynomial in c, whose coefficients are p-adic integers.

If $f(x)+cg(x)$ is a PP for a given c, then $G(c)$ is divisible by pU. Now, there are $C(f,g)$ PPs of the form $f(x)+cg(x)$. It follows that the equation

$$G(c)\equiv 0 \pmod{pU}, \tag{2.4}$$

has at least $C(f,g)$ different solutions $c\in T_q$. By the definition of U, the constant term of $G(c)$ is not divisible by pU. Removing all of the powers of p from congruence (2.4), we obtain a non-zero polynomial $G^*(c)$ over the finite field F_q whose degree is at most the degree of G, and yet the polynomial $G^*(c)$ has at least $C(f,g)$ distinct roots in F_q. Thus, the degree of $G^*(c)$ is at least $C(f,g)$. This shows that the polynomial $G(c)$ modulo pU has degree at least $C(f,g)$. Thus, there is a positive integer $i\geqq C(f,g)$ such that

$$\binom{U}{i}\sum_{x\in T_q}g(x)^i f(x)^{U-i}\not\equiv 0 \pmod{pU}. \tag{2.5}$$

Since $U\leqq q-1$, q is divisible by pU as a p-adic integer. A necessary condition for (2.5) to be true is that the degree of the polynomial $g(x)^i f(x)^{U-i}$ is at least $q-1$, i.e., $id_g+(U-i)d_f\geqq q-1$. Solving this inequality, we get $i\leqq(Ud_f-(q-1))/(d_f-d_g)$. Since $C(f,g)\leqq i$, the lemma follows.

It is clear that $C(f,g)=C(f+cg,g)$ for all $c\in F_q$ and so Lemma 2.1 immediately implies

Lemma 2.2. *Let*

$$u=\min_{c\in F_q}U_q(f(x)+cg(x)).$$

Then

$$C(f,g)\leqq\frac{ud_f-(q-1)}{d_f-d_g}. \tag{2.6}$$

We now prove Theorem 1.2. Take $t=k+r+j(d-1)$. Since $j\leqq k-1$, we have $t\leqq k+r+(k-1)(d-1)=r+1+(k-1)d=q-d\leqq q-2$. Write

$$(f(x)+cx)^t=\sum_{i=0}^{t}\binom{t}{i}f(x)^i(cx)^{t-i}.$$

For $i=k-j$, the degree of $f(x)^i(cx)^{t-i}$ is $(k-j)d+t-k+j=q-1$. For $i<k-j$, the degree of $f(x)^i(cx)^{t-i}$ is less than $q-1$. Since $\binom{t}{k-j}\not\equiv 0 \pmod{pt}$, we have that

https://doi.org/10.1017/S001309150000626X Published online by Cambridge University Press

$$G(c) \equiv \sum_{x \in T_q} (f(x)+cx)^t \pmod{pt}$$

is a non-zero polynomial in c of degree exactly $t-(k-j)=r+jd<q-1$. Following the argument right after equation (2.4), we deduce that there is at least one $c \in T_q$ such that $G(c)$ is not zero modulo pt. Thus

$$u = \min_{c \in F_q} U_q(f(x)+cx) \leqq t,$$

and hence by (2.6)

$$C(f) \leqq \frac{td-(q-1)}{d-1} = r + jd.$$

To prove Theorem 1.4, we work as above in the p-adic field K. Consider

$$(f(x)+cg(x))^{r+s} = \sum_{i=0}^{r+s} \binom{r+s}{i} c^i g(x)^i f(x)^{r+s-i}. \tag{2.7}$$

The degree of the term $g(x)^r f(x)^s$ is exactly

$$rd_g + sd_f = (q-1).$$

For $i>r$, the degree of $g(x)^i f(x)^{r+s-i}$ is bounded by

$$id_g + (r+s-i)d_f = (r+s)d_f - i(d_f - d_g) < (r+s)d_f - r(d_f - d_g) = q-1.$$

Since $\binom{r+s}{r} \not\equiv 0 \pmod{p(r+s)}$, the above argument and (2.7) show that the polynomial $G(c) = \sum_{x \in T_q} (f(x)+cg(x))^{r+s}$ modulo $p(r+s)$ is a polynomial in c of degree r. It follows that there is at least one $c \in T_q$ such that $G(c) \not\equiv 0 \pmod{p(r+s)}$, that is, $U_q(f(x)+cg(x)) \leqq (r+s)$ for such c. By Lemma 2.2, we obtain

$$C(f,g) \leqq \frac{(r+s)d_f - (q-1)}{d_f - d_g} = r.$$

The theorem is proved.

3. A comparison with earlier bounds

Let k be a positive divisor of $q-1$. Let C_k be the number of PPs over F_q of the form $f_a(x) = x(x^{(q-1)/k} - a)$. Let g be a primitive root of F_q and $\omega = g^{(q-1)/k}$ be a primitive kth root of unity. It can be easily proved (see [1] or Theorem 1.3 in [22]) that $f_a(x)$ is a PP

https://doi.org/10.1017/S001309150000626X Published online by Cambridge University Press

over F_q if and only if there is a permutation π of $\{0,1,\ldots,k-1\}$ such that $g^{i-\pi(i)}(\omega^i-a)$ is a kth power in F_q^* for all $0\leqq i\leqq k-1$.

For a permutation π of $\{0,1,\ldots,k-1\}$, let $C_k(\pi)$ be the set of $a\in F_q$ such that $g^{i-\pi(i)}(\omega^i-a)$ is a kth power in F_q^* for all $0\leqq i<k$. Standard arguments of character sums show that

$$\left|\text{Card}\, C_k(\pi)-\frac{1}{k^k}q\right|\leqq O(\sqrt{q}). \tag{3.1}$$

If π and π' are different permutations, then the corresponding sets $C_k(\pi)$ and $C_k(\pi')$ are disjoint. This follows from the fact that if $\pi\neq\pi'$, then $g^{\pi(i)-\pi'(i)}$ is not a kth power for some i with $0\leqq i\leqq k-1$. Summing (3.1) over all permutations π, we deduce that

$$C_k=\frac{k!}{k^k}q+O(\sqrt{q}). \tag{3.2}$$

If $k=2$, it was noted that the bound in Theorem 1.1 is best possible.

Assume $q\geqq 7$ so that if $k=3$, the degree of $f_a(x)$ is $(q+2)/3$ and $(q-1)=2(q+2)/3+(q-7)/3$. Thus, $\binom{J}{r}=\binom{(q-1)/3}{2}$ is not divisible by p if $p>2$. The bound in Theorem 1.1 gives the estimate $C_3\leqq(q-7)/3$ if $p>2$. Chou's bound [1] gives $C_3\leqq(2q-5)/3$. The bound of Evans, Greene, and Niederreiter [8] is $C_3\leqq q-3$. The actual value of C_3 is $2q/9+O(\sqrt{q})$.

Assume $q\geqq 13$ so that if $k=4$, the degree of $f_a(x)$ is $(q+3)/4$ and $(q-1)=3(q+3)/4+(q-13)/4$. Thus, $\binom{J}{r}=\binom{(q-1)/4}{3}$ is not divisible by p if $p\neq 3,5$. The bound in Theorem 1.1 gives the estimate $C_4\leqq(q-13)/4$ if $p\neq 3,5$ while Chou's bound gives $C_4\leqq(3q-7)/4$ and the bound of Evans, Greene, and Niederreiter is $C_4\leqq q-4$. The actual value of C_4 is $3q/32+O(\sqrt{q})$.

4. Maximal sets of orthogonal latin squares

In this section we present an application of the previous bounds to the construction of maximal sets of mutually orthogonal latin squares (MOLS). Recall that a latin square of order n is an $n\times n$ array consisting of n distinct symbols with the property that each of the n symbols appears once in each row and once in each column. Two such squares are orthogonal if when superimposed, each of the n^2 possible ordered pairs occurs once, and a set of latin squares is orthogonal if any two distinct squares are orthogonal. Finally a set of MOLS is said to be maximal if there is no latin square orthogonal to each square in the set, (see Evans [7]).

In [7] Evans uses orthomorphisms of the additive group of F_p, p prime, to construct maximal sets of MOLS. Specifically an orthomorphism θ of F_q is a PP with $\theta(0)=0$ for which $\theta(x)-x$ is also a PP. Two orthomorphisms θ and ϕ are adjacent if $\theta(x)-\phi(x)$ is a PP. The set of all orthomorphisms of F_p forms a graph called the orthomorphism graph of F_p, denoted by Orth (F_p), where two vertices θ and ϕ are connected by an edge if θ and ϕ are adjacent orthomorphisms. An r-clique of Orth(F_p) is a set of r mutually

https://doi.org/10.1017/S001309150000626X Published online by Cambridge University Press

adjacent orthomorphisms and it is a maximal clique if it cannot be extended to a larger clique.

As indicated in [7], an r-clique of $\mathrm{Orth}(G)$ where G is a group of order n, can be used to construct a set of $r+1$ MOLS of order n, and the set of MOLS is maximal whenever the r-clique is maximal. More specifically if $G=\{g_1,\dots,g_n\}$ and $\theta_1,\dots,\theta_r$ form an r-clique of $\mathrm{Orth}(G)$, then define $n\times n$ matrices $L_0,L_1,\dots,L_r$ as follows. The (i,j) entry of L_0 is g_i+g_j and the (i,j) entry of L_k is $g_i+\theta_k(g_j)$ for $k=1,\dots,r$. Moreover $L_0,L_1,\dots,L_r$ are MOLS of order n.

The motivation for studying orthomorphisms comes from the long standing conjecture that every projective plane of prime order is Desarguesian, see Dénes and Keedwell [5, p. 276]. The linear PPs ax with $a\neq 1\in F_p$ clearly form a $(p-2)$-clique in $\mathrm{Orth}(F_p)$ and it was shown by Evans and McFarland in [9] that the existence of another $(p-2)$-clique in $\mathrm{Orth}(F_p)$ distinct from the linear one would imply the existence of a non-Desarguesian affine plane of order p which admits translations. Such planes have long been conjectured not to exist.

We first turn to the construction of nonisomorphic planes through the use of orthomorphisms of finite fields. We first prove the elementary lemma:

Lemma 4.1. *Let $q=p^n$ and let $0\leqq k<n$. Then the number of PPs of F_p of the form $x^{p^k}+bx$ with $b\in F_q$ is given by $q-(q-1)/(q-1,p^k-1)$.*

Proof. We first note that $f(x)=x^{p^k}+bx$ is a p-linearized polynomial and so it is a PP of F_q if and only if $f(x)=0$ has no nonzero solution in F_q, see Lidl and Niederreiter [13, Thm. 7.9]. Thus the number of $b\in F_q$ for which $f(x)$ is not a PP is the number of nonzero elements of F_q in the value set of the polynomial x^{p^k-1}, which is $(q-1)/(q-1,p^k-1)$.

Let $e=q-(q-1)/(q-1,p^k-1)$ and suppose that $x^{p^k}+c_ix$ is a PP of F_q for e elements $c_1,\dots,c_e\in F_q$. By making the linear substitution $x\to(1/(c_1-c_2))x$, we may assume that $c_1-1=c_2$ so that $f(x)=ax^{p^k}+c_1x$, with $a\neq 0$, is an orthomorphism. For $i=3,\dots,e$, let $d_i=c_1-c_i$ so that

$$f(x)-d_ix=ax^{p^k}+c_ix,\ a\neq 0,$$

is a PP of F_q for $i=3,\dots,e$. Thus $f(x)$ is adjacent to the linear orthomorphisms $d_3x,\dots,d_ex$.

Suppose now that $g(x)=bx^{p^k}+cx$ is an orthomorphism which is adjacent to $d_3x,\dots,d_ex$. Let $N=(q-1)/(q-1,p^k-1)$. Then $b^N-(d_i-c)^N\neq 0$ for $i=3,\dots,e$. Moreover the d_i consist of all elements $d\in F_q$ such that $a^N-(d-c_1)^N\neq 0$. Hence whenever

$$b^N-(d-c)^N=0, \tag{4.1}$$

then

$$a^N-(d-c_1)^N=0. \tag{4.2}$$

Now (4.1) has N solutions $d=c+ub$, parameterized by the Nth roots of unity, which we denote by u. Substituting d into (4.2) we obtain the identity

$$a^N=(c-c_1+ub)^N=b^N+Nb^{N-1}(c-c_1)u^{N-1}+\cdots+(c-c_1)^N.$$

This is a polynomial equation in u of degree at most $N-1$, and yet it has N solutions u. Thus the polynomial must be identically zero. In particular we have $c_1=c$ and $b^N=a^N$. Writing $b=ua$ with u an Nth root of unity in F_q, we have $g_u(x)=uax^{p^k}+c_1x$. Indeed as u runs through the Nth roots of unity, each such $g_u(x)$ is adjacent to d_ix for $i=3,\ldots,e$. Moreover these $g_u(x)$ are adjacent to each other.

Hence a family of adjacent orthomorphisms is given by the $g_u(x)$ and $d_3x,\ldots,d_ex$. The cardinality of this family is $N+e-2=q-2$, which implies that we have a maximal $(q-2)$-clique in $\mathrm{Orth}(F_q)$. This in turn implies the existence of a complete set of $q-1$ MOLS of order q. Hence for a, c_1 and d_i for $i=3,\ldots,e$ as above, we have proved:

Theorem 4.2. *For $q=p^n$, let $0\leqq k<n$ and set $N=(q-1)/(q-1,p^k-1)$. Let u be a primitive Nth root of unity in F_q. Then the polynomials*

$$au^jx^{p^k}+c_1x,\ j=1,\ldots,N$$
$$d_ix,\ i=3,\ldots,e,$$

form a maximal $(q-2)$-clique in $\mathrm{Orth}(F_q)$.

Given a polynomial $f(x,y)$ over F_q we may form a $q\times q$ square by placing the element $f(x,y)$ at the intersection of row x and column y of the square.

Corollary 4.3. *Using the notation from Theorem 4.2, the polynomials*

$$\begin{gathered} au^jx^{p^k}+c_1x+y,\ j=1,\ldots,N \\ d_ix+y,\ i=3,\ldots,e \\ x+y, \end{gathered} \tag{4.3}$$

represent a complete set of $q-1$ MOLS of order q.

Given $q=p^n$ with $n\geqq 2$, it is natural to ask as one varies k with $0\leqq k<n$, how many different or inequivalent complete sets of MOLS of order q do we obtain? Recall from Dénes and Keedwell [5, p. 168], that two complete sets of MOLS of the same order are equivalent or isomorphic, if the squares of the two sets can be put into one-to-one correspondence in such a way that by renaming symbols and/or reordering or permuting the rows and columns of each square in one set, we obtain the squares of the second set. It is well known that the existence of a complete set of MOLS of order n is equivalent to the existence of a finite projective plane of order n, and that non-isomorphic complete sets of MOLS correspond to non-isomorphic projective planes, i.e.

https://doi.org/10.1017/S001309150000626X Published online by Cambridge University Press

to projective planes whose co-ordinatizing planar ternary rings are non-isomorphic, see Dénes and Keedwell [5, p. 481].

Corollary 4.4. *For each $n \geqq 2$ and any odd prime p, the above construction gives $\tau(n) \geqq 2$, non-isomorphic projective planes of order p^n, where $\tau(n)$ denotes the number of positive divisors of n.*

Proof. We first note that $(p^n-1, p^k-1) = p^{(n,k)}-1$, and so we have $\tau(n)$ different values of N in Theorem 4.2. We now show that each of these leads to a non-isomorphic plane. Recall from Lidl and Niederreiter [13, Cor. 7.5], that if f is a PP of F_q of degree $n > 1$, then n cannot divide $q-1$.

For $0 \leqq k < n$, let $M(k)$ be the complete set of MOLS of order q constructed in the above way using the integer k. We want to show that if k_1 and k_2 are two integers in the interval $[0, n)$ satisfying $(n, k_1) \neq (n, k_2)$, then $M(k_1)$ and $M(k_2)$ are not isomorphic. Without loss of generality, we may assume that $(n, k_2) > (n, k_1) > 0$. Suppose there is an isomorphism ϕ between $M(k_1)$ and $M(k_2)$ via the row permutation $\sigma_r(x) = \sum_{i=0}^{q-2} r_i x^i$, the column permutation $\sigma_c(y) = \sum_{i=0}^{q-2} c_i y^i$ and the symbol permutation $\sigma_s(z) = \sum_{i=0}^{q-2} s_i z^i$. We want to derive a contradiction.

In the construction of $M(k)$, there are $(q-1)/(q-1, p^k-1)$ non-linear polynomials if $k > 0$ and there are no non-linear polynomials if $k = 0$. Let

$$N(k_1, k_2) = \begin{cases} q-1-\dfrac{q-1}{(q-1, p^{k_1}-1)} - \dfrac{q-1}{(q-1, p^{k_2}-1)} & \text{if } k_2 > 0 \\[2ex] q-1-\dfrac{q-1}{(q-1, p^{k_1}-1)} & \text{if } k_2 = 0. \end{cases}$$

The isomorphism ϕ will take at least $N(k_1, k_2)$ linear polynomials in $M(k_1)$, (say, $d_i x + y$, $1 \leqq i \leqq N(k_1, k_2)$, $d_i \neq 0$) to $N(k_1, k_2)$ linear polynomials in $M(k_2)$, (say, $e_i x + y$, $1 \leqq i \leqq N(k_1, k_2)$, $e_i \neq 0$). Since the isomorphism ϕ is obtained via the row permutation $\sigma_r(x)$, the column permutation $\sigma_c(y)$ and the symbol permutation $\sigma_s(z)$, it follows that

$$d_i \sigma_r(x) + \sigma_c(y) = \sigma_s(e_i x + y), \quad 1 \leqq i \leqq N(k_1, k_2), \tag{4.4}$$

for all x, $y \in F_q$. The left hand side of (4.4) has no terms divisible by xy and thus it is easy to see that $\sigma_s(z)$ has to be a p-linearized polynomial.

Since $N(k_1, k_2) > 1$, comparing the constant terms on both sides of (4.4), we see that $\sigma_r(x)$ also has no constant term. Using this fact and comparing the x-part and y-part in (4.4), we deduce that

$$\sigma_c(y) = \sigma_s(y) \tag{4.5}$$

$$d_i \sigma_r(x) = \sigma_s(e_i x), \quad 1 \leqq i \leqq N(k_1, k_2). \tag{4.6}$$

Equation (4.6) shows that $\sigma_r(x)$ and $\sigma_s(x)$ have the same non-zero terms except that

https://doi.org/10.1017/S001309150000626X Published online by Cambridge University Press

their coefficients may be different. In particular, both $\sigma_r(x)$ and $\sigma_s(x)$ are p-linearized polynomials without constant terms. Thus we may write

$$\sigma_s(x)=a_1x^{p^{j_1}}+a_2x^{p^{j_2}}+\ldots,\ j_1>j_2>\cdots\geqq 0,$$
$$\sigma_r(x)=b_1x^{p^{j_1}}+b_2x^{p^{j_2}}+\ldots,\ j_1>j_2>\cdots\geqq 0,$$

where $a_1b_1\neq 0$. We claim that all other coefficients in $\sigma_s(x)$ and $\sigma_r(x)$ are zero.

If the claim is not true, we may assume that $a_2b_2\neq 0$. Equation (4.6) then shows

$$d_ib_1=a_1(e_i)^{p^{j_1}} \text{ and } d_ib_2=a_2(e_i)^{p^{j_2}},\ 1\leqq i\leqq N(k_1,k_2).$$

Thus we have

$$\frac{b_1}{b_2}=\frac{a_1}{a_2}(e_i)^{p^{j_1}-p^{j_2}}=\frac{a_1}{a_2}(e_i^{p^{j_2}})^{p^{j_1-j_2}}-1.$$

However the equation

$$\frac{b_1}{b_2}=\frac{a_1}{a_2}x^{p^{j_1-j_2}}-1$$

has at most $p^{(j_1-j_2,n)}-1\leqq p^{n/2}-1$ solutions in F_q. Thus we have the inequality

$$p^{n/2}-1\geqq N(k_1,k_2). \tag{4.7}$$

If $k_2=0$, then

$$N(k_1,k_2)=q-1-\frac{q-1}{(q-1,p^{k_1}-1)}\geqq(q-1)\left(1-\frac{1}{3-1}\right)=\frac{q-1}{2}.$$

However $(q-1)/2>p^{n/2}-1$ for $p\geqq 3$ and $n\geqq 2$. This contradicts (4.7).

If $k_2>0$, then $(k_2,n)>(k_1,n)>0$ and so we have $(k_2,n)\geqq 2$, $n\geqq 3$. Furthermore in this case,

$$N(k_1,k_2)\geqq(q-1)\left(1-\frac{1}{3-1}-\frac{1}{3^2-1}\right)=\frac{3}{8}(q-1).$$

One checks that $\frac{3}{8}(q-1)>p^{n/2}-1$ for $p\geqq 3$, $n\geqq 3$. This again contradicts (4.7). Thus we have proved the claim that $\sigma_s(x)=a_1x^{p^{j_1}}$ and $\sigma_r(x)=a_2x^{p^{j_2}}$.

Since $0<(n,k_1)<(n,k_2)$, there are more non-linear polynomials in $M(k_1)$ than in $M(k_2)$. Thus, the isomorphism ϕ will take one of the latin squares constructed from a non-linear polynomial (say $ax^{p^{k_1}}+c_1x+y$), to a latin square in $M(k_2)$ constructed from a linear polynomial, (say $ex+y$). Thus

https://doi.org/10.1017/S001309150000626X Published online by Cambridge University Press

$$a(\sigma_r(x))^{p^{k_1}}+c_1\sigma_r(x)+\sigma_c(y)=\sigma_s(ex+y).$$

Since $\sigma_c(x)=\sigma_s(x)=a_1x^{p^{j_1}}$, $\sigma_r(x)=a_2x^{p^{j_1}}$, the above equation simplifies to

$$a(a_2x^{p^{j_1}})^{p^{k_1}}+c_1(a_2x^{p^{j_1}})=a_1(ex)^{p^{j_1}}. \tag{4.8}$$

Since $0<(n,k_1)<(n,k_2)$, and thus $0<k_1<n$, we have $p^{j_1+k_1}\not\equiv p^{j_1} \bmod (q-1)$. Thus the left hand side of (4.8) has two nonzero terms while the right hand side has only one. We have thus proved that no isomorphism can hold between $M(k_1)$ and $M(k_2)$, and so the proof is complete.

Alternatively we have:

Corollary 4.5. *For each $n\geqq 2$ and any odd prime p, the above construction gives $\tau(n)\geqq 2$, non-isomorphic affine translation planes of order p^n.*

Proof. This follows from Hachenberger and Jungnickel [**12**, p. 301] where it is shown that $s-2$ pairwise orthogonal orthomorphisms of a group G of order s describe an affine translation plane if and only if these orthomorphisms are in fact fixed point free group automorphisms.

It may be worth remarking here that this construction gives for any odd prime p, a non-Desarguesian affine translation plane of order p^2, constructed without the use of a right quasifield as used in Dénes and Keedwell [**5**, p. 278$^+$]. As an illustration for the smallest case of $q=9$, let F_9 be generated by the primitive polynomial $f(x)=x^2+2x+2$ over F_3. Let α be a root of $f(x)$ in an extension field. The MOLS corresponding to the Desarguesian plane of order 9 may be constructed by using the polynomials

$$f_{\alpha^i}(x,y)=\alpha^i x+y,\ i=0,\ldots,7. \tag{4.6}$$

Since $u=\alpha^2$ is a primitive 4th root of unity, the construction from Corollary 4.3 leads to the polynomials

$$\begin{matrix}\alpha x^3+y & \alpha^5x^3+y\\ \alpha^3x^3+y & \alpha^7x^3+y,\end{matrix} \tag{4.7a}$$

which represent 4 MOLS. To complete the set to 8 MOLS of order 9, we consider the linear polynomials

$$\begin{matrix}\alpha^2x+y & \alpha^6x+y\\ \alpha^4x+y & x+y.\end{matrix} \tag{4.7b}$$

Thus four of the squares are the same in both the Desarguesian and non-Desarguesian constructions.

https://doi.org/10.1017/S001309150000626X Published online by Cambridge University Press

Before considering a different type of orthomorphism of F_q, we mention the following conjecture of Evans, Green and Niederreiter [**8**, Conj. 2].

Conjecture. *Let f be a polynomial over F_q such that $f(x)+cx$ is a PP of F_q for at least $\lfloor q/2 \rfloor$ values of $c \in F_q$. Then $f(x)-f(0)$ is a linearized p-polynomial over F_q.*

By a linearized p-polynomial is meant a polynomial each of whose terms has degree equal to a power of p, (see [**13**, Defn. 3.49]). In [**8**] it is shown that the conjecture is true for $q=p$ a prime, and it is also true for $f(x)=x^e$ with $0<e<q$. The truth of this conjecture would have implications for the construction of sets of MOLS of order q via automorphisms of the field F_q.

We now turn to a study of orthomorphisms over F_q of the form $ax^{(q+1)/2}+bx$. In [**7**] for p an odd prime, Evans used PPs of the form $ax^{(p+1)/2}+bx$ to construct a maximal set of $(p-3)/2$ MOLS of order p if $p\equiv 3 \pmod 4$ and a maximal set of $(p-1)/2$ MOLS if $p\equiv 1 \pmod 4$. Let $f(x)=ax^{(p+1)/2}+bx$ with a, $b \in F_p$, p prime. As indicated after Theorem 1.1, with $d=(p+1)/2$, $r=(p-3)/2$ and $J=(p-1)/2$, the binomial coefficient $\binom{J}{r}=(p-1)/2$ is not divisible by p so Theorem 1.1 applies. As a result it is clear that an orthomorphism over F_q of the form $ax^{(q+1)/2}+bx$ can be adjacent to at most $(q-7)/2$ linear orthomorphisms αx. Moreover from Niederreiter and Robinson [**17**, Thm. 5 and Remark 1], for every odd prime power q there are orthomorphisms of the form $ax^{(q+1)/2}+bx$ which are indeed adjacent to exactly $(q-7)/2$ linear orthomorphisms.

What if $q=p^n$ is a prime power with $n>1$. For $q=9$, Evans [**7**] exhibits a maximal set of 6 (quadratic) orthomorphisms of the form $ax^{(q+1)/2}+bx$ and a linear orthomorphism which yields a maximal 7-clique in Orth (F_9) and hence a complete set of 8 MOLS of order 9 which can be used to construct the dual translation plane of order 9, (see [**5**, p. 280–281] and [**12**, p. 301]).

From this example one might suspect that for any odd prime power $q=p^n$ with $n>1$, it is possible to construct a complete set of $q-1$ MOLS of order q using orthomorphisms of the form $ax^{(q+1)/2}+bx$ and linear orthomorphisms. However to the contrary, Pott in [**18**] conjectures that for any odd $q=p^n$ with $n>1$ except for $q=9$, no orthomorphism of the form $ax^{(q+1)/2}+bx$ leads to a maximal clique with $q-2$ elements. Instead Pott conjectures as in the case of prime p, that except for $q=9$, there are such polynomials leading to maximal sets of MOLS with $(q-3)/2$ squares if $q\equiv 3 \pmod 4$ and with $(q-1)/2$ squares if $q\equiv 1 \pmod 4$. While Pott bases his conjecture on computer evidence from the cases $q=25$, 27, and 49, we provide the following results toward the proof of Pott's conjecture. First any polynomial $ax^{(q+1)/2}+bx$ meeting the bound in Theorem 1.1 can be used to construct a set of $(q-3)/2$ MOLS of order q if $q\equiv 3$ (mod 4) and $(q-1)/2$ MOLS if $q\equiv 1 \pmod 4$. As indicated earlier, from [**17**] such polynomials exist for all odd q. In addition we prove:

Theorem 4.6. (*i*) *If the orthomorphism $g(x)$ is adjacent to $(q-7)/2$ linear orthomorphisms over F_q, then the degree of $g(x)\leq(q+1)/2$.*

(*ii*) *Let $e=(q-3)/2$ and let $f(x)=ax^{(q+1)/2}+bx$ with $a\neq 0$ be another polynomial such that $f(x)-d_ix$ is a PP for $i=1,\dots,e$. Let $g(x)=a_1x^{(q+1)/2}+b_1x$ with $a_1\neq 0$ be another* *polynomial such that $g(x)-d_ix$ is a PP for $i=1,\dots,e$. If $q>9$, then $b_1=b$ and $a_1=a$ or $a_1=-a$.*

Proof. Part (i) follows immediately from Chou [**2**, Thm. 5] or [**1**, Thm 2.3.3] where it is shown that if $f(x)+bx$ is a PP for m values of $b\in F_q$, then the degree of f is at most $q-1-m$.

For (ii), let $t_1(i)=(b-d_i)/a$ and $t_2(i)=(b_1-d_i)/a_1$. Hence

$$t_2(i)=(a/a_1)t_1(i)+(b_1-b)/a_1=At_1(i)+B.$$

Let η denote the quadratic character on F_q. The binomial $x^{(q+1)/2}+tx$ is a PP if and only if $\eta(t^2-1)=1$, (see [**13**, Thm. 7.11]). Thus the $t_1(i)$'s are characterized by the condition $\eta(t_1^2-1)=1$. Similarly the $t_2(i)$'s are characterized by the condition $\eta(t_2^2-1)=1$. The relation $t_2(i)=At_1(i)+B$ shows that if $t\in F_q$ with $t^2\neq 1$ and $(At+B)^2\neq 1$, then $\eta(t^2-1)=\eta((At+B)^2-1)$. As a result $(t^2-1)((At+B)^2-1)$ is either a nonzero square or zero for all $t\in F_q$. If for some t, $t^2\neq(At+B)^2$, then by Weil's estimate for character sums, [**13**, Thm. 5.41], we have

$$q-4\leqq\sum_{t\in F_q}\eta((t^2-1)((At+B)^2-1))\leqq 3\sqrt{q}.$$

This is impossible if $q>16$, or equivalently if $q>9$ since q is odd and not prime. Finally $t^2=(At+B)^2$ for all $t\in F_q$ implies $B=0$ and $A=1$ or -1, and thus $b_1=b$ and $a_1=a$ or $a_1=-a$, which completes the proof.

It may be of interest to give the polynomials over F_9 which represent the dual of the translation plane of order 9, (see Dénes and Keedwell [**5**, p. 280]). As in the previous example, we assume F_9 is generated by a root α of x^2+2x+2 over F_3. In this case 6 of the MOLS of order 9 are represented by the polynomials

$$\begin{array}{cc} \alpha^2x^5+y & \alpha^6x^5+y \\ \alpha^2x^5+x+y & \alpha^6x^5+x+y \\ \alpha^2x^5+2x+y & \alpha^6x^5+2x+y. \end{array} \tag{4.8a}$$

To complete the set we consider the linear polynomials

$$\alpha^4x+y \quad x+y. \tag{4.8b}$$

We thus note that two of the MOLS occur in each of the three non-isomorphic complete sets of MOLS of order 9, namely those represented by α^4x+y and $x+y$. We also note from the proof of Corollary 4.5, that since six of these orthomorphisms are not automorphisms of F_9, the corresponding plane is not isomorphic to an affine translation plane.

https://doi.org/10.1017/S001309150000626X Published online by Cambridge University Press

As noted in Evans [7] for an odd prime p, the quadratic orthomorphism of F_p defined by

$$x \to \begin{cases} ax & \text{if } x \text{ is a nonzero square} \\ bx & \text{if } x \text{ is a nonsquare} \\ 0 & \text{if } x=0, \end{cases}$$

can be represented in the form

$$\frac{a-b}{2}x^{(p+1)/2}+\frac{a+b}{2}x. \tag{4.9}$$

This can clearly be extended to F_q where q is any odd prime power. The structure of the group of all PPs of the form (4.9) was determined in Mullen and Niederreiter [15].

More generally if $e|(q-1)$, then every element $x \in F_q^*$ can be written in the form $x=\gamma^{ek+j}$ for some $j=0,\ldots,e-1$ with γ a primitive element of F_q. Consider the map $f: F_q \to F_q$ defined by $x \to a_j x$ for $x \neq 0$ and $f(0)=0$. Let ω be a primitive eth root of unity in F_q. Then generalizing (4.9), $f(x)$ can be represented via the polynomial

$$f(x)=\frac{1}{e}\sum_{i=0}^{e-1}\sum_{j=0}^{e-1}\omega^{j(i+1)}a_j x^{(i(q-1)/e)+1}. \tag{4.10}$$

As indicated earlier, PPs of the form (4.9) meet the bound from Theorem 1.1 while those of the form (4.10) in general do not. However if $e=(q-1)/2$, then one can construct a PP of the form (4.10) with degree $q-2$ and so we obtain another class of PPs meeting the bound in Theorem 1.1. We also point out that Wan and Lidl in [22] have determined the structure of the group of all PPs of the form (4.10).

We close by pointing out several results concerning the existence of orthomorphisms of F_p, p prime, which show that they must have degrees which are relatively large. For example from Cohen's proof [3] of the Chowla–Zassenhaus conjecture, if f is an orthomorphism of F_p of degree n, then n must satisfy $p \leqq (n^2-3n+4)^2$. In addition if f and g are adjacent orthomorphisms of degree n over F_p and t is the degree of $f-g$, then Cohen, Mullen, and Shiue [4] shows that if $p>(n^2-3n+4)^2$, then $t \geqq 3n/5$ and $(t,n)>1$. We also mention in closing that if an orthomorphism f is adjacent to m linear orthomorphisms, then by Chou [1, 2], the degree of f is at most $q-m-3$.

Acknowledgement. We would like to thank D. Jungnickel and C. F. Laywine for helpful comments regarding Section 4. We would also like to thank the referee for several helpful comments.

REFERENCES

1. W.-S. Chou, *Permutation Polynomials and Combinatorial Applications* (Ph.D. thesis, Pennsylvania State University, 1990).

https://doi.org/10.1017/S001309150000626X Published online by Cambridge University Press

2. W.-S. Chou, Set-complete mappings on finite fields, in *Finite Fields, Coding Theory, and Advances in Communications and Computing* (Proc. of the Las Vegas Conference of the same title, Aug. 1991, edited by G. L. Mullen and P. J.-S. Shiue, Lecture Notes in Pure and Applied Mathematics, **141**, Marcel Dekker, 1993), 33–41.

3. S. D. Cohen, Proof of a conjecture of Chowla and Zassenhaus on permutation polynomials, *Canad. Math. Bull.* **33** (1990), 230–234.

4. S. D. Cohen, G. L. Mullen and P. J.-S. Shiue, The difference between permutation polynomials over finite fields, *Proc. Amer. Math. Soc.*, to appear.

5. J. Dénes and A. D. Keedwell, *Latin Squares and their Applications* (Academic Press, New York, 1974).

6. A. B. Evans, Orthomorphisms of $GF(q)^+$, *Ars. Combin.* **27** (1989), 121–132.

7. A. B. Evans, Maximal sets of mutually orthogonal Latin squares, II, *European J. Combin.* **13** (1992), 345–350.

8. R. J. Evans, J. Greene and H. Niederreiter, Linearized polynomials and permutation polynomials of finite fields, *Michigan Math. J.* **39** (1992), 405–413.

9. A. B. Evans and R. L. McFarland, Planes of prime order with translations, *Congr. Numer.* **44** (1984), 41–46.

10. M. Fried, On a conjecture of Schur, *Michigan Math. J.* **17** (1970), 41–55.

11. M. D. Fried, R. Guralnick and J. Saxl, Schur covers and Carlitz's conjecture, *Israel J. Math.* **82** (1993), 157–225.

12. D. Hachenberger and D. Jungnickel, Bruck nets with a transitive direction, *Geom. Dedicata* **36** (1990), 287–313.

13. R. Lidl and H. Niederreiter, *Finite Fields* (Addison-Wesley Publishing Company, 1983) (now distributed by Cambridge University Press).

14. G. L. Mullen, Permutation polynomials over finite fields, in *Finite Fields, Coding Theory, and Advances in Communications and Computing* (Proc. of the Las Vegas Conference of the same title, Aug. 1991, edited by G. L. Mullen and P. J.-S. Shiue, Lecture Notes in Pure and Applied Mathematics, 141, Marcel Dekker, 1993, 131–151.

15. G. L. Mullen and H. Niederreiter, The structure of a group of permutation polynomials, *J. Austral. Math. Soc. Ser. A* **38** (1985), 164–170.

16. H. Niederreiter, Finite fields and their applications, *Contributions to General Algebra* **7** (Proc. Vienna Conf., 1990, Teubner, Stuttgart, 1991), 251–264.

17. H. Niederreiter and K. H. Robinson, Complete mappings of finite fields, *J. Austral. Math. Soc. Ser. A* **33** (1982), 197–212.

18. A. Pott, Maximal difference matrices of order q, *J. Combin. Designs*, to appear.

19. W. W. Stothers, On permutation polynomials whose difference is linear, *Glasgow Math. J.* **32** (1990) 165–171.

20. D. Wan, On a problem of Niederreiter and Robinson about finite fields, *J. Austral. Math. Soc. Ser. A* **41** (1986), 336–338.

21. D. Wan, A generalization of the Carlitz conjecture, in *Finite Fields, Coding Theory, and Advances in Communications and Computing* (Proc. of the Las Vegas Conference of the same title, Aug. 1991, edited by G. L. Mullen and P. J.-S. Shiue, Lecture Notes in Pure and Applied Mathematics, **141**, Marcel Dekker, 1993), 431–432.

https://doi.org/10.1017/S001309150000626X Published online by Cambridge University Press

22. D. Wan and R. Lidl, Permutation polynomials of the form $x^t f(x^{(q-1)/d})$ and their group structure, *Monatsh. Math.* **112** (1991), pp. 149–163.

23. D. Wan, P. J.-S. Shiue and C. S. Chen, Value sets of polynomials over finite fields, *Proc. Amer. Math. Soc.* **119** (1993), 711–717.

Department of Mathematical Sciences
University of Nevada, Las Vegas
Las Vegas, NV 89154
USA
e-mail: dwan@nevada.edu

Department of Mathematical Sciences
University of Nevada, Las Vegas
Las Vegas, NV 89154
USA
e-mail: shiue@nevada.edu

Department of Mathematics
The Pennsylvania State University
University Park, PA 16802
USA
e-mail: mullen@math.psu.edu

https://doi.org/10.1017/S001309150000626X Published online by Cambridge University Press