Canad. Math. Bull. Vol. **30** (1), 1987

DICKSON POLYNOMIALS OVER FINITE FIELDS AND COMPLETE MAPPINGS

BY

GARY L. MULLEN* AND HARALD NIEDERREITER

ABSTRACT. Dickson polynomials over finite fields are familiar examples of permutation polynomials, i.e. of polynomials for which the corresponding polynomial mapping is a permutation of the finite field. We prove that a Dickson polynomial can be a complete mapping polynomial only in some special cases. Complete mapping polynomials are of interest in combinatorics and are defined as polynomials $f(x)$ over a finite field for which both $f(x)$ and $f(x) + x$ are permutation polynomials. Our result also verifies a special case of a conjecture of Chowla and Zassenhaus on permutation polynomials.

1. **Introduction and statement of result.** A polynomial $f(x)$ over a finite field F_q with q elements induces a mapping $c \in F_q \rightarrow f(c)$ of F_q into itself, and the Lagrange interpolation formula shows that any mapping of F_q into itself is induced by some polynomial. A polynomial over F_q is called a permutation polynomial of F_q if the induced mapping is a permutation of F_q; see Lausch and Nöbauer [8, Ch. 4] and Lidl and Niederreiter [9, Ch. 8]. A polynomial $f(x)$ over F_q is called a complete mapping polynomial of F_q if both $f(x)$ and $f(x) + x$ are permutation polynomials of F_q. The mapping of F_q into itself induced by a complete mapping polynomial of F_q is called a complete mapping (of the additive group) of F_q. Complete mappings of groups were introduced by Mann [10] in connection with the construction of orthogonal latin squares. A detailed account of the relationship between complete mappings and orthogonal latin squares can be found in Dénes and Keedwell [3]. Recently, the interest in complete mappings has been renewed because of other applications in combinatorics (see Atkin, Hay, and Larson [1], Hsu and Keedwell [5], and Keedwell [6]) and in nonassociative algebra (see Niederreiter and Robinson [11]). A detailed study of complete mappings of finite fields was carried out by Niederreiter and Robinson [12].

An important family of permutation polynomials is formed by the Dickson polynomials (see Dickson [4]). For a positive integer k and an element a of a commutative ring R with identity, the Dickson polynomial $g_k(x, a)$ is defined by

Received by the editors November 13, 1984 and, in revised form, September 4, 1985.

*This author would like to thank the Institute for Algebra and Discrete Mathematics of the Technological University of Vienna for its hospitality during the summer of 1983 when this work was completed.

AMS Subject Classification: 12C05.

$$g_k(x, a) = \sum_{j=0}^{h} \frac{k}{k-j}\binom{k-j}{j}(-a)^j x^{k-2j},$$

where h is the greatest integer $\leq k/2$. We will be interested in the case $R = F_q$. For $a = 0$ we have $g_k(x, 0) = x^k$, so that $g_k(x, 0)$ is a permutation polynomial of F_q if and only if $\gcd(k, q-1) = 1$. For $a \in F_q$ with $a \neq 0$, $g_k(x, a)$ is a permutation polynomial of F_q if and only if $\gcd(k, q^2 - 1) = 1$. See Lausch and Nöbauer [8, Ch. 4], Lidl and Niederreiter [9, Ch. 8], and Williams [14] for proofs of these results. Since Dickson polynomials are frequently used as permutation polynomials, this raises the question to what extent they can also serve as complete mapping polynomials. We consider a slightly more general problem, namely whether a polynomial of the form $bg_k(x, a) + cx$ with $b, c \in F_q$, $bc \neq 0$, can be a permutation polynomial of F_q. For $a = 0$ it was shown by Niederreiter and Robinson [12] that this can only happen if either k is a power of the characteristic of F_q or else q is small in terms of k. We prove that in the more complicated case where $a \neq 0$ we have a rather similar situation. We exclude now the trivial case $k = 1$.

THEOREM. *Let $k \geq 2$ be an integer and let $a, b, c \in F_q$ with $abc \neq 0$. Then $bg_k(x, a) + cx$ can be a permutation polynomial of F_q only in one of the following cases:*

(i) $k = 3$, $c = 3ab$, *and* $q \equiv 2 \bmod 3$;
(ii) $k \geq 3$ *and the characteristic of* F_q *divides* k;
(iii) $k \geq 4$, *the characteristic of* F_q *does not divide* k, *and* $q < (9k^2 - 27k + 22)^2$.

We now show that in each of the cases (i), (ii), and (iii), permutation polynomials of the form $bg_k(x, a) + cx$ can indeed be constructed. To illustrate case (i), put $k = 3$, $c = 3ab$, and note that

$$bg_3(x, a) + cx = b(x^3 - 3ax) + 3abx = bx^3$$

is a permutation polynomial of F_q whenever $q \equiv 2 \bmod 3$. To illustrate case (ii), let p be the characteristic of F_q and let $k \geq 3$ be a power of p. For $a \in F_q$, $a \neq 0$, we have $g_p(x, a) = x^p$, and a repeated application of the substitution formula in [9, p. 359, Eq. (7.10)] yields $g_k(x, a) = x^k$. It follows then from [12, Theorem 10] that there exist infinitely many examples of a finite field F_q of characteristic p and a $b \in F_q$, $b \neq 0$, such that $bg_k(x, a) + x$ is a permutation polynomial of F_q. To illustrate case (iii), choose $k = 5$, $q = 13$, and a nonzero square $a \in F_{13}$, and note that

$$g_5(x, a) + 5a^2x = (x^5 - 5ax^3 + 5a^2x) + 5a^2x = x^5 - 5ax^3 + 3(-5a)^2x$$

is a permutation polynomial of F_{13} by [9, p. 352, Table 7.1] and evidently $13 < (112)^2$.

We remark also that if q divides k, say $k = q^t u$ with $t \geq 1$ and $\gcd(q, u) = 1$, then

$$bg_k(x, a) + cx = bg_u(x, a)^{q^t} + cx,$$

which induces the same mapping as the polynomial $bg_u(x, a) + cx$. This case can therefore be reduced to the one where the characteristic of F_q does not divide the degree

https://doi.org/10.4153/CMB-1987-003-3 Published online by Cambridge University Press

of the Dickson polynomial, leaving only the possibility $u = 1$ or the cases (i) and (iii) in the theorem with u in the role of k.

If we return to the original problem of complete mapping polynomials, then our theorem immediately yields the following result. We remark that the case (i) in the theorem can now be dropped since it follows from [12, Table 2] that for $q \equiv 2 \bmod 3$ there is no complete mapping polynomial of F_q of degree 3.

COROLLARY. *Let $k \geq 2$ be an integer and let $a, b, c \in F_q$ with $ab \neq 0$. Then $bg_k(x, a) + cx$ can be a complete mapping polynomial of F_q only in one of the following cases:*

(i) *$k \geq 3$ and the characteristic of F_q divides k;*
(ii) *$k \geq 4$, the characteristic of F_q does not divide k, and $q < (9k^2 - 27k + 22)^2$.*

We now show that in both cases (i) and (ii), complete mapping polynomials of the form $bg_k(x, a) + cx$ do indeed exist. Case (i) can be illustrated by taking $k = p^\alpha$ and $a, b, c \in F_q$ with $ab \neq 0$ and $c = 0$. It follows from [12, Theorem 10] that there exist infinitely many examples of a finite field F_q of characteristic p and a $b \in F_q$, $b \neq 0$, such that $bg_k(x, a) + cx = bx^k$ is a complete mapping polynomial. Case (ii) can be illustrated by taking $k = 5$, $q = 13$ and letting $a = 5d$ with a nonsquare $d \in F_{13}$, $b = 5d^{-2}$, and $c = 0$, so that $bg_k(x, a) + cx = 5d^{-2}(x^5 + dx^3 + 8d^2x)$ which is a complete mapping polynomial by [12, Table 2].

The proof of the theorem is given in Section 3. A crucial lemma on absolute irreducibility is shown in Section 2. It should be noted that our theorem is also connected with a conjecture of Chowla and Zassenhaus [2] to the effect that if $f(x)$ is a polynomial of degree ≥ 2 over the ring $\mathbb{Z}$ of rational integers and p is a sufficiently large prime for which $f(x)$ is a permutation polynomial of F_p when considered modulo p, then for no $c \in F_p$ with $c \neq 0$ is $f(x) + cx$ a permutation polynomial of F_p. In fact, our theorem verifies this conjecture for $f(x) = bg_k(x, a) + cx$ with $a, b, c \in \mathbb{Z}$ and $ab \neq 0$. The case $f(x) = bg_k(x, 0) + cx = bx^k + cx$ with $b, c \in \mathbb{Z}$ and $b \neq 0$ is settled by Theorem 9 of Niederreiter and Robinson [12].

2. **Absolute irreducibility**.

A polynomial $f(x, y)$ over a field F is called absolutely irreducible over F if it is irreducible over the algebraic closure $\bar{F}$ of F. The following result plays an important role in the proof of the theorem and may also be of independent interest.

LEMMA 1. *Let $k \geq 2$ be an integer and let $a, c \in F$ with $ac \neq 0$. Then the polynomial*

$$f(x, y) = \frac{x^k - a^k y^{2k}}{x - ay^2} \cdot \frac{x^k - 1}{x - 1} + cx^{k-1}y^{k-1}$$

is absolutely irreducible over F in each of the following cases:

(i) *$k = 2$;*
(ii) *$k = 3$, $c \neq 3a$, and the characteristic of F is $\neq 3$;*
(iii) *$k \geq 4$ and the characteristic of F does not divide k.*

PROOF. Suppose one of the conditions (i), (ii), (iii) is satisfied and that $f(x, y)$ is not absolutely irreducible, i.e. that it has a nontrivial factorization over $\bar{F}$. Since the coefficients of $f(x, y)$, considered as a polynomial in y, are relatively prime, this factorization is of the form

$$(1) \qquad f(x, y) = (f_m(x)y^m + \ldots + f_0(x))\,(h_n(x)y^n + \ldots + h_0(x))$$

in $\bar{F}[x][y]$ with $m, n \geq 1$ and $m + n = 2k - 2$. A comparison of leading coefficients yields

$$(2) \qquad a^{k-1}\frac{x^k - 1}{x - 1} = f_m(x)\,h_n(x),$$

so that in particular one of $f_m(x)$ and $h_n(x)$ has positive degree, say w.l.o.g. $f_m(x)$. We will frequently use the fact that in the cases (i), (ii), (iii) the polynomial $(x^k - 1)/(x - 1)$ has no multiple roots.

Let $\zeta \in \bar{F}$ be a root of $f_m(x)$ and substitute $x = \zeta$ in (1). This yields

$$c\zeta^{k-1}\,y^{k-1} = (f_m(\zeta)y^m + \ldots + f_0(\zeta))(h_n(\zeta)y^n + \ldots + h_0(\zeta)).$$

Using $h_n(\zeta) \neq 0$ and unique factorization in $\bar{F}[y]$, we obtain $n \leq k - 1$, $h_j(\zeta) = 0$ for $0 \leq j \leq n - 1$, $f_{k-1-n}(\zeta) \neq 0$, and $f_i(\zeta) = 0$ for $i \neq k - 1 - n$. As this holds for any root ζ of $f_m(x)$, it follows that

$$(3) \qquad f_m(x)|h_j(x) \text{ for } 0 \leq j \leq n - 1,\ f_m(x)|f_i(x) \text{ for } i \neq k - 1 - n.$$

If $n < k - 1$, then (3) implies $f_m(x)|h_0(x), f_m(x)|f_0(x)$. Comparing constant coefficients in (1), we get

$$(4) \qquad x^{k-1}\frac{x^k - 1}{x - 1} = f_0(x)\,h_0(x).$$

It follows that $f_m^2(x)$ divides $(x^k - 1)/(x - 1)$, a contradiction.

Thus we must have $n = k - 1$, hence also $m = k - 1$. If $h_{k-1}(x)$ is constant, then (2) and (3) yield

$$(5) \qquad \frac{x^k - 1}{x - 1}\,\Big|\, f_i(x),\ \frac{x^k - 1}{x - 1}\,\Big|\, h_i(x) \text{ for } 1 \leq i \leq k - 2,$$

$$(6) \qquad f_{k-1}(x)\,|\,h_0(x),\ h_{k-1}(x)\,|\,f_0(x).$$

If $h_{k-1}(x)$ has positive degree, then the argument leading to (3) can be applied with $h_{k-1}(x)$ in place of $f_m(x)$. This yields in analogy with (3):

$$h_{k-1}(x)\,|\,f_i(x) \text{ for } 0 \leq i \leq k - 2,\ h_{k-1}(x)\,|\,h_i(x) \text{ for } 1 \leq i \leq k - 2.$$

Combining this with (3) and observing (2) and the relative primality of $f_{k-1}(x)$ and $h_{k-1}(x)$, we see that (5) and (6) hold again in this case.

Combining (2), (4), and (6), we conclude that

https://doi.org/10.4153/CMB-1987-003-3 Published online by Cambridge University Press

$$(7) \qquad f_0(x) = c_1 x^r h_{k-1}(x),\ h_0(x) = c_2 x^s f_{k-1}(x)$$

with $c_1, c_2 \in \bar{F}$ and

$$(8) \qquad r + s = k - 1,\ c_1 c_2 = a^{1-k}.$$

Substituting $x = 0$ in (1), we get

$$a^{k-1} y^{2k-2} = (f_{k-1}(0)\, y^{k-1} + \ldots + f_0(0))\,(h_{k-1}(0)\, y^{k-1} + \ldots + h_0(0)).$$

Unique factorization in $\bar{F}[y]$ implies $f_i(0) = h_i(0) = 0$ for $0 \le i \le k-2$. In particular, we have $r \ge 1$ and $s \ge 1$ in (7). On account of the first identity in (8) this already settles the case (i), so that we can assume $k \ge 3$ from now on. Furthermore, for $1 \le i \le k-2$ each $f_i(x)$ and each $h_i(x)$ is divisible by x, so that together with (5) we see that we can put

$$f_i(x) = \frac{x^k - 1}{x - 1} x F_i(x),\ h_i(x) = \frac{x^k - 1}{x - 1} x H_i(x) \text{ for } 1 \le i \le k - 2.$$

Combining this with (7), we can write (1) in the form

$$(9) \qquad \begin{aligned} f(x, y) = {} & \left(f_{k-1}(x) y^{k-1} + \frac{x^k - 1}{x - 1} x F_{k-2}(x) y^{k-2} + \ldots + \frac{x^k - 1}{x - 1} x F_1(x) y \right. \\ & \left. + c_1 x^r h_{k-1}(x) \right) \\ & \left(h_{k-1}(x) y^{k-1} + \frac{x^k - 1}{x - 1} x H_{k-2}(x) y^{k-2} + \ldots + \frac{x^k - 1}{x - 1} x H_1(x) y + c_2 x^s f_{k-1}(x) \right). \end{aligned}$$

We consider first the case where at least one $F_i(x) \ne 0$ and at least one $H_i(x) \ne 0$. Then

$$\max_{1 \le i \le k-2} \deg(F_i(x)) = t \ge 0, \quad \max_{1 \le i \le k-2} \deg(H_i(x)) = u \ge 0.$$

Let d_i be the coefficient of x^t in $F_i(x)$ and let e_i be the coefficient of x^u in $H_i(x)$. Let c_3 be the coefficient of x^{k+t} in $c_1 x^r h_{k-1}(x)$ and let c_4 be the coefficient of x^{k+u} in $c_2 x^s f_{k-1}(x)$. Put

$$D(y) = d_{k-2}\, y^{k-2} + \ldots + d_1 y + c_3,$$
$$E(y) = e_{k-2} y^{k-2} + \ldots + e_1 y + c_4.$$

Since $D(y)$ and $E(y)$ are nonzero polynomials, there exists $\eta \in \bar{F}$ with $D(\eta) \ne 0$ and $E(\eta) \ne 0$. Substitute $y = \eta$ in (9) and consider the degree in x on both sides. On the left-hand side the degree is $2k - 2$. On the right-hand side the degree is $\ge (k + t) + (k + u) \ge 2k$ since $D(\eta)$ (resp. $E(\eta)$) is the coefficient of x^{k+t} (resp. x^{k+u}) in the first (resp. second) factor, and we obtain a contradiction.

Thus we have shown that either all $F_i(x) = 0$ or all $H_i(x) = 0$. Suppose all $F_i(x) = 0$, but not all $H_i(x) = 0$. We choose the maximal i with $H_i(x) \ne 0$ and compare

https://doi.org/10.4153/CMB-1987-003-3 Published online by Cambridge University Press

the coefficients of y^{k-1+i} on both sides of (9). Depending on whether $k - 1 + i$ is even or odd, we obtain

$$\left.\begin{array}{r} a^{(k-1+i)/2} x^{(k-1-i)/2} \dfrac{x^k - 1}{x - 1} \\ \\ 0 \end{array}\right\} = \frac{x^k - 1}{x - 1} x H_i(x) f_{k-1}(x).$$

The first alternative yields $f_{k-1}(x) | x^{(k-1-i)/2}$, and this is a contradiction to (2) and the fact that $f_{k-1}(x)$ has positive degree. The second alternative contradicts $H_i(x) \neq 0$.

Thus it follows that all $H_i(x) = 0$. If $\deg(h_{k-1}(x)) = 0$, then $\deg(f_{k-1}(x)) = k - 1$ by (2), and a comparison of coefficients of y^{k-1} on both sides of (9) yields (depending on whether $k - 1$ is even or odd)

$$\left.\begin{array}{r} a^{(k-1)/2} x^{(k-1)/2} \dfrac{x^k - 1}{x - 1} + cx^{k-1} \\ \\ cx^{k-1} \end{array}\right\} = c_2 x^s f_{k-1}^2(x) + c_1 x^r h_{k-1}^2(x).$$

This is a contradiction since the degree of the left-hand side is $\leq \frac{3}{2}(k - 1)$, whereas the degree of the right-hand side is $> 2(k - 1)$. Thus we must have $\deg(h_{k-1}(x)) > 0$. In this case, however, the argument in the preceding paragraph can be used to show that all $F_i(x) = 0$.

Therefore we are left with the case where $F_i(x) = H_i(x) = 0$ for $1 \leq i \leq k - 2$ and $\deg(h_{k-1}(x)) > 0$. We recall that $\deg(f_{k-1}(x)) > 0$ is our standing assumption. For $k \geq 4$ we have $2k - 4 > k - 1$, so that a comparison of coefficients of y^{2k-4} on both sides of (9) yields

$$a^{k-2} x \frac{x^k - 1}{x - 1} = 0,$$

an obvious contradiction. Hence the case (iii) is settled.

In the remaining case $k = 3$ we have $r + s = 2$ from (8) and also $r \geq 1$, $s \geq 1$, hence $r = s = 1$. Thus (9) attains the form

$$(10) \qquad (x^2 + axy^2 + a^2y^4)(x^2 + x + 1) + cx^2y^2 = (f_2(x)y^2 + c_1xh_2(x))(h_2(x)y^2 + c_2xf_2(x)).$$

Since $\deg(f_2(x)) > 0$, $\deg(h_2(x)) > 0$, we must have

$$f_2(x) = c_5(x - \zeta),\ h_2(x) = c_6(x - \zeta^2)$$

with $c_5, c_6 \in \bar{F}$ and a primitive third root of unity $\zeta \in \bar{F}$. Comparing the coefficients of y^2 on both sides of (10), we get

$$(11) \qquad a(x^2 + x + 1) + cx = c_2c_5^2(x - \zeta)^2 + c_1c_6^2(x - \zeta^2)^2.$$

https://doi.org/10.4153/CMB-1987-003-3 Published online by Cambridge University Press

Substituting $x = \zeta$ and $x = \zeta^2$ in (11) and using $(\zeta - \zeta^2)^2 = -3$, we obtain

$$c\zeta = -3c_1c_6^2,\ c\zeta^2 = -3c_2c_5^2. \tag{12}$$

Substituting $x = 1$ in (11) and using (12), we get $3a + c = 2c$, hence $c = 3a$, a contradiction to the condition $c \neq 3a$ in case (ii). The proof of Lemma 1 is now complete.

We remark that if $k = 3$, $c = 3a$, and the characteristic of F is $\neq 3$, then $f(x, y)$ has the nontrivial factorization

$$\begin{aligned} f(x, y) &= (x^2 + axy^2 + a^2y^4)(x^2 + x + 1) + 3ax^2y^2 \\ &= (a(x - \zeta)y^2 - \zeta x(x - \zeta^2))(a(x - \zeta^2)y^2 - \zeta^2 x(x - \zeta)) \end{aligned}$$

over $\bar{F}$, where $\zeta \in \bar{F}$ is a primitive third root of unity. We note also that if $k \geq 3$ is a power of the characteristic of F, then

$$f(x, y) = (x - ay^2)^{k-1}(x - 1)^{k-1} + cx^{k-1}y^{k-1}$$

has the nontrivial factor $(x - ay^2)(x - 1) - \alpha xy$, where $\alpha \in \bar{F}$ is a root of the polynomial $x^{k-1} + c$.

3. **Proof of the theorem**

LEMMA 2. *Let $k \geq 2$ be an integer and let $a, c \in F_q$ with $ac \neq 0$. If $g_k(x, a) + cx$ is a permutation polynomial of F_q, then every solution $(x_0, y_0) \in F_q \times F_q$ of the equation*

$$f(x, y) = \frac{x^k - a^k y^{2k}}{x - ay^2} \cdot \frac{x^k - 1}{x - 1} + cx^{k-1}y^{k-1} = 0$$

satisfies either $x_0 = 1$ or $y_0 = 0$ or $x_0 = ay_0^2$.

PROOF. Suppose $g_k(x, a) + cx$ is a permutation polynomial of F_q and that $f(x, y) = 0$ has a solution $(x_0, y_0) \in F_q \times F_q$ with $x_0 \neq 1$, $y_0 \neq 0$, and $x_0 \neq ay_0^2$. Then also $x_0 \neq 0$, for otherwise $0 = f(x_0, y_0) = f(0, y_0) = a^{k-1}y_0^{2k-2}$, a contradiction. Put

$$d_1 = y_0^{-1} + ay_0,\ d_2 = x_0y_0^{-1} + ax_0^{-1}y_0. \tag{13}$$

Then

$$\begin{aligned} g_k(d_1, a) &= g_k(y_0^{-1} + ay_0, a) = y_0^{-k} + a^k y_0^k, \\ g_k(d_2, a) &= g_k(x_0y_0^{-1} + ax_0^{-1}y_0, a) = x_0^k y_0^{-k} + a^k x_0^{-k} y_0^k, \end{aligned}$$

by the functional equation

$$g_k\left(y + \frac{a}{y}, a\right) = y^k + \frac{a^k}{y^k}$$

https://doi.org/10.4153/CMB-1987-003-3 Published online by Cambridge University Press

for Dickson polynomials (see [9, p. 356, Eq. (7.8)]). Thus we get

$$\begin{aligned}
&g_k(d_1, a) + cd_1 - g_k(d_2, a) - cd_2 \\
&\quad = y_0^{-k}(1 - x_0^k) + a^k y_0^k(1 - x_0^{-k}) + cy_0^{-1}(1 - x_0) + acy_0(1 - x_0^{-1}) \\
&\quad = x_0^{-k} y_0^{-k}(1 - x_0) \left[(x_0^k - a^k y_0^{2k}) \frac{x_0^k - 1}{x_0 - 1} + cx_0^{k-1} y_0^{k-1}(x_0 - ay_0^2) \right] \\
&\quad = x_0^{-k} y_0^{-k}(1 - x_0)(x_0 - ay_0^2) f(x_0, y_0),
\end{aligned}$$

and so

$$g_k(d_1, a) + cd_1 = g_k(d_2, a) + cd_2.$$

Since $g_k(x, a) + cx$ is a permutation polynomial of F_q, it follows that $d_1 = d_2$. By (13) this yields

$$y_0^{-1}(1 - x_0) = ax_0^{-1}y_0(1 - x_0),$$

so that either $x_0 = 1$ or $x_0 = ay_0^2$. This contradiction completes the proof of Lemma 2.

To prove the theorem, we note first that we can assume $b = 1$ since the property of being a permutation polynomial of F_q is invariant under multiplication by a nonzero element of F_q. We recall the hypothesis $ac \neq 0$. If now $k = 2$, then $g_2(x, a) + cx = x^2 + cx - 2a$ cannot be a permutation polynomial of F_q by [9, p. 352, Table 7.1]. Therefore we can assume that $k \geq 3$ and that the characteristic of F_q does not divide k. If in particular $k = 3$, then by [9, p. 352, Table 7.1] $g_3(x, a) + cx = x^3 + (c - 3a)x$ can only be a permutation polynomial of F_q if $c = 3a$ and $q \equiv 2 \bmod 3$, which is case (i) of the theorem.

It remains to consider the situation where $k \geq 4$, the characteristic of F_q does not divide k, and $g_k(x, a) + cx$ is a permutation polynomial of F_q for some $a, c \in F_q$ with $ac \neq 0$. By Lemma 2 we can bound the number N of solutions of the equation $f(x, y) = 0$ in $F_q \times F_q$ by considering the cases $x = 1$, $y = 0$, and $x = ay^2$. The equation $f(1, y) = 0$ is a polynomial equation in y of degree $2k - 2$ and thus has at most $2k - 2$ solutions. The equation $f(x, 0) = 0$ has at most k solutions, including $(0, 0)$. The equation $f(ay^2, y) = 0$ has at most $2k - 2$ solutions $\neq (0, 0)$. Therefore

$$N \leq 5k - 4. \tag{14}$$

On the other hand, under the hypotheses above $f(x, y)$ is absolutely irreducible over F_q by Lemma 1, and its total degree is $d = 3k - 3$. By a well-known result of Lang and Weil [7], in the form given by Schmidt [13, p. 210], we have

$$|N - q| \leq (d - 1)(d - 2)q^{1/2} + d^2.$$

In particular,

$$N \geq q - (3k - 4)(3k - 5)q^{1/2} - (3k - 3)^2 = G(q^{1/2}),$$

where $G(t) = t^2 - (3k - 4)(3k - 5)t - (3k - 3)^2$. Now suppose we had $q \geq (9k^2 - 27k + 22)^2$. Since $G(t)$ is increasing for $t > \frac{1}{2}(9k^2 - 27k + 20)$, we would get

$$N \geq G(q^{1/2}) \geq G(9k^2 - 27k + 22) = 9k^2 - 36k + 35 > 5k - 4$$

for $k \geq 4$. This contradiction to (14) completes the proof of the theorem.

ACKNOWLEDGMENT: The authors would like to thank the referee for his comments.

REFERENCES

1. A. O. L. Atkin, L. Hay, and R. G. Larson, *Enumeration and construction of pandiagonal latin squares of prime order*, Computers and Math. with Appl., **9** (1983), 267–292.

2. S. Chowla and H. Zassenhaus, *Some conjectures concerning finite fields*, Norske Vid. Selsk. Forh. (Trondheim), **41** (1968), 34–35.

3. J. Dénes and A. D. Keedwell, *Latin Squares and Their Applications*, Academic Press, New York, 1974.

4. L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Dover, New York, 1958.

5. D. F. Hsu and A. D. Keedwell, *Generalized complete mappings, neofields, sequenceable groups and block designs*. I, Pacific J. Math., **111** (1984), 317–332.

6. A. D. Keedwell, *Sequenceable groups, generalized complete mappings, neofields and block designs*, Combinatorial Mathematics X (Adelaide, 1982), pp. 49–71, Lecture Notes in Math., vol. 1036, Springer-Verlag, Berlin-Heidelberg-New York, 1983.

7. S. Lang and A. Weil, *Number of points of varieties in finite fields*, Amer. J. Math., **76** (1954), 819–827.

8. H. Lausch and W. Nöbauer, *Algebra of Polynomials*, North-Holland, Amsterdam, 1973.

9. R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Math. and Its Appl., vol. 20, Addison-Wesley, Reading, Mass., 1983.

10. H. B. Mann, *The construction of orthogonal latin squares*, Ann. Math. Statist., **13** (1942), 418–423.

11. H. Niederreiter and K. H. Robinson, *Bol loops of order pq*, Math. Proc. Cambridge Philos. Soc., **89** (1981), 241–256.

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

13. W. M. Schmidt, *Equations over Finite Fields*, Lecture Notes in Math., vol. 536, Springer-Verlag, Berlin-Heidelberg-New York, 1976.

14. K. S. Williams, *Note on Dickson's permutation polynomials*, Duke Math. J., **38** (1971), 659–665.

DEPARTMENT OF MATHEMATICS
THE PENNSYLVANIA STATE UNIVERSITY
UNIVERSITY PARK, PA 16802
U.S.A.

MATHEMATICAL INSTITUTE
AUSTRIAN ACADEMY OF SCIENCES
DR. IGNAZ-SEIPEL-PLATZ 2
A-1010 VIENNA
AUSTRIA