J. Austral. Math. Soc. (*Series A*) **43** (1987), 375–384

ON A CONJECTURE OF CARLITZ

WAN DAQING

(Received 29 August 1985)

Communicated by R. Lidl

Abstract

A conjecture of Carlitz on permutation polynomials is as follow: Given an even positive integer n, there is a constant C_n, such that if F_q is a finite field of odd order q with $q > C_n$, then there are no permutation polynomials of degree n over F_q. The conjecture is a well-known problem in this area. It is easily proved if n is a power of 2. The only other cases in which solutions have been published are $n = 6$ (Dickson [5]) and $n = 10$ (Hayes [7]); see Lidl [11], Lausch and Nöbauer [9], and Lidl and Niederreiter [10] for remarks on this problem. In this paper, we prove that the Carlitz conjecture is true if $n = 12$ or $n = 14$, and give an equivalent version of the conjecture in terms of exceptional polynomials.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*): 12 C 05.

1. Introduction

Let F_q denote the finite field with $q = p^m$ elements where p is a prime. A polynomial $f(x)$ in $F_q(x)$ is called a permutation polynomial of F_q if $f(x) = a$ has a solution in F_q for every a in F_q. In 1897, Dickson [5] classified the permutation polynomials of degrees less than 7 over a finite field. His results are quite remarkable in a number of ways. For example, he found that except for a few "accidents" over fields of low order, the permutation polynomials of a given degree fall into a finite number of well-defined categories. Further, his results show that, except for "accidents", there are no permutation polynomials of degree 2, 4, and 6 except when the characteristic of the field is 2. In an address before the

Mathematical Association of America, Professor L. Carlitz suggested that this behaviour is perhaps characteristic: that is, Carlitz suggested the conjecture stated in the abstract.

Dickson's results show that the conjecture is true if $n = 2$, 4, or 6. Hayes [7] introduced some geometric ideas into the study of permutation polynomials. The principal advantage in looking at permutation polynomials from this point of view is that one is able to make use of a powerful theorem of Lang and Weil [8] which estimated the number of rational points on an absolutely irreducible curve defined over a finite field. Then he was able to prove the Carlitz conjecture when n is 8 or 10. In this paper, we go further along these lines.

2. Some connected results

Hayes' ideas could reduce the Carlitz conjecture to the study of exceptional polynomials. In this section, we present some known results on the relation between permutation polynomials and exceptional polynomials, and give an equivalent version of the Carlitz conjecture in terms of generalized exceptional polynomials.

For a field K, a polynomial in $K[x, y]$ of positive degree is called absolutely irreducible if it is irreducible over any algebraic extension of K. A polynomial $f \in F_q(x)$ of degree at least 2 is said to be exceptional over F_q if no irreducible factor of

$$\phi(x, y) = \frac{f(y) - f(x)}{y - x} \tag{1}$$

in $F_q(x, y)$ is absolutely irreducible. MacCluer [12], Williams [15], Gwehenberger [6] and Cohen [2] proved the following theorem.

THEOREM 2.1. *Every exceptional polynomial over F_q is a permutation polynomial of F_q.*

When the converse of the theorem holds is a difficult problem, intimately connected with the Carlitz conjecture. In 1967, Hayes proved the following general theorem.

THEOREM 2.2. *There exists a sequence $c_1, c_2, \ldots$ of integers such that for any finite field F_q of order $q > c_n$ with $(n, q) = 1$, the following holds: if $f \in F_q[x]$ is a permutation polynomial of degree n, then f is exceptional over F_q.*

This theorem was proved for fields F_p, p prime, by Davenport and Lewis [3] and quantitive versions for this case were established by Bombieri and Davenport [1] and Tietäväinen [13].

Using the Lang and Weil theorem [7], it is easily seen that the following theorem is true

THEOREM 2.3. *Let $p(x, y) \in F_q[x, y]$ be an absolutely irreducible polynomial with total degree n, with $p(x, y)$ not of the form $a(y - x)$ for any $a \in F_q$. Then for sufficiently large q relative to n, $p(x, y)$ has a rational point (α, β) over F_q with $\alpha \neq \beta$.*

For any $f(x) \in F_q[x]$, there exists a non-negative integer t such that $f(x) = g(x^{p^t})$ for some $g(x) \in F_q[x]$ but with $f(x) \neq h(x^{p^{t+1}})$ for any $h(x) \in F_q[x]$. We verify directly that

$$\phi(x, y) = \frac{f(y) - f(x)}{y - x} = \frac{g^{p^t}(y) - g^{p^t}(x)}{y - x} = (y - x)^{p^t - 1}\left(\frac{g(y) - g(x)}{y - x}\right)^{p^t}.$$

When $t > 0$ (this happens only in the case $f'(x) = 0$), $\phi(x, y)$ has an absolutely irreducible factor $y - x$, and hence, $f(x)$ is not exceptional over F_q. Even in this case, $f(x)$ may be a permutation polynomial; for example, take $f(x) = x^p$. In order to exclude this case, we introduce the following definition.

DEFINITION. Let $f(x) = g(x^{p^t})$ for some $g(x) \in F_q[x]$, where $g'(x) \neq 0$. We call $f(x)$ a generalized exceptional polynomial over F_q if $g(x)$ is exceptional over F_q or if $\deg(g(x)) = 1$.

From Theorem 2.1, we prove

THEOREM 2.4. *There exists a sequence $c_1, c_2, \ldots$ of positive integers such that for any finite field F_q of order $q > c_n$ the following statement holds: $f(x) \in F_q[x]$ is a permutation polynomial of F_q with degree $(f) \geqslant 2$ if and only if $f(x)$ is a generalized exceptional polynomial over F_q.*

PROOF. Let $f(x) = g(x^{p^t})$, with $g'(x) \neq 0$.

If $f(x)$ is a generalized exceptional polynomial, then $\deg(g(x)) = 1$, or $g(x)$ is exceptional over F_q. By Theorem 2.1, $g(x)$ is a permutation polynomial over F_q, and so is $g(x^{p^t}) = f(x)$.

If $f(x)$ is not a generalized exceptional polynomial, then $g(x)$ is not exceptional. It is easily proved that $y - x \nmid (g(y) - g(x))/(y - x)$ (otherwise $g'(x) = 0$). Therefore, $(g(y) - g(x))/(y - x)$ has an absolutely irreducible factor

$h(x,y) \in F_q(x, y)$ not of the form $a(y - x)$. Theorem 2.3 shows that $g(x)$ is not a permutation polynomial, and hence $f(x)$ is not a permutation polynomial over F_q.

For large q, Theorem 2.4 gives the converse of Theorem 2.1. It can also be used to establish the following equivalent form of the Carlitz conjecture.

Given an even positive integer n, there is a constant C_n such that if F_q is a finite field of odd order q with $q > C_n$, then there are no generalized exceptional polynomials of degree n over F_q.

3. The Carlitz conjecture for $n = 12$ and $n = 14$

In this section, we use some ideas of Hayes to prove the Carlitz conjecture for $n = 12$ and $n = 14$. Without loss of generality, we always suppose $f(x)$ is a polynomial of $F_q[x]$ with leading coefficient 1. Let $q = p^m$, p prime, and let Ω be an algebraic closure of F_q. We use an idea of Hayes to prove

LEMMA 3.1. *Let $f(x)$ be a polynomial of $F_q[x]$ with degree n, and put*

$$\phi(x, y) = \frac{f(y) - f(x)}{y - x}.$$

(i) *If $\phi(x, y)$ has a linear factor of the form $y - x + \alpha$, $\alpha \neq 0$, then*

(2)
$$\phi(x, y) = \left((y - x)^{p-1} + d\right) \cdots$$

and hence $\phi(x, y)$ has at least $p - 1$ linear factors of the form $y - x + \alpha$. Moreover, if $p^2 \nmid n$, then $d \in F_q$.

(ii) *Suppose p is odd and $p^2 \nmid n$. If $\phi(x, y)$ has a linear factor of the form $y + x + \beta$, then $f(x)$ is not a generalized exceptional polynomial over F_q.*

PROOF. The proof is nearly the same as Hayes [7]. We can regard

(3)
$$\varphi(y) = f(y) - f(x)$$

as a polynomial in y over the function field $E = \Omega(f(x))$, which is a subfield of $\Omega(x)$. This polynomial $\varphi(y)$ is irreducible over E as is well known (see van der Waerden [14]) and has the root $y = x$ in $\Omega(x)$. Therefore, $\Omega(x)$ is a simple algebraic extension field of E of degree d, and for any two roots y_1, y_2 of $\varphi(y)$ in $\Omega(x)$, there exists an E-automorphism of $\Omega(x)$ which maps $y_1 \mapsto y_2$, by a fundamental theorem on the extension of isomorphisms.

(i) From the definition of $\varphi(y)$, we have the factorization

(4)
$$\varphi(y) = (y - x)(y - x + \alpha) \cdot \phi_1(x, y).$$

Let σ be an E-automorphism of $\Omega(x)$ which takes the root x of $\varphi(y)$ onto the root $x-\alpha$. Applying this automorphism to the factorization of $\varphi(y)$ we learn that $\varphi(y)$ has the factors $y-x+i\alpha$ $(i=0,1,2,\dots,p-1)$. Therefore $\varphi(y)$ is divisible by

$$\begin{aligned} h(x,y) = \prod_{i=0}^{p-1}(y-x+i\alpha) &= (y-x)^p - \alpha^{p-1}(y-x) \\ &= (y-x)^p + d(y-x). \end{aligned}$$

Now, if $p^2 \nmid n$, then $h(x,y)$ is a product of linear factors with $y-x$ as the homogeneous part of degree 1. Therefore, by unique factorization, any F_q-automorphism of Ω preserves the factor, as such an automorphism preserves $f(y)-f(x)$. It follows that $d=-\alpha^{p-1}$ belongs to F_q.

(ii) We may let $\beta \notin F_q$; then there is an F_q-automorphism σ of Ω such that $\sigma(\beta)=\beta_1$, where $\beta_1 \neq \beta$ is one of the conjugates of β over F_q. Now, $\sigma(\phi(x,y)) = \phi(x,y)$, as σ is an F_q-automorphism. Therefore, by applying σ to the factorization (4), we learn that $y+x+\beta_1$ is also a factor of $\varphi(y)$. Therefore, $\varphi(y)$ has the factorization

$$\varphi(y) = (y-x)(y+x+\beta)(y+x+\beta_1)\cdot\phi_2(x,y). \tag{5}$$

Applying an E-automorphism of $\Omega(x)$, which takes the root x of $\varphi(y)$ onto the root $-x-\beta_1$, to the factorization (5), we obtain

$$\varphi(y) = (y+x+\beta_1)(y-x+\beta-\beta_1)(y-x)\cdot\phi_3(x,y),$$

which shows that $\varphi(y)$ has the factor $y-x+\alpha$, where $\alpha=\beta-\beta_1\neq 0$. By (i), $\varphi(y)$ is divisible by

$$(y-x)^p - \alpha^{p-1}(y-x) = \prod_{i=0}^{p-1}(y-x+i\alpha).$$

Now we apply the E-automorphism of $\Omega(x)$ which maps $x \mapsto -x-\beta$ to this last factor and find that $\varphi(y)$ also has the factor

$$\begin{aligned} &(y+x+\beta)^p - \alpha^{p-1}(y+x+\beta) \\ &\qquad = (y+x)^p - \alpha^{p-1}(y+x) + (\beta^p - \alpha^{p-1}\beta). \end{aligned}$$

Therefore

$$\varphi(y) = (y-x)\big((y-x)^{p-1}+d\big)\big((y+x)^p + d(y+x)+e\big) \tag{6}$$

where $d=-\alpha^{p-1}$, $e=\beta^p-\alpha^{p-1}\beta$.

Since $p^2 \nmid n$, similarly to (i), we have both d and e belong to F_q. Now we consider the polynomials $x^{p-1}+d$ and x^p+dx+e in $F_q[x]$. At least one of the polynomials has a rational root $c \in F_q$: for if $x^{p-1}+d$ has not root in F_q, then the map x^p+dx is an additive homomorphism of F_q into itself with kernel

0 and hence is a permutation of F_q. Thus, there exists an element c of F_q such that $c^p + dc = -e$. Returning to (6), we see that $\varphi(y)$ has a factor of the form $y - x + c$ with $c \neq 0$ or a factor of the form $y + x + c$ in $F_q[x, y]$. That is, $f(x)$ is not a generalized exceptional polynomial.

The following lemma is a version of a theorem of Hayes [7].

LEMMA 3.2. *If $p \nmid n$, and F_q contains an n-th root of unity $\xi \neq 1$ (this is equivalent to $(n, q-1) > 1$), then any polynomial of $F_q[x]$ with degree n is not a generalized exceptional polynomial.*

The lemma shows that the Carlitz conjecture is true if $p \nmid n$. We now consider the case $p \mid n$.

LEMMA 3.3. *Let $p = 3$, and let $f(x)$ be a polynomial of $F_q[x]$ with degree 12. Then $f(x)$ is not a generalized exceptional polynomial over F_q.*

PROOF. Suppose $f(x)$ is a generalized exceptional polynomial; we deduce a contradiction.

Case I: $(y - x) \mid \phi(x, y)$. Put $x = y$. Then $f'(x) = \phi(x, x) = 0$, which implies that $f(x) = g^3(x)$ for some $g(x) \in F_q[x]$ with degree $(g(x)) = 4$. Therefore

$$\phi(x, y) = (y - x)^2 \left(\frac{g(y) - g(x)}{y - x} \right)^3 .$$

Lemma 3.2 shows that $g(x)$ is not a generalized exceptional polynomial, and hence $f(x) = g^3(x)$ is not either. This is a contradiction.

Case II: $(y - x) \nmid \phi(x, y)$. Factor ϕ in $\Omega[x, y]$, obtaining

$$\phi(x, y) = G_1(x, y) \cdot G_2(x, y) \cdots G_r(x, y) \tag{7}$$

where the G_i are absolutely irreducible. Since $f(x)$ is a generalized exceptional polynomial, we have $G_i \notin F_q[x, y]$ for all i.

Let G_{ij} be the homogeneous part whose degree is (degree $(g_i) - j$) in G_i; then

$$G_i = G_{i0} + G_{i1} + G_{i2} + \cdots ,$$

$$\frac{y^{12} - x^{12}}{y - x} = (y - x)^2 \left((y + x)(y^2 + x^2) \right)^3 = G_{10} \cdot G_{20} \cdots G_{r0} .$$

(i) Suppose $(y - x)^2 \mid G_{i0}$ for some i. Then G_i is preserved under any automorphism σ of Ω. Since $(y - x)^2 = \sigma((y - x)^2) \mid \sigma(G_{i0})$ and $(y - x) \nmid G_{j0}$ for $j \neq i$, then $\sigma(G_{i0}) = G_{i0}$, $\sigma(G_{i0}) \neq G_{j0}$. We must have $\sigma(G_i) = G_i$, that is, $G_i \in F_q[x]$. This contradicts $G_i \notin F_q[x]$.

(ii) Suppose $(y-x)^2 \nmid G_{i0}$ for all i. We may suppose $(y-x)\|G_{10}$, and $(y-x)\|G_{20}$. Then G_1 can only be taken to G_1 or G_2 under automorphisms of Ω. According to our hypothesis on $f(x)$, G_1 must be taken to G_2 under some automorphism ρ_1 of Ω.

Now, $(y+x)^3\|G_{10}G_{20}\cdots G_{r0}$. If $(y+x)^h\|G_{10}$, then $(y+x)^h = \rho_1((y+x)^h)\|\rho_1(G_{10}) = G_{20}$, and hence $h=1$ and some G_{i0} $(i \geqslant 3)$ is divisible by $y+x$: G_i is then preserved under any automorphism of Ω. This is a contradiction. Therefore $(y+x)^3\|G_{30}G_{40}\cdots G_{r0}$. Let $(y+x)\,|\,G_{30}$. Then $(y+x)^2 \nmid G_{30}$, for otherwise G_3 is preserved under any automorphism of Ω. Therefore, we may suppose $(y+x)\|G_{30}$, $(y+x)\|G_{40}$, $(y+x)\|G_{50}$ and G_3, G_4, G_5 can be transformed to one another.

By Lemma 3.1, no one of G_3, G_4, G_5 can be a linear factor of the form $y+x+\beta$. Let $\pm\xi$ be the roots of x^2+1 in Ω; then $y+\xi x\,|\,G_{30}$ or $y-\xi x\,|\,G_{30}$. Without loss of generality, we suppose $y-\xi x\,|\,G_{30}$. We now prove that G_1 and G_2 must be linear factors and

$$(y-\xi x)\,|\,G_{30}, \qquad (y-\xi x)\,|\,G_{40}, \qquad (y-\xi x)\,|\,G_{50}.$$

Let τ_2, τ_3 be F_q-automorphisms of Ω such that $\tau_2(G_3) = G_4$, $\tau_3(G_3) = G_5$. If $\xi \in F_q$, then similarly to the proof that $(y+x) \nmid G_{10}$, we have $(y \pm \xi x) \nmid G_{10}$, $(y \pm \xi x) \nmid G_{20}$, and hence both G_1 and G_2 are linear factors. From $(y-\xi x)\,|\,G_{30}$ and $\xi \in F_q$, it is easily seen that applications of τ_2, τ_3 show that $(y-\xi x)\,|\,G_{40}$ and $(y-\xi x)\,|\,G_{50}$.

If $\xi \notin F_q$, we also have $(y-\xi x)\,|\,G_{40}$ and $(y-\xi x)\,|\,G_{50}$, for otherwise, let σ_1 be an F_q-automorphism of Ω such that $\sigma_1(\xi) = -\xi$ (when $(y-\xi x) \nmid G_{40}$, $(y-\xi x) \nmid G_{50}$). Then $(y+\xi x)\,|\,G_{40}$, $(y+\xi x)\,|\,G_{50}$ and $\sigma_1(G_4) = G_3$, $\sigma_1(G_5) = G_3$, which is impossible. If $y-\xi x \nmid G_{40}$ and $y-\xi x\,|\,G_{50}$ then $y+\xi x\,|\,G_{40}$, $y+\xi x \nmid G_{50}$ and $\sigma_1(G_3) = G_4$, $\sigma_1(G_5) = G_4$, which is also impossible. Therefore, $(y-\xi x)\,|\,G_{30}$, $(y-\xi x)\,|\,G_{40}$, $(y-\xi x)\,|\,G_{50}$. If G_1 and G_2 are not linear factors, then $(y+\xi x)\,|\,G_{10}$, $(y+\xi x)\,|\,G_{20}$, and $(y+\xi x)\,|\,G_{i0}$ for some $i \geqslant b$, which leads to $G_i \in F_q[x]$. Thus we must have both G_1 and G_2 are linear factors, and $(y-\xi x)\,|\,G_{30}$, $(y-\xi x)\,|\,G_{40}$, $(y-\xi x)\,|\,G_{50}$. Let $G_1 = y-x+\alpha_1$, $G_2 = y-x+\alpha_2$, $\alpha_1\alpha_2 \neq 0$.

In the factorization (7), put $y = x$; then

$$11a_{11}x^{10} + 10a_{10}x^{f} + \cdots = f'(x) = \alpha_1\alpha_2 \cdot G_3(x,x)\cdots G_r(x,x).$$

The right hand polynomial has degree $11-2=9$, and therefore $a_{11}=0$, and $a_{10} \neq 0$. We put $y = \xi x$; then

$$\sum_{i=1}^{12} a_i x^{i-1}\frac{1-\xi^i}{1-\xi} = a_{10}x^{p}(1-\xi) + a_9x^8 + \cdots = G_1(x,\xi x)\cdots G_r(x,\xi x).$$

The right hand polynomial has degree at most $11 - 3 = 8$, and since $1 + \xi \neq 0$, we deduce that $a_{10} = 0$, which is a contradiction. Lemma 3.3 is proved.

LEMMA 3.4. *Let $p = 7$, and let $f(x)$ be a polynomial of $F_q[x]$ with degree 14. Then $f(x)$ is not a generalized exceptional polynomial over F_q.*

PROOF. Factorise $\phi(x, y)$ in $\Omega[x, y]$, obtaining

$$\phi(x, y) = \frac{f(y) - f(x)}{y - x} = G_1(x, y) G_2(x, y) \cdots G_r(x, y). \tag{8}$$

Suppose $f(x)$ is a generalized exceptional polynomial over F_q. Then all G_i are absolutely irreducible and $G_i \notin F_q[x, y]$.

Let G_{ij} be the homogeneous part of G_i whose degree is $(\deg(G_i) - j)$. Then

$$G_i = G_{i0} + G_{i1} + G_{i2} + \cdots, \quad \frac{y^{14} - x^{14}}{y - x} = (y - x)^6 (y + x)^7 = G_{10} G_{20} \cdots G_{r0}.$$

If no one of G_{i0} is divisible by $(y + x)^2$, then one of them must be a linear factor of the form $y + x$. Lemma 3.1 shows that $f(x)$ is not a generalized exceptional polynomial.

Now, suppose $(y + x)^h \| G_{10}$ $(h \geqslant 2)$. Since $G_1 \notin F_q[x, y]$, G_1 is taken to some G_i under automorphism of Ω; let G_2 be one of the images of G_1 with $G_2 \neq G_1$. Then $(y + x)^h \| G_2$. If G_1 can also be taken to G_3 then $(y + x)^h \| G_3$. Since $(y + x)^7 \| G_{10} G_{20} \cdots G_{r0}$, we have $h = 2$, and $(y + x) \| G_{40} G_{50} \cdots G_{r0}$. Therefore $(y + x) \mid G_{i0}$ for only one i $(i \geqslant 4)$; G_i is then preserved and $G_i \in F_q[x, y]$. This is impossible. Thus G_1 can only be taken to G_2 and $h = 3$ or $h = 2$. If $h = 3$, then $(y + x) \| G_{30} G_{40} \cdots G_{r0}$ shows that $G_i \in F_q[x, y]$ for some i $(i \geqslant 3)$, which is also impossible.

We have proved that $h = 2$ and $(y + x)^3 \| G_{30} G_{40} \cdots G_{r0}$. It is easily seen that we may suppose $y + x \| G_{30}$, $y + x \| G_{40}$, $y + x \| G_{50}$ and G_3, G_4, G_5 can be transformed to one another. Since $\phi(x, y)$ has no factors of the form $y + x + \beta$, then $y - x \mid G_{30}$, $y - x \mid G_{40}$, $y - x \mid G_{50}$, and $G_{60} \cdots G_{r0} \mid (y - x)^3$. If $G_{60} \cdots G_{r0} \neq 1$, then one of G_i $(i \geqslant 6)$ must be a linear factor of the form $y - x + \alpha$ $(\alpha \neq 0)$, and Lemma 3.1 shows that $\phi(x, y)$ would have 6 linear factors of the form $y - x + \alpha$, which is impossible, and hence $G_{60} \cdots G_{r0} = 1$.

Now, $(y - x)^6 \| G_{10} \cdots G_{50}$. Let $(y - x)^{h_i} \| G_i$. Then $h_1 = h_2$, and $h_3 = h_4 = h_5 \geqslant 1$, $2h_1 + 3h_3 = 6$, which leads to $h_1 = 0$, $h_3 = 2$. In the factorization (8), we put $y = x$; then

$$f'(x) = \sum_{i=1}^{14} i a_i x^{i-1} = G_1(x, x) \cdots G_5(x, x).$$

The right hand polynomial has degree at most $13 - 3 = 10$, and hence $a_{13} = a_{12} = 0$. Comparing the homogeneous parts of (8) of degree 11, we have

$$0 = a_{12}\frac{y^{12} - x^{12}}{y - x} = G_{11}G_{21}(G_{30}G_{40}G_{50}) + \sum_i G_{i2}\frac{G_{10}G_{20}\cdots G_{50}}{G_{i0}}$$
$$+ \sum_{(i,j)\neq(1,2)} G_{i1}G_{j1}\frac{G_{10}G_{20}\cdots G_{50}}{G_{i0}G_{j0}}$$
$$\equiv G_{11}G_{21}(G_{30}G_{40}G_{50}) \pmod{(y+x)^4}.$$

Thus $y + x \mid G_{11}G_{21}$. Let $y + x \mid G_{11}$; then $G_1 = (y+x)^2 + \alpha(y+x) + \beta$ for some $\alpha, \beta \in \Omega$, which contradicts that G_1 is absolutely irreducible. Lemma 3.4 is proved.

Collecting Lemmas 3.2, 3.3, 3.4 together, we have

THEOREM 3.5. *Let $n = 12$ or 14. Then the Carlitz conjecture is valid.*

Therefore, up to now the conjecture has been proved for $n \leqslant 16$.

References

1 E. Bombieri and H. Davenport, 'On two problems of Mordell', *Amer. J. Math.* **88** (1966), 61–70.
2. S. D. Cohen, 'The distribution of polynomials over finite fields', *Acta. Arith.* **17** (1970), 255–271.
3. H. Davenport and D. J. Lewis, 'Notes on congruences (II)', *Quart. J. Math.* (2) **14** (1963), 51–60.
4. L. E. Dickson, *Linear groups with an exposition of the Galois field theory* (Dover, New York, 1958).
5. 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. of Math.* **11** (1897), 65–120, 161–183.
6. G. Gwehenberger, *Über die Darstellung von Permutationene durch Polynome und rationale Funktionen* (Diss. TH Wien. 1970).
7. D. R. Hayes, 'A geometric approach to permutation polynomials over a finite field', *Duke Math. J.* **34** (1967), 293–305.
8. S. Lang and A. Weil, 'Number of points of varietes in finite fields', *Amer. J. Math.* **76** (1953), 819–827.
9. H. Lausch and W. Nöbauer, *Algebra of polynomials* (North-Holland, Amsterdam, 1973).
10. R. Lidl and H. Niederreiter, *Finite fields*, (Addison-Wesley, Reading, Massachusetts, 1983).
11. R. Lidl, 'Einige ungelöste Probleme bei endlichen Körpern', *Math. Balkanica* **4** (1974), 409–414.
12. C. R. MacCluer, 'On a conjecture of Davenport and Lewis concerning exceptional polynomials', *Acta. Arith.* **12** (1967), 289–299.

13. A. Tietäväinen, 'On non-residues of polynomial', *Ann. Univ. Turku Ser. AI* **94** (1966), 6 pp.
14. B. L. van der Waerden, *Modern algebra* (Frederick Ungar, New York, 1953).
15. K. S. Williams, 'On exceptional polynomials', *Canad. Math. Bull.* **11** (1968), 179–282.

Department of Mathematics
The University of Washington
Seattle, Washington 98195
U.S.A.