Internat. J. Math. & Math. Sci.
Vol. 10, No. 3 (1987) 535-544

ON PERMUTATION POLYNOMIALS OVER FINITE FIELDS

R.A. MOLLIN and C. SMALL

Department of Mathematics and Statistics
University of Calgary
Calgary, Alberta, Canada, T2N 1N4

Department of Mathematics and Statistics
Queen's University
Kingston, Ontario, Canada K7L 3N6

(Received July 31, 1986 and in revised form October 3, 1986)

ABSTRACT. A polynomial f over a finite field F is called a *permutation polynomial* if the mapping $F \longrightarrow F$ defined by f is one-to-one. In this paper we consider the problem of characterizing permutation polynomials; that is, we seek conditions on the coefficients of a polynomial which are necessary and sufficient for it to represent a permutation. We also give some results bearing on a conjecture of Carlitz which says essentially that for any even integer m, the cardinality of finite fields admitting permutation polynomials of degree m is bounded.

KEY WORDS AND PHRASES. *Polynomials, irreducibility, factorization, distribution of values.*
1980 Mathematics Subject Classification. 11T06.

1. INTRODUCTION.

A polynomial $f(x) \in GF(q)[x]$, where GF(q) is a finite field with q elements, is called a *permutation polynomial* if the mapping defined by f is one-to-one; i.e. the f(a) where $a \in GF(q)$ are a permutation of the a's. It is well known (eg. see [1]) that any mapping $GF(q) \longrightarrow GF(q)$ is given by a unique polynomial of degree less than q. A natural question to ask (albeit difficult to answer) is: given a polynomial $f(x) = \sum_{i=0}^{d} a_i x^i$, what are necessary and sufficient conditions on the coefficients $a_0, a_1, \ldots, a_d$ for f to be a permutation? (We may assume $d < q$ since f has a unique such representation). Despite an extensive literature on permutation polynomials (e.g. see [1] for an extensive list of references), there is surprisingly little which deals with the classification problem as posed above. However some very special cases are known. For example the cases $d \leq 2$ are trivial since polynomials of degree 0 (respectively 1) are never (respectively always) permutation polynomials; whereas in the quadratic case $f(x) = ax^2 + bx + c$ $(a \neq 0)$, f is a permutation polynomial on GF(q) if and only if $b = 0$ and char GF(q) = 2. The latter is a trivial consequence of one of the

results in this paper (see Corollary 2.3 below).

There has also been such a characterization of the so-called Dickson polynomials; i.e., those polynomials of the form $g_k(x,a) = \sum_{j=0}^{\lfloor k/2 \rfloor} (k/(k-j))\binom{k-j}{j}(-a)^j x^{k-2j}$ where $0 \neq a \in GF(q)$ and $k \in N$, the natural numbers. For such a description the reader is referred to [1, pp. 355-357], where it is proved that $g_k(x,a)$ is a permutation of $GF(q)$ if and only if g.c.d. $(k, q^2 - 1) = 1$.

Some other specialized results toward our characterization problem have also been established. For example S.R. Cavior [2] investigated octics of the form $f(x) = x^8 + ax^t$ with $1 \leq t \leq 7$ and t odd. Carlitz [3], in an attempt to generalize Dickson's result [4] that the quartic $f(x) = x^4 + 3x$ is a permutation polynomial for $GF(7)$ but not $GF(7^n)$ for $n > 1$, shows that if $q = 2m + 1$ and $a \in GF(q)$ is suitably chosen then $f(x) = x^{m+1} + ax$ is a permutation polynomial on $GF(q)$ but not on $GF(q^r)$ with $r > 1$. As a final example, S. Chowla [5] considered polynomials of the form $g(x) = x^5 + ax^3 + bx^2 + cx$, and proved that $g(x)$ is a permutation of $GF(p)$, where p is a sufficiently large prime with $p \equiv \pm 2 \pmod 5$, if and only if $b \equiv 0$ and $5c \equiv a^2 \pmod p$.

In this paper we completely settle the characterization problem for at least one class of polynomials; viz., cyclotomic polynomials $\phi_m(x)$. We prove that $\phi_m(x)$ is a permutation polynomial on $GF(q)$ if and only if either $m = 2$, or both q and m are powers of 2.

Dickson (e.g. see [6] or [7]) classified all permutation polynomials of degree less than 6 over $GF[q]$. In fact, Dickson (eg. see [1] p. 349] where it is called Hermite's condition since Dickson [6], [7] attributed the prime field case to Hermite) gave necessary and sufficient conditions for a polynomial to be a permutation polynomial. However the characterization is not explicit in the sense outlined above, and Dickson's theorem is not easy to use in the sense that is extremely difficult to extract results from the theorem which give concrete criteria in terms of the polynomial's coefficients. One of the major tasks of this paper is to provide necessary and sufficient conditions, in terms of the coefficients, for certain polynomials to be permutations. For example we are able to determine at a glance precisely when $f(x) = ax^i + bx^j + c \in GF(q)$ is a permutation polynomial in terms of a, b and c.

There is a relative scarcity of permutation polynomials as may be seen by the fact that they are necessarily polynomials with *exactly one* root. However this obvious necessary condition is far from sufficient as the example $\phi_3(x) = x^2 + x + 1$ over $GF(3)$ illustrates. Another reason for the scarcity of permutation polynomials may be seen by the fact that, of the q^q mappings $GF(q) \longrightarrow GF(q)$, only q! of them are permutations. The fact that $\lim_{q\to\infty} q!/q^q = 0$ means therefore that permutations get increasingly scarce in large fields, and this points to the difficulty in our characterization problem.

A second major goal of this paper (the first being progress in the characterization problem) is to make advances in establishing Carlitz's conjecture,

namely that for a given even integer m, q may be chosen sufficiently large such that there are no permutation polynomials of degree m on GF(q). Hayes [8] established the conjecture when the characteristic of the field does not divide m. However he used the deep Lang-Weil Theorem [9] which is closely connected to the *Riemann hypothesis* for curves over finite fields (eg. see [1, p. 331] for an explanation of the connection). Our techniques and method of proof in this paper are less complicated. We establish that, subject to the absolute irreducibility over GF(q) of a certain polynomial, no permutation polynomials of any given even degree exist on GF(q) for sufficiently large q. Of course there are infinitely many permutation polynomials of a given odd degree on infinitely many GF(q) as will be seen by our characterization of such polynomials as $f(x) = ax^i + bx^j + c$ in terms of a, b and c (see §2). The latter generalizes the work of Niederreiter and Robinson [10].

We note that Carlitz's conjecture follows from one of our main results *provided* that any one of several conditions (which we will outline) can be shown to hold.

It should be noted that in both Dickson's 1896 thesis [4] and his 1901 monograph [6], the motivation for studying permutation polynomials is their connection with finite simple groups. The linear groups over finite fields F (that is, the subgroups of the full linear group of all invertible linear transformations over F) were already well known (at least in the prime-field case) as a rich source of simple groups. Indeed, while this may have delayed the liberation of groups from their representations as groups of substitutions and matrix groups, it was doubtless the route by which, primarily thanks to Dickson, finite fields entered mathematics in a serious way, except of course for the prime fields, which had arrived on the scene centuries earlier via number theory. Dickson wanted to know which polynomials represented permutations because he wanted to study linear groups (which are after all groups of permutations) by computations with generators for them. The context, in both [4] and [6], is always the applications to the linear groups, and his methods did lead him to previously unknown classes of simple groups (see [4], part II, §17, as well as part II of [6]).

Finally, the reader is referred to the well-written compendium by Lidl and Niederreiter [1, Chapter 7] for an outline of basic results on permutation polynomials, and to Schmidt [11] for some results on equations over finite fields which we will need in §3.

2. THE CHARACTERIZATION PROBLEM.

We begin by observing that the composition of two polynomials is a permutation polynomial if and only if each constituent is one. This leads to the following useful fact.

LEMMA 2.1. Let $f(x) = \sum_{i=1}^{n} c_i x^{m_i} \in GF(q)$ where $m_n > m_{n-1} > \ldots > m_1 \geq 1$ and $\prod_{i=1}^{n} c_i \neq 0$. Suppose $e = \text{g.c.d.}\ \{m_i\}_{1 \leq i \leq n}$. Then $f(x)$ is a permutation polynomial on GF(q) if and only if g.c.d. $(e, q-1) = 1$ and $\sum_{i=1}^{n} c_i x^{m_i/e}$ is a permutation

polynomial.

This observation generalizes [10, Lemma 5, p. 210]. The proof is immediate from the fact that the monomial x^e is a permutation polynomial of GF(q) if and only if g.c.d. (e,q - 1) = 1, (see [1, Theorem 7.8 (ii), p. 351]).

The following result characterizes a certain class of polynomials as permutation polynomials in terms of their coefficients.

THEOREM 2.2. Suppose that k and j are positive integers such that $q > k > j \geq 1$ and g.c.d. (k - j,q - 1) = 1. Then $ax^k + bx^j + c$ with $a \neq 0$ is a permutation of GF(q) if and only if g.c.d. (k,q - 1) = 1 and b = 0.

PROOF. $ax^k + bx^j + c$ is a permutation polynomial if and only if $x^k + a^{-1}bx^j$ is a permutation polynomial. Let $\alpha = -a^{-1}b$. If $\alpha = 0$ then x^k is a permutation polynomial if and only if g.c.d. (k,q - 1) = 1. Assume that $\alpha \neq 0$ and $f(x) = x^k - \alpha x^j$ is a permutation polynomial on GF(q). Since g.c.d. (k - j,q - 1) = 1 then $\alpha \in GF(q)^{k-j}$, say $\alpha = y^{k-j}$ with $y \neq 0$. Therefore $f(x) = x^j(x^{k-j} - \alpha) = x^j(x^{k-j} - y^{k-j})$, so $f(y) = 0 = f(0)$, a contradiction. Q.E.D.

COROLLARY 2.3. $ax^2 + bx + c$ $(a \neq 0)$ is a permutation polynomial on GF(q) if and only if b = 0 and the characteristic of GF(q) is 2.

The following advances Cavior [2].

COROLLARY 2.4. Suppose q - 1 is not divisible by 3, 5 or 7. Then $x^8 + ax^t$, for t odd and $t < 8$, is a permutation polynomial on GF(q) if and only if a = 0 and GF(q) has characteristic 2.

PROOF. g.c.d. (8 - t,q - 1) = 1 by hypothesis. Therefore Theorem 2.2 applies and forces a = 0 and g.c.d. (8,q - 1) = 1; i.e., q must be even.

Q.E.D.

Note that the restriction $q \not\equiv 1$ modulo 3, 5, or 7 is necessary for Corollary 2.4 to hold since it is known for example that $x^8 + 4x$ permutes GF(29), and $x^8 + ax^3$ permutes GF(11). Moreover it is open as to whether $x^8 + ax^5$ permutes $GF(13^n)$ or $GF(7^n)$ for odd n. For details see Cavior [2].

In the next section we will make headway on the question left at the end of Cavior's paper, and conjectured to be true by Carlitz, namely that for a given k there exists a bound N_k such that if $q > N_k$ there is no permutation polynomial of degree 2k on GF(q), in particular for k = 4 as above.

We note furthermore that if we remove the condition g.c.d. (k - j,q - 1) = 1 from the hypothesis of Theorem 2.2 then, as noted above, we must search for new criteria for f(x) to be a permutation of GF(q). One simple observation is that $f(x) = x^k - \alpha x^j$, $\alpha \neq 0$, cannot be a permutation polynomial unless α *fails* to be a $(k - j)^{th}$ power in GF(q): for if $\alpha = \beta^{k-j}$ for some $\beta \in GF(q)$ then $f(0) = f(\beta) = 0$. However this is not a sufficient condition: 3 is not a cube in GF(13), yet $f(x) = x^4 - 3x$ is not a permutation of GF(13) since f(5) = f(-3) = 1.

Furthermore, Dickson [4, p. 77] (see also [1]), proved that a polynomial of degree m over GF(q) cannot permute GF(q) if $q \equiv 1 \pmod{m}$. Therefore one immediately gets from this discussion:

THEOREM 2.5. Let $f(x) = ax^k + bx^j + c$ be a polynomial over GF(q) with $a \neq 0$ and $-ba^{-1}$ is a $(k - j)^{th}$ power in GF(q). Then f permutes GF(q) if and only if $b = 0$ in GF(q) and g.c.d. $(k, q - 1) = 1$.

The clear necessity for $-ba^{-1}$ to fail to be a $(k - j)^{th}$ power is further demonstrated by the following example: $x^4 + 3x$ permutes GF(7) although $3 \neq 0$ in GF(7) and g.c.d. $(4,6) = 2 > 1$.

An immediate corollary of Theorem 2.5 is:

COROLLARY 2.6. If f is as in Theorem 2.5 and $-ba^{-1}$ is a d^{th} power in GF(q) where d = g.c.d. $(q - 1, k - j)$ then f permutes GF(q) if and only if $b = 0$ and g.c.d. $(k, q - 1) = 1$.

Theorem 2.2 is somewhat unsatisfying in that the condition g.c.d. $(k - j, q - 1) = 1$ does not allow us to touch the case where q is odd and $k - j$ is even. The following result relaxes the g.c.d. condition (replacing it with other conditions) thereby allowing us to make headway in such cases where j divides k.

THEOREM 2.7. Let $f(x) = ax^k + bx^j + c$ where j divides k; a, b, $c \in GF(q)$ with $a \neq 0$; g.c.d. $((k/j) - 1, q - 1) = d$, and g.c.d. $(j, q - 1) = 1$. Suppose $-ba^{-1}\beta^{-1}$ is a d^{th} power in GF(q), where $\beta = z^{(k/j)-1} + z^{(k/j)-2} + \ldots + 1$ for some $z \in GF(q)$, $z \neq 1$. Then f permutes GF(q) if and only if $b = 0$ and g.c.d. $(k, q - 1) = 1$.

PROOF. f(x) permutes GF(q) if and only if $x^k - \alpha x^j$ permutes GF(q) where $\alpha = -ba^{-1}$. If $b = 0$ then f permutes GF(q) if and only if g.c.d. $(k, q - 1) = 1$. If $b \neq 0$ (equivalently $\alpha \neq 0$) then by Lemma 2.1 we have that $x^k - \alpha x^j$ permutes GF(q) if and only if $x^{k/j} - \alpha x$ permutes GF(q). Let $k' = k/j$. Since $\alpha\beta^{-1}$ is a d^{th} power in GF(q) we have $\alpha\beta^{-1} = y^{k'-1}$ for some $y \in GF(q)$. Thus $\alpha = y^{k'-1}\beta$. Now let $x = yz$ where $x \neq y$ since $z \neq 1$. Then $x^{k'-1} + x^{k'-2}y + \ldots + y^{k'-1} = y^{k'-1}(z^{k'-1} + z^{k'-2} + \ldots + z + 1) = y^{k'-1}\beta = \alpha$. Thus $x^{k'} - y^{k'} = \alpha(x - y)$ and so $y^{k'} - \alpha y = x^{k'} - \alpha x$ with $x \neq y$, a contradiction. Q.E.D.

We note that as a straightforward application the reader may use Theorem 2.7 to characterize polynomials of degree 3. This requires reducing $f(x) = ax^3 + bx^2 + cx + d$ to the form $x^3 - \alpha x$. If α is a square there is no problem. When α is not a square one shows it can be written as $\alpha = x^2 + xy + y^2$ with $x \neq y$ by finding an element $z \neq 1$ for which $z^2 + z + 1$ is a non-square. The result is Corollary 2.9 below.

However Theorem 2.7 may be difficult to apply in general since a rather technical condition must be satisfied. However when $j = k - 2$ we have a simpler result.

THEOREM 2.8. If $f(x) = ax^k + bx^{k-2} + c$ (where $a \neq 0$ and $k \geq 2$) permutes GF(q) then either $q \not\equiv \pm 1 \pmod{k}$ or $b = 0$.

PROOF. As before, f permutes GF(q) if and only if $x^k - \alpha x^{k-2}$ does, where $\alpha = -ba^{-1}$. We assume the conclusion is false and reach a contradiction. Thus we assume f is a permutation, $q \equiv \pm 1 \pmod{k}$ and $\alpha \neq 0$. Let $n = (q \pm 1)/k$. It is clear that $n \neq q - 1$. Hence, using [1, Lemma 7.3, p. 349] and the fact that f is a permutation we have: $\sum_{x \in GF(q)} (x^k - \alpha x^{k-2})^n = 0$, and

therefore: $0 = \sum_{x\in GF(q)} \sum_{i=0}^{n} \binom{n}{i}(-\alpha)^i x^{kn-ki+i(k-2)} = \sum_{i=0}^{n} \binom{n}{i}(-\alpha)^i \sum_{x\in GF(q)} x^{kn-2i}$. Now by the same lemma from [1] we have $\sum_{x\in GF(q)} x^{kn-2i} = 0$ unless $kn - 2i = q - 1$. But this can occur only for $i = 0$ (when $nk = q - 1$) or $i = 1$ (when $nk = q + 1$). In the former case we get $\sum_{i=0}^{n} \binom{n}{i}(-\alpha)^i \sum_{x\in GF(q)} x^{kn-2i} = \sum_{x\in GF(q)} x^{q-1}$, contradicting [1, ibid], and similarly in the remaining case. This completes the proof. Q.E.D.

COROLLARY 2.9. Let $GF(q)$ have characteristic different from 3. Then $f(x) = ax^3 + bx^2 + cx + d$ $(a \neq 0)$ permutes $GF(q)$ if and only if $b^2 = 3ac$ and $q \equiv 2 \pmod 3$.

PROOF. f permutes $GF(q)$ if and only if $x(x^2 + ba^{-1}x + ca^{-1})$ does. Put $y = x + b(3a)^{-1}$, then $x(x^2 + ba^{-1}x + ca^{-1}) = y^3 + c'y + d'$ with $c' = (3ac - b^2)(3a^2)^{-1}$. Thus f permutes $GF(q)$ if and only if $x^3 - \alpha x$ does where $\alpha = (b^2 - 3ac)(3a^2)^{-1}$. Observe that $\alpha = 0$ means $b^2 = 3ac$. By Theorem 2.8, if $\alpha \neq 0$ then f is not a permutation polynomial. If $\alpha = 0$ then f is a permutation polynomial if and only if g.c.d. $(q - 1,3) = 1$, i.e., $q \equiv 2 \pmod 3$. Q.E.D.

Now we consider the case where the degree of the polynomial is a power of the characteristic.

PROPOSITION 2.10. Let $GF(q)$ have characteristic p, and let $f(x) = x^{p^s} - \alpha x$ with $0 \neq \alpha \in GF(q)$ and $s > 0$. Then:

(1) f permutes $GF(q)$ if and only if α is not a $(p^s - 1)^{th}$ power in $GF(q)$.

(2) If f permutes $GF(q)$ then g.c.d. $(q - 1,p^s - 1) > 1$, and

(3) If α is a primitive root in $GF(q)$ then g.c.d. $(q - 1,p^s - 1) > 1$ if and only if f permutes $GF(q)$.

PROOF. If α is a $(p^s - 1)^{th}$ power in $GF(q)$, say $\alpha = \beta^{p^s-1}$, then f has both 0 and $\beta \neq 0$ as roots, hence is not a permutation. Conversely if $c_1 \neq c_2$ such that $c_1^{p^s} - \alpha c_1 = c_2^{p^s} - \alpha c_2$ then $(c_1 - c_2)^{p^s} = \alpha(c_1 - c_2)$, and $\alpha = (c_1 - c_2)^{p^s-1}$. This proves (1).

If g.c.d. $(q - 1,p^s - 1) = 1$ then α is a $(p^s - 1)^{th}$ power in $GF(q)$ since $\alpha^{q-1} = 1$. This secures (2).

If g.c.d. $(q - 1,p^s - 1) = g > 1$ then α is a $(p^s - 1)^{th}$ power if and only if $\alpha^{(q-1)/g} = 1$. However α is primitive. Thus, α is not a $(p^s - 1)^{th}$ power. Q.E.D.

We note that an immediate consequence of Proposition 2.10 is [10, Theorem 10, p. 209].

Finally we close this section with a characterization of cyclotomic polynomials $\phi_m(x)$ which are permutations.

THEOREM 2.11. The m^{th} cyclotomic polynomial $\phi_m(x)$ is a permutation polynomial on $GF(q)$ if and only if either $m = 2$, or both m and q are powers of 2.

PROOF. If $m = 2^a$ then $\phi_m(x) = x^{2^{a-1}} + 1$ which is a permutation polynomial if and only if $x^{2^{a-1}}$ is one. If $a = 1$ then $x^{2^{a-1}} = x$ is always a permutation polynomial, and for $a > 1$ it is one if and only if g.c.d. $(2, q-1) = 1$; i.e., $p = 2$. Conversely if m is not a power of 2 then:

CASE (i): If $m = 2p^b$, p an odd prime, then $\phi_m(1) = 1 = \phi_m(0)$; and

CASE (ii): If m is not twice the power of an odd prime then $\phi_m(-1) = 1 = \phi_m(0)$. Q.E.D.

3. CARLITZ CONJECTURE AND EVEN DEGREE PERMUTATIONS.

We begin with a characterization of permutatation polynomials in terms of solutions of certain $f(x,y) = 0$.

The equivalence of (1) and (2) in what follows is a natural generalization of [10, Lemma 4, p. 210], whereas the equivalence of (2) and (3) is the central idea of Hayes [8].

We will later use this result to make headway towards the Carlitz conjecture mentioned previously.

THEOREM 3.1. Let $f(x) = \sum_{i=1}^{n} c_i x^i \in GF(q)[x]$ with $c_n \neq 0$. Then the following are equivalent:

(1) $f(x)$ is a permutation polynomial on $GF(q)$;

(2) The equation $\sum_{i=1}^{n} c_n^{-1} c_i y^{n-i}[x^{i-1} + x^{i-2} + \ldots + 1] = 0$, only has solutions $(x_0, y_0) \in GF(q) \times GF(q)$, with either $x_0 = 1$ or $y_0 = 0$;

(3) The equation $(f(x) - f(y))/(x - y) = 0$ has no solutions $(x_0, y_0) \in GF(q) \times GF(q)$ with $x_0 \neq y_0$.

PROOF. First we prove the equivalence of (1) and (2). If $f(x)$ is not a permutation polynomial then $f(a) = f(b)$ with $a \neq b$, and we may assume without loss of generality that $b \neq 0$.

Thus $\sum_{i=1}^{n} c_i b^i[(ab^{-1})^i - 1] = 0$. Now, let $x_0 = ab^{-1} \neq 1$, and $y_0 = b^{-1} \neq 0$. Then $\sum_{i=1}^{n} c_i y_0^{-i}[x_0^i - 1] = 0$, and hence $\sum_{i=1}^{n} c_n^{-1} c_i y_0^{n-i}(x_0^i - 1)/(x_0 - 1) = 0$.

Conversely, suppose that $\sum_{i=1}^{n} c_n^{-1} c_i y_0^{n-i}[x_0^{i-1} + x_0^{i-2} + \ldots + 1] = 0$, for $x_0 \neq 1$ and $y_0 \neq 0$. It follows that $\sum_{i=1}^{n} c_i (x_0 y_0^{-1})^i = \sum_{i=1}^{n} c_i (y_0^{-1})^i$ with $x_0 y_0^{-1} \neq y_0^{-1}$. This establishes the equivalence of (1) and (2), and the equivalence of (2) and (3) is clear. Q.E.D.

THEOREM 3.2. Let $f(x) = \sum_{i=1}^{n} c_i x^{m_i}$ with $0 \neq c_i \in GF(q)$ for $i = 1, \ldots, n$; $0 < m_1 < m_2 < \ldots < m_n$, $n > 1$. Put $\underset{1 \leq i \leq n}{\text{g.c.d.}}\{m_i\} = g$ and assume g.c.d. $(q - 1, g) = 1$. Suppose that

$$f(x,y) = \sum_{i=1}^{n} c_n^{-1} c_i y^{m_n' - m_i'} \left[x^{m_i' - 1} + x^{m_i' - 2} + \ldots + 1 \right]$$

is absolutely irreducible

over GF(q), where $m_i' = m_i/g$. Then, whenever $q > 250(m_n' - 1)^5$, $f(x)$ is not a permutation polynomial over GF(q).

PROOF. By Lemma 2.1, $f(x)$ is a permutation polynomial on GF(q) if and only if $\sum_{i=1}^{n} c_i x^{m_i'}$ is one. Now let N be the number of zeros of $f(x,y)$ in GF(q) × GF(q). By [11, Theorem 1A, p. 92] we have $|N - q| < \sqrt{2}(m_n' - 1)^{5/2} q^{1/2}$. Now let N^* be the number of zeros of $f(x,y)$ with $x_0 = 1$ or $y_0 = 0$. For $x_0 = 1$ we have $\sum_{i=1}^{n} c_n^{-1} c_i y_0^{m_n' - m_i'} m_i' = 0$. Since the m_i' are $\neq 0$ this is a polynomial of degree $\leq m_n' - 1$ and there are at most $m_n' - 1$ values for y_0. If $y_0 = 0$ we have $x_0^{m_n'-1} + x_0^{m_n'-2} + \ldots + 1 = 0$, and again there are at most $m_n' - 1$ values for x_0. In total then we have $N^* \leq 2(m_n' - 1)$. But clearly $N > 2(m_n' - 1)$ since $N > q - \sqrt{2}(m_n' - 1)^{5/2} q^{1/2}$, and by Theorem 3.1 $f(x)$ cannot be a permutation polynomial unless $N = N^*$. Hence $f(x)$ is not a permutation polynomial on GF(q). Q.E.D.

Note that as special cases of Theorem 3.2 we recover Theorem 9, Lemma 7 and Theorem 11 of [10].

Now we state one final result which links the results of §2 and §3.

COROLLARY 3.3. Let $f(x) = ax^k + bx + c$ $(a \neq 0)$ with k not a power of the characteristic of GF(q), and suppose $q > 250\ (k - 1)^5$. Then f permutes GF(q) if and only if $b = 0$ and g.c.d. $(k, q - 1) = 1$.

PROOF. By [10, Lemma 3, p. 208] $f(x,y)$ of Theorem 3.2 is absolutely irreducible in this case. Thus by Theorem 3.2 f is not a permutation polynomial on GF(q) unless $b = 0$. But once we know $b = 0$ then f is a permutation polynomial if and only if g.c.d. $(k, q - 1) = 1$, as before. Q.E.D.

In fact, the hypothesis $q > 250\ (k - 1)^5$ in Corollary 3.3 can be weakened to $q > (k^2 - 4k + 6)^2$; see [10, Theorem 9].

ACKNOWLEDGEMENT. The research for this paper was supported by N.S.E.R.C. Canada.

REFERENCES

1. LIDL, R. and NIEDERREITER, H., Finite Fields, Addison-Wesley, Reading, Mass. (1983).

2. CAVIOR, S., A Note on Octic Permutation Polynomials, Math. Comp., 17 (1963), 450-452.

3. CARLITZ, L., Permutations in Finite Fields, Acta Sci. Math. Szeded, 24 (1963), 196-203.

4. DICKSON, L.E., The Analytic Representation of Substitutions, Ann. of Math., 11 (1896-97), 65-120 and 161-183.

5. CHOWLA, S., On Substitution Polynomials (mod p), Norske Vid. Selsk. Fordh., 41 (1968), 4-6.

6. DICKSON, L.E., Linear Groups with an Exposition of the Galois Field Theory, Teubner (Leipzig), 1901.

7. DICKSON, L.E., Linear Groups, Dover, New York, (1958).

8. HAYES, D.R., A Geometric Approach to Permutation Polynomials over a Finite Field, Duke Math. J., 34 (1967), 293-305.

9. LANG, S. and WEIL, A., Number of Points of Varieties in Finite Fields, Amer. J. Math., 76 (1953), 819-827.

10. NIEDERREITER, H. and ROBINSON, K.H., Complete Mappings of Finite Fields, J. Austral. Math. Soc. (Series A), 33 (1982), 197-212.

11. SCHMIDT, W.M., Equations Over Finite Fields, An Elementary Approach, Springer Lecture Notes, 536 (1976).