J. Austral. Math. Soc. (*Series A*) **33** (1982), 197–212

COMPLETE MAPPINGS OF FINITE FIELDS

HARALD NIEDERREITER and KARL H. ROBINSON

(Received 3 April 1981; revised 5 October 1981)

Communicated by R. Lidl

Abstract

We discuss complete mapping polynomials of finite fields, which are a special class of permutation polynomials. Complete mapping polynomials of small degree are classified. Results are obtained on a class of complete mapping binomials and on permutation binomials.

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

1. Introduction and general properties

We discuss a special class of mappings of a finite field into itself which arises in connection with combinatorial and algebraic problems. We start with the following general definition.

DEFINITION 1. Let G be a group and $\psi: G \to G$ a bijection of G. Then a bijection $\theta: G \to G$ is called a ψ-complete mapping of G if $\tau: G \to G$ defined by $\tau(g) = \theta(g)\psi(g)$ for $g \in G$ is also a bijection of G. If $\psi = 1_G$, the identity mapping on G, we speak of a complete mapping of G.

Complete mappings were introduced in [8], where they were shown to be pertinent to the problem of constructing orthogonal latin squares. Considerable attention has been given to the question of determining which groups possess complete mappings (see for example [3]), and one result obtained is that every group of odd order possesses at least one complete mapping. From the following result we see that a problem involving ψ-complete mappings can be reduced to a problem involving only complete mappings.

PROPOSITION 1. *Let G be a group and ψ: $G \to G$ a bijection of G. Then a mapping θ: $G \to G$ is a ψ-complete mapping of G if and only if the composition $\theta \circ \psi^{-1}$ is a complete mapping of G.*

PROOF. Let τ: $G \to G$ be defined by $\tau(g) = \theta(g)\psi(g)$. Then θ is a ψ-complete mapping of G if and only if θ and τ are both bijections of G. Now, since ψ is a bijection of G, θ and τ are bijections of G if and only if $\theta \circ \psi^{-1}$ and $\tau \circ \psi^{-1}$ are bijections of G. But $(\tau \circ \psi^{-1})(g) = (\theta \circ \psi^{-1})(g)g$ for all $g \in G$. Hence, θ is a ψ-complete mapping of G if and only if $\theta \circ \psi^{-1}$ is a complete mapping of G.

If F_q is a finite field with q elements, then θ: $F_q \to F_q$ is called a complete mapping of F_q if it is a complete mapping of the additive group of F_q. In [9] it was shown that nonsimple Bol loops of order pr, $p > r$ odd primes, can be characterized by pairs of complete mappings of F_p. This raises the problem of finding interesting classes of complete mappings of finite fields. The present paper addresses itself to this question.

By known interpolation techniques, for example Lagrange's interpolation formula, one shows that any mapping θ of an arbitrary finite field F_q into itself can be represented by a polynomial, in the sense that there exists $f \in F_q[x]$ such that $\theta(c) = f(c)$ for all $c \in F_q$. The polynomial f is unique if we require $\deg(f) < q$. In fact, for $f, h \in F_q[x]$ we have $f(c) = h(c)$ for all $c \in F_q$ if and only if $f(x) \equiv h(x) \bmod (x^q - x)$. The degree of the reduction of f modulo $(x^q - x)$ is called the reduced degree of f. Thus, the reduced degree is always less than q.

A polynomial $f \in F_q[x]$ is called a permutation polynomial of F_q if the induced mapping $c \in F_q \mapsto f(c)$ is a bijection (see [7]). By analogy, we call $f \in F_q[x]$ a complete mapping polynomial of F_q if $c \in F_q \mapsto f(c)$ is a complete mapping of F_q, that is if both $f(x)$ and $f(x) + x$ are permutation polynomials of F_q. Trivial examples of complete mapping polynomials are the linear polynomials $f(x) = ax$ with $a \neq 0, -1$. One of our aims will be to find complete mapping polynomials of reduced degree > 1. The following result, stated and proved in [5], [7], provides a useful criterion for permutation polynomials.

PROPOSITION 2. *A polynomial $f \in F_q[x]$ is a permutation polynomial of F_q if and only if the following two conditions are satisfied*:

(i) *f has a unique root in F_q;*

(ii) *for each integer n with $1 \leqslant n \leqslant q - 2$ and $\gcd(n, q) = 1$, the nth power f^n of f has reduced degree $\leqslant q - 2$.*

A consequence of this result is that if $f \in F_q[x]$ has reduced degree $m > 1$ and m divides $q - 1$, then f is not a permutation polynomial of F_q. We also obtain the following restriction on the reduced degree of a complete mapping polynomial.

THEOREM 1. *For a finite field F_q with odd $q > 3$, any complete mapping polynomial of F_q has reduced degree $\leqslant q - 3$.*

PROOF. By (ii) of Proposition 2, a complete mapping polynomial $f(x)$ of F_q has reduced degree $\leqslant q - 2$. Similarly, $f(x)^2$ and $(f(x) + x)^2$ have reduced degrees $\leqslant q - 2$. But $(f(x) + x)^2 = f(x)^2 + 2xf(x) + x^2$, and since $(f(x) + x)^2$, $f(x)^2$, and x^2 have reduced degrees $\leqslant q - 2$, then $2xf(x)$ has reduced degree $\leqslant q - 2$ and the result follows.

This bound is in a sense best possible since $f(x) = x^4 + 3x$ is a complete mapping polynomial of F_7 of reduced degree 4. It would be of interest to determine whether Theorem 1 holds also for even q. Let F_q^* denote the multiplicative group of nonzero elements of F_q.

THEOREM 2. *If $f(x)$ is a complete mapping polynomial of F_q, then so are the following polynomials*:

(i) *$f(x + a) + b$ for all $a, b \in F_q$;*

(ii) *$af(a^{-1}x)$ for all $a \in F_q^*$;*

(iii) *any polynomial representing the inverse mapping of $c \in F_q \mapsto f(c)$.*

PROOF. (i) is trivial. For (ii) write $f^{(a)}(x) = af(a^{-1}x)$ and $g(x) = f(x) + x$, then $f^{(a)}(x) + x = af(a^{-1}x) + aa^{-1}x = ag(a^{-1}x)$, so that both $f^{(a)}(x)$ and $f^{(a)}(x) + x$ are permutation polynomials being compositions of permutation polynomials. For (iii) let $h \in F_q[x]$ be any polynomial representing the inverse mapping of $c \in F_q \mapsto f(c)$. Then h is a permutation polynomial and $h(c) + c = h(c) + f(h(c)) = g(h(c))$ for all $c \in F_q$, so that $h(x) + x$ is a permutation polynomial.

2. Complete mapping polynomials of small degree

We shall determine all complete mapping polynomials of degree < 6, as well as those of degree 6 for finite fields of order prime to 6. To do this, we make use of the classification given by Dickson [4], [5] of the corresponding set of permutation polynomials.

Let $f \in F_q[x]$ be a polynomial of degree $n \geqslant 1$. If $\gcd(n, q) = 1$, let $f(x) = a_0x^n + na_1x^{n-1} + a_2x^{n-2} + \cdots + a_n$. The normalized polynomial $\tilde{f}$ of f is defined by

$$\tilde{f}(x) = a_0^{-1}\left[f\left(x - a_1a_0^{-1}\right) - f\left(-a_1a_0^{-1}\right)\right].$$

https://doi.org/10.1017/S1446788700018346 Published online by Cambridge University Press

If $\gcd(n, q) > 1$, let $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$. The normalized polynomial $\tilde{f}$ is then defined by

$$\tilde{f}(x) = a_0^{-1}[f(x) - a_n].$$

The normalized polynomial has the property of being monic of degree n and having no constant term. Furthermore, when $\gcd(n, q) = 1$, the coefficient of x^{n-1} in $\tilde{f}(x)$ is zero.

Let $f \in F_q[x]$ have degree $n \geqslant 1$ and leading coefficient a_0, and let $\tilde{f}$ be its normalized polynomial. If $\gcd(n, q) = 1$, then $f(x) = a_0\tilde{f}(x + b) + c$ for some $b, c \in F_q$, and if $\gcd(n, q) > 1$, then $f(x) = a_0\tilde{f}(x) + c$ for some $c \in F_q$. Note that f is a permutation polynomial of F_q if and only if $\tilde{f}$ is one.

We include here Dickson's results in the form of a table listing all normalized permutation polynomials of F_q of degree < 6 and those of degree 6 for finite fields F_q with $\gcd(q, 6) = 1$.

TABLE 1

Normalized Permutation Polynomials	q
x	all q
x^2	$q \equiv 0 \bmod 2$
x^3	$q \not\equiv 1 \bmod 3$
$x^3 - ax$, a not a square in F_q	$q \equiv 0 \bmod 3$
$x^4 \pm 3x$	7
$x^4 + ax^2 + bx$ if $x = 0$ is its only root in F_q	$q \equiv 0 \bmod 2$
x^5	$q \not\equiv 1 \bmod 5$
$x^5 - ax$, a not a fourth power in F_q	$q \equiv 0 \bmod 5$
$x^5 + ax$, $a^2 = 2$	9
$x^5 \pm 2x^2$	7
$x^5 + ax^3 \pm x^2 + 3a^2x$, a not a square in F_q	7
$x^5 + ax^3 + 5^{-1}a^2x$, $a \in F_q$ arbitrary	$q \equiv \pm 2 \bmod 5$
$x^5 + ax^3 + 3a^2x$, a not a square in F_q	13
$x^5 - 2ax^3 + a^2x$, a not a square in F_q	$q \equiv 0 \bmod 5$
$x^6 \pm 2x$	11
$x^6 \pm a^4x^3 + a^2x^2 \pm 5x$, $a \neq 0$	11
$x^6 \pm 4a^2x^3 + ax^2 \pm 4x$, $a = 0$ or a not a square in F_q	11

The following result provides the connection between complete mapping polynomials and normalized permutation polynomials.

https://doi.org/10.1017/S1446788700018346 Published online by Cambridge University Press

THEOREM 3. *Let $f \in F_q[x]$ be of degree n with $n \geqslant 3$ if $\gcd(n, q) = 1$ and $n \geqslant 2$ if $\gcd(n, q) > 1$, and let $\tilde{f}$ be the normalized polynomial of f. Then f is a complete mapping polynomial of F_q if and only if there exists a normalized polynomial $\tilde{g}$ such that:*

(i) *$\tilde{f}$ and $\tilde{g}$ are permutation polynomials of F_q;*

(ii) *$\tilde{g}(x) - \tilde{f}(x) = a_0^{-1}x$, where a_0 is the leading coefficient of f.*

PROOF. If $\gcd(n, q) = 1$, let $f(x) = a_0x^n + na_1x^{n-1} + a_2x^{n-2} + \cdots + a_n$. Then

$$\tilde{f}(x) = a_0^{-1}\left[f\left(x - a_1a_0^{-1}\right) - f\left(-a_1a_0^{-1}\right)\right]$$

and the normalized polynomial $\tilde{g}(x)$ of $f(x) + x$ is given by

$$\begin{aligned}\tilde{g}(x) &= a_0^{-1}\left[f\left(x - a_1a_0^{-1}\right) + \left(x - a_1a_0^{-1}\right) - f\left(-a_1a_0^{-1}\right) + a_1a_0^{-1}\right] \\ &= a_0^{-1}\left[f\left(x - a_1a_0^{-1}\right) + x - f\left(-a_1a_0^{-1}\right)\right].\end{aligned}$$

Hence $\tilde{g}(x) - \tilde{f}(x) = a_0^{-1}x$. If f is a complete mapping polynomial of F_q, then (i) and (ii) follow. Conversely, if (i) and (ii) hold, then $f(x) = a_0\tilde{f}(x + b) + c$ for suitable $b, c \in F_q$, and so $f(x)$ and $a_0\tilde{g}(x + b) + c - b = a_0[\tilde{f}(x + b) + a_0^{-1}x + a_0^{-1}b] + c - b = f(x) + x$ are permutation polynomials of F_q, that is f is a complete mapping polynomial of F_q.

If $\gcd(n, q) > 1$, let $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$, then $\tilde{f}(x) = a_0^{-1}[f(x) - a_n]$ and the normalized polynomial $\tilde{g}(x)$ of $f(x) + x$ is given by $\tilde{g}(x) = a_0^{-1}[f(x) + x - a_n]$. Hence $\tilde{g}(x) - \tilde{f}(x) = a_0^{-1}x$. The proof is completed in the same way as in the case where $\gcd(n, q) = 1$.

Degree $\leqslant 1$. $f(x) = ax + b \in F_q[x]$ is a permutation polynomial of F_q if and only if $a \neq 0$. Thus $f(x)$ is a complete mapping polynomial of F_q if and only if $a \neq 0, -1$.

Degree 2. If $f(x) = ax^2 + bx + c \in F_q[x]$ is a complete mapping polynomial of F_q of degree 2, then by Theorem 3 and Table 1 we have q even and $\tilde{f}(x) = \tilde{g}(x) = x^2$. Thus $a^{-1}x = \tilde{g}(x) - \tilde{f}(x) = 0$, a contradiction. There are thus no complete mapping polynomials of degree 2.

Degree 3. If $f(x) = a_0x^3 + \cdots + a_3 \in F_q[x]$ is a complete mapping polynomial of F_q of degree 3, then by Theorem 3 and Table 1 either $q \equiv 2 \bmod 3$ or $q \equiv 0 \bmod 3$. If $q \equiv 2 \bmod 3$, then $\tilde{f}(x) = \tilde{g}(x) = x^3$, thus $a_0^{-1}x = \tilde{g}(x) - \tilde{f}(x) = 0$, a contradiction. Let $q \equiv 0 \bmod 3$. Then $\tilde{f}(x) \neq \tilde{g}(x)$, otherwise we obtain a contradiction. Thus either (i) $\tilde{g}(x) = x^3 - ax$ and $\tilde{f}(x) = x^3$; (ii) $\tilde{g}(x) = x^3$ and $\tilde{f}(x) = x^3 - ax$; or (iii) $\tilde{g}(x) = x^3 - ax$ and $\tilde{f}(x) = x^3 - bx$, where $a \neq b$ and

both are nonsquares in F_q. If (i) holds, then $a_0^{-1}x = \tilde{g}(x) - \tilde{f}(x) = -ax$, therefore $a_0 = -a^{-1}$. If (ii) holds, then $a_0^{-1}x = \tilde{g}(x) - \tilde{f}(x) = ax$, thus $a_0 = a^{-1}$. If (iii) holds, then $a_0^{-1}x = \tilde{g}(x) - \tilde{f}(x) = (b-a)x$, thus $a_0 = (b-a)^{-1}$. Thus $f(x) \in F_q[x]$ is a complete mapping polynomial of F_q of degree 3 if and only if $q \equiv 0 \bmod 3$ and either $f(x) = -ax^3 + c$, $f(x) = ax^3 - x + c$, or $f(x) = (b-a)^{-1}x^3 - b(b-a)^{-1}x + c$, where $a \neq b$ are nonsquares in F_q and $c \in F_q$ is arbitrary.

In like manner, the complete mapping polynomials of degree 4 and 5 can be determined, as can be those of degree 6 for fields of order relatively prime to 6. These results are summarized in the following table.

TABLE 2

Complete Mapping Polynomials	q
$ax + b$, $a, b \in F_q$, $a \neq 0, -1$	all q
$-ax^3 + c$, $ax^3 - x + c$, $(b-a)^{-1}x^3 - b(b-a)^{-1}x + c$, $a, b, c \in F_q$, $a \neq b$ nonsquares in F_q	$q \equiv 0 \bmod 3$
$-(x+a)^4 + 3x + b$, $(x+a)^4 + 3x + b$, $a, b \in F_7$ arbitrary	7
$a^{-1}(x^4 + bx^2 + cx) + d$, $a, b, c, d \in F_q$, $a \neq 0$, such that $x^4 + bx^2 + cx$ and $x^4 + bx^2 + (a+c)x$ each have $x = 0$ as the unique root in F_q	$q \equiv 0 \bmod 2$
$5a^{-2}[(x+b)^5 + a(x+b)^3 + 8a^2x] + c$, $8a^{-2}[(x+b)^5 + a(x+b)^3 + 3a^2x] + c$, $a, b, c \in F_{13}$, a not a square in F_{13}	13
$a(x+b)^5 + c$, $a(x+b)^5 \pm x + c$, $b, c \in F_9$ arbitrary, $a^2 = 2$	9
$-ax^5 + c$, $ax^5 - x + c$, $(a-b)^{-1}x^5 - a(a-b)^{-1}x + c$, $a, b, c \in F_q$, $a \neq b$ not fourth powers in F_q	$q \equiv 0 \bmod 5$
$-5(x+b)^6 + x + c$, $-2(x+b)^6 - 4x + c$, $2(x+b)^6 - 4x + c$, $5(x+b)^6 + x + c$, $-3(x+b)^6 + 5x + c$, $3(x+b)^6 + 5x + c$, $5(x+b)^6 - 2x + c$, $-2(x+b)^6 + 3x + c$, $2(x+b)^6 + 3x + c$, $-5(x+b)^6 - 2x + c$, $4(x+b)^6 + 5x + c$, $-4(x+b)^6 + 5x + c$, $b, c \in F_{11}$ arbitrary	11

https://doi.org/10.1017/S1446788700018346 Published online by Cambridge University Press

3. A special class of complete mapping binomials

In this section we obtain a necessary and sufficient condition for a binomial in $F_q[x]$ of the form $ax^{(q+n-1)/n} + bx$, $q \equiv 1 \bmod n$, $n \geqslant 2$, to be a complete mapping polynomial of F_q, and the case $n = 2$ is examined more closely. In this way we will establish the existence of complete mapping polynomials of reduced degree > 1 for all F_q with $q > 5$.

From Theorem 8.92 of [7] it follows that, for q sufficiently large, permutation polynomials of F_q of the form $x^{(q+n-1)/n} + bx$, $q \equiv 1 \bmod n$, $n \geqslant 2$, exist. Polynomials of the form $x^{(q+1)/2} + bx$, q odd, have been studied in [1], [2], and sufficient conditions were obtained for such binomials to be permutation polynomials of F_q.

If $n \geqslant 2$ is an integer and $q \equiv 1 \bmod n$, let ω be a primitive nth root of unity in F_q. Let $\psi_n: F_q \to F_q$ be the mapping defined by $\psi_n(c) = c^{(q-1)/n}$, $c \in F_q$. Then ψ_n maps F_q^* homomorphically onto the subgroup of F_q^* generated by ω.

LEMMA 1. *If $n \geqslant 2$ is an integer such that $q \equiv 1 \bmod n$, then $x^{(q+n-1)/n} + bx \in F_q[x]$ is a permutation polynomial of F_q if and only if the following conditions hold*:

(i) $(-b)^n \neq 1$;

(ii) $\psi_n((b + \omega^i)(b + \omega^j)^{-1}) \neq \omega^{j-i}$ *for all* $0 \leqslant i < j < n$, *where* ω *is a fixed primitive nth root of unity in* F_q.

PROOF. Put $f(x) = x^{(q+n-1)/n} + bx$. Let b satisfy (i) and (ii) of the lemma. If $f(c) = 0$ for some $c \in F_q^*$, then for some $0 \leqslant i < n$ we have $0 = bc + c^{(q+n-1)/n} = (b + c^{(q-1)/n})c = (b + \omega^i)c$. Now $(-b)^n \neq 1$ implies that $b + \omega^i \neq 0$, hence $c = 0$, a contradiction. If $f(c_1) = f(c_2)$, $c_1, c_2 \in F_q^*$, then $(b + c_1^{(q-1)/n})c_1 = (b + c_2^{(q-1)/n})c_2$, thus for some $0 \leqslant i, j < n$ we have $(b + \omega^i)c_1 = (b + \omega^j)c_2$. Without loss of generality we may assume $i \leqslant j$. Thus $(b + \omega^i)(b + \omega^j)^{-1} = c_2c_1^{-1}$, hence $\psi_n((b + \omega^i)(b + \omega^j)^{-1}) = \psi_n(c_2)\psi_n(c_1^{-1}) = \omega^{j-i}$, which is a contradiction unless $i = j$. In this case $c_2c_1^{-1} = (b + \omega^i)(b + \omega^i)^{-1} = 1$, thus $c_1 = c_2$. Therefore $f(x)$ is a permutation polynomial of F_q.

To prove the necessity, suppose first that $(-b)^n = 1$. Then $b + \omega^i = 0$ for some $0 \leqslant i < n$. Let $c \in F_q$ be such that $\psi_n(c) = \omega^i$. Then $c \neq 0$ and $f(c) = 0 = f(0)$, so that $f(x)$ fails to be a permutation polynomial of F_q.

Suppose $\psi_n((b + \omega^i)(b + \omega^j)^{-1}) = \omega^{j-i}$ for some $0 \leqslant i < j < n$. Let $a = (b + \omega^i)(b + \omega^j)^{-1}$ and let $d \in F_q^*$ be such that $\psi_n(d) = \omega^j$. Then $(b + \omega^i)(b + \omega^j)^{-1} = a = dd^{-1}a$ and $\psi_n(da^{-1}) = \omega^i$. Therefore $(b + \omega^i)da^{-1} = (b + \omega^j)d$ and $f(da^{-1}) = f(d)$, so that $f(x)$ fails to be a permutation polynomial of F_q since $a \neq 1$.

https://doi.org/10.1017/S1446788700018346 Published online by Cambridge University Press

THEOREM 4. *If $n \geqslant 2$ is an integer such that $q \equiv 1 \bmod n$, then $ax^{(q+n-1)/n} + bx \in F_q[x]$, $a \neq 0$, is a complete mapping polynomial of F_q if and only if the following conditions hold*:

(i) $b^n \neq (-a)^n$, $(b+1)^n \neq (-a)^n$;

(ii) $\psi_n((b + a\omega^i)(b + a\omega^j)^{-1}) \neq \omega^{j-i}$ *and* $\psi_n((b + 1 + a\omega^i)(b + 1 + a\omega^j)^{-1}) \neq \omega^{j-i}$ *for all* $0 \leqslant i < j < n$, *where ω is a fixed primitive nth root of unity in F_q.*

PROOF. $f(x) = ax^{(q+n-1)/n} + bx$ is a complete mapping polynomial of F_q if and only if $a^{-1}f(x)$ and $a^{-1}(f(x) + x)$ are permutation polynomials of F_q. But by Lemma 1, $a^{-1}f(x)$ and $a^{-1}(f(x) + x)$ are permutation polynomials of F_q if and only if:

(A) $(-a^{-1}b)^n \neq 1$, $(-a^{-1}(b+1))^n \neq 1$;

(B) $\psi_n((a^{-1}b + \omega^i)(a^{-1}b + \omega^j)^{-1}) \neq \omega^{j-i}$ and $\psi_n[(a^{-1}(b+1) + \omega^i)(a^{-1}(b+1) + \omega^j)^{-1}] \neq \omega^{j-i}$ for all $0 \leqslant i < j < n$.

(i) is equivalent to (A) and (ii) is seen to be equivalent to (B) by noting that $(a^{-1}b + \omega^i)(a^{-1}b + \omega^j)^{-1} = (b + a\omega^i)(b + a\omega^j)^{-1}$ and $(a^{-1}(b+1) + \omega^i)(a^{-1}(b+1) + \omega^j)^{-1} = (b + 1 + a\omega^i)(b + 1 + a\omega^j)^{-1}$.

Let $n = 2$ and q be odd. We shall denote ψ_2 simply by ψ. In this case $\omega = -1$, and $\psi(c) = 1$ if and only if $c \neq 0$ and c is a square in F_q.

THEOREM 5. *Let q be odd and $\tilde{f}(x) = x^{(q+1)/2} + bx \in F_q[x]$. Then $f(x)$ is a permutation polynomial of F_q if and only if $\psi(b^2 - 1) = 1$.*

PROOF. By Lemma 1 with $n = 2$ and $\omega = -1$, $f(x)$ is a permutation polynomial of F_q if and only if $b^2 - 1 \neq 0$ and $\psi[(b+1)(b-1)^{-1}] \neq -1$. But $\psi[(b+1)(b-1)^{-1}] = \psi[(b+1)(b-1)^{-1}]\psi((b-1)^2) = \psi(b^2 - 1)$, and $b^2 - 1 \neq 0$ if and only if $\psi(b^2 - 1) \neq 0$. Thus $f(x)$ is a permutation polynomial of F_q if and only if $\psi(b^2 - 1) \neq 0, -1$. *Since the image of ψ is $\{0, \pm 1\}$, the result follows.*

REMARK 1. It is easily seen that $\psi(b^2 - 1) = 1$ precisely if b is of the form $b = (c^2 + 1)(c^2 - 1)^{-1}$ for some $c \in F_q$ with $c^2 \neq 0, 1$. Carlitz [1] has shown that for elements b of this form, $x^{(q+1)/2} + bx$ is a permutation polynomial of F_q. One arrives at a simpler form for b by noting that $\psi(b^2 - 1) = 1$ if and only if $b = 2^{-1}(c + c^{-1})$ for some $c \in F_q$ with $c^2 \neq 0, 1$.

THEOREM 6. *Let q be odd and $f(x) = ax^{(q+1)/2} + bx \in F_q[x]$, $a \neq 0$. Then $f(x)$ is a complete mapping polynomial of F_q if and only if $\psi(b^2 - a^2) = \psi((b+1)^2 - a^2) = 1$.*

https://doi.org/10.1017/S1446788700018346 Published online by Cambridge University Press

PROOF. Using arguments similar to those in the proof of Theorem 4, this follows from Theorem 5.

REMARK 2. It can be verified that the family of polynomial mappings in $F_q[x]$ of the form $ax^{(q+1)/2} + bx$ is closed under composition. In fact, if $f_1(x) = ax^{(q+1)/2} + bx$ and $f_2(x) = cx^{(q+1)/2} + dx$ are in $F_q[x]$, q odd, then

$$(f_1 \circ f_2)(x) \equiv (ae + bc)x^{(q+1)/2} + (af + bd)x \bmod (x^q - x),$$

where $e + f = (c + d)^{(q+1)/2}$ and $e - f = (d - c)^{(q+1)/2}$.

REMARK 3. Let $q > 3$ be odd and $f(x) = bx^{q-2} + x^{(q-3)/2} \in F_q[x]$. By arguments similar to those in Lemma 1 and Theorem 5 one shows that $f(x)$ is a permutation polynomial of F_q if and only if $\psi(b^2 - 1) = 1$. It should be noted, however, that for $b \neq 0$, $f(x)$ is never a complete mapping polynomial of F_q. This follows from Theorem 1 and the fact that $f(x)$ has reduced degree $q - 2$.

The criterion in Theorem 6 leads to enumerative results which indicate that there are comparatively many complete mapping polynomials of F_q of the form $x^{(q+1)/2} + bx$.

THEOREM 7. *The number N of elements $b \in F_q$ such that $x^{(q+1)/2} + bx$ is a complete mapping polynomial of F_q satisfies*

$$N \geqslant \tfrac{1}{4}q - \tfrac{5}{2} - \tfrac{3}{4}q^{1/2} \tag{1}$$

if F_q is of characteristic > 3. If F_q is of characteristic 3, we have

$$N = \begin{cases} \dfrac{q-9}{4} & \text{if } q \equiv 1 \bmod 4, \\ \dfrac{q-3}{4} & \text{if } q \equiv 3 \bmod 4. \end{cases} \tag{2}$$

PROOF. Let η be the quadratic character of F_q. Then from Theorem 6 and the definition of ψ we get for F_q of characteristic > 3,

$$\begin{aligned} N &= \tfrac{1}{4} \sum_{\substack{b \in F_q \\ b \neq -2,-1,0,1}} \left[1 + \eta(b^2 - 1)\right]\left[1 + \eta\left((b+1)^2 - 1\right)\right] \\ &= \tfrac{1}{4} \sum_{b \in F_q} \left[1 + \eta(b^2 - 1)\right]\left[1 + \eta\left((b+1)^2 - 1\right)\right] - \tfrac{1}{4}(4 + 2\eta(3) + 2\eta(-1)) \\ &= \tfrac{1}{4}q + \tfrac{1}{2} \sum_{b \in F_q} \eta(b^2 - 1) + \tfrac{1}{4} \sum_{b \in F_q} \eta((b-1)b(b+1)(b+2)) \\ &\quad - 1 - \tfrac{1}{2}(\eta(3) + \eta(-1)). \end{aligned}$$

https://doi.org/10.1017/S1446788700018346 Published online by Cambridge University Press

Now

$$\sum_{b\in F_q} \eta((b+c_1)(b+c_2)) = -1 \quad \text{for } c_1, c_2 \in F_q, c_1 \neq c_2, \tag{3}$$

by [6], Lemma 14.1.1, and so

$$N = \tfrac{1}{4}q - \tfrac{3}{2} - \tfrac{1}{2}(\eta(3) + \eta(-1)) + \tfrac{1}{4}\sum_{b\in F_q} \eta((b-1)b(b+1)(b+2)).$$

According to Weil's estimate for character sums (see [11, page 43, Theorem 2C']) we have

$$\left|\sum_{b\in F_q} \eta((b-1)b(b+1)(b+2))\right| \leqslant 3q^{1/2},$$

hence (1) follows. If F_q is of characteristic 3, then

$$\begin{aligned} N &= \tfrac{1}{4}\sum_{\substack{b\in F_q \\ b\neq 0,\pm 1}} \left[1+\eta(b^2-1)\right]\left[1+\eta\left((b+1)^2-1\right)\right] \\ &= \frac{q-3}{4} + \tfrac{1}{2}\sum_{\substack{b\in F_q \\ b\neq 0,\pm 1}} \eta(b^2-1) + \tfrac{1}{4}\sum_{\substack{b\in F_q \\ b\neq 0,\pm 1}} \eta\left(b(b+1)(b-1)^2\right) \\ &= \frac{q-3}{4} + \tfrac{1}{2}\sum_{b\in F_q} \eta(b^2-1) - \tfrac{1}{2}\eta(-1) + \tfrac{1}{4}\sum_{b\in F_q} \eta(b(b+1)) - \tfrac{1}{4}\eta(-1) \\ &= \tfrac{1}{4}(q-6-3\eta(-1)) \end{aligned}$$

by (3). Thus (2) follows since $\eta(-1) = 1$ for $q \equiv 1 \bmod 4$ and $\eta(-1) = -1$ for $q \equiv 3 \bmod 4$.

COROLLARY 1. *Complete mapping polynomials of F_q of the form $x^{(q+1)/2} + bx$ exist exactly for all odd $q \geqslant 13$ and for $q = 7$.*

PROOF. The lower bound in (1) and the expressions in (2) are positive for $q > 25$. Thus it remains to consider the odd prime powers $q \leqslant 25$. We can take $b = 2$ for $q = 23$ and 25, $b = 3$ for $q = 7$ and 17, $b = 5$ for $q = 19$, and $b = 6$ for $q = 13$. The cases $q = 3$ and 9 can be eliminated by (2), and for $q = 5$ and 11 one shows by inspection that there is no complete mapping polynomial of the desired form.

A basic question for the applications (see for example [9]) is that of the existence of complete mapping polynomials of reduced degree > 1, which can now be settled as follows.

https://doi.org/10.1017/S1446788700018346 Published online by Cambridge University Press

THEOREM 8. *For any finite field F_q with $q > 5$ there exist complete mapping polynomials of F_q of reduced degree > 1.*

PROOF. For $q = 7$ and all odd $q \geqslant 13$, this follows from Corollary 1. For $q = 9$ and 11, polynomials of the desired type can be obtained from Table 2. For even $q > 5$, we use the following argument to show that there exist complete mapping polynomials of F_q of degree 4. The number of monic irreducible polynomials over F_q of degree 3 is given by $(q^3 - q)/3$. On the other hand, there are q^2 ordered pairs of elements of F_q. Since $(q^3 - q)/3 > q^2$ for $q > 5$, there exist an ordered pair (a_1, a_2) with $a_1, a_2 \in F_q$ and two distinct elements $d_1, d_2 \in F_q$ such that $x^3 + a_1x^2 + a_2x + d_i$ is irreducible over F_q for $i = 1, 2$. Changing x into $x - a_1$, we get two irreducible polynomials $x^3 + bx + c_i$, $i = 1, 2$, over F_q with $c_1 \neq c_2$. It follows then from Table 2 that $(c_2 - c_1)^{-1}(x^4 + bx^2 + c_1x)$ is a complete mapping polynomial of F_q.

REMARK 4. Theorem 8 is best possible in the sense that for $q \leqslant 5$ every complete mapping polynomial of F_q is of reduced degree 1. This is trivial for $q = 2$. For $q = 3$ it is obvious and for $q = 4, 5$ it follows, respectively, from the remark after Proposition 2 and Theorem 1 that every complete mapping polynomial of F_q has reduced degree $\leqslant 2$. Since there are no quadratic complete mapping polynomials (see Section 2), the claim is established.

REMARK 5. Theorem 8 can also be proved elementarily, that is without using Corollary 1 which depends on Weil's estimate. If F_q is of characteristic > 7, then Theorem 6 shows that $24x^{(q+1)/2} + 25x$ is a complete mapping polynomial of F_q of reduced degree > 1. If F_q is of characteristic 3 or 5, then suitable polynomials can be obtained from Table 2. If F_q is of characteristic 7, then $x^{(q+1)/2} + 3x$ is suitable by Theorem 6. For F_q of characteristic 2 the same argument as in the proof of Theorem 8 is used. We note that "almost universal" complete mapping polynomials obtained from Theorem 6, such as $24x^{(q+1)/2} + 25x$, are obviously connected with Pythagorean triples.

4. Permutation binomials

In the preceding section we considered binomials $ax^k + bx$ with k depending on q, and many complete mapping polynomials were obtained. If k is fixed independently of q, the situation changes. In fact, apart from some obvious exceptions, such a binomial is not even a permutation polynomial of F_q once q is sufficiently large. One such exception is the case $b = 0$, since it is known that ax^k,

$a \in F_q^*$, is a permutation polynomial of F_q if and only if $\gcd(k, q-1) = 1$, and from this it follows easily that for fixed $k \geqslant 1$ there exist infinitely many q such that x^k is a permutation polynomial of F_q. For if k is odd, take the infinitely many primes $q \equiv 2 \bmod k$. If k is even, consider $q = 2^r$ and note that $\gcd(k, 2^r - 1) > 1$ if and only if $2^r \equiv 1 \bmod p_i$ for one of the odd prime divisors p_i of k. But the latter condition is equivalent to $r \equiv 0 \bmod e_i$ for some i, where e_i is the multiplicative order of $2 \bmod p_i$, and there are of course infinitely many r which do not satisfy any of these congruences.

LEMMA 2. *The binomial $ax^k + bx \in F_q[x]$ with $ab \neq 0$ is permutation polynomial of F_q if and only if the equation*

$$y^{k-1} + ab^{-1}\left(x^{k-1} + x^{k-2} + \cdots + x + 1\right) = 0 \tag{4}$$

only has solutions $(x_0, y_0) \in F_q \times F_q$ with either $x_0 = 1$ or $y_0 = 0$.

PROOF. Suppose the condition of the Lemma is satisfied. Now let $ac_1^k + bc_1 = ac_2^k + bc_2$ with $c_1, c_2 \in F_q$, $c_1 \neq c_2$. Without loss of generality, we can assume $c_2 \neq 0$. Then

$$ac_2^k\left[\left(c_1c_2^{-1}\right)^k - 1\right] + bc_2\left(c_1c_2^{-1} - 1\right) = 0.$$

Put $x_0 = c_1c_2^{-1} \neq 1$, $y_0 = c_2^{-1} \neq 0$. Then $ay_0^{-k}(x_0^k - 1) + by_0^{-1}(x_0 - 1) = 0$, hence $y_0^{k-1} + ab^{-1}(x_0^{k-1} + x_0^{k-2} + \cdots + x_0 + 1) = 0$, a contradiction. Thus $ax^k + bx$ is a permutation polynomial of F_q. The converse is shown similarly.

We note that when $k = 2$, we cannot have a permutation polynomial of F_q of the form $ax^2 + bx$, $ab \neq 0$. This follows either from Lemma 2 or directly from the fact that such a binomial has two distinct roots in F_q. Thus we can assume $k > 2$.

Equation (4) is of the form $y^d - f(x) = 0$, which has been studied extensively both by the methods of algebraic geometry and by the well-known elementary methods of Stepanov and Schmidt. When $k > 2$, then for equation (4) we have $d = k - 1$, $m = \deg(f) = k - 1$, thus we have here a case where Stepanov's standard condition $\gcd(m, d) = 1$ is not satisfied. We will therefore use Schmidt's more general results for absolutely irreducible equations (see [10], [11]). By an absolutely irreducible equation we mean an equation $G(x, y) = 0$ with $G(x, y)$ absolutely irreducible over F_q, that is irreducible over the algebraic closure $\bar{F}_q$.

LEMMA 3. *Let $k > 2$. Then $y^{k-1} + c(x^{k-1} + x^{k-2} + \cdots + x + 1)$, $c \in F_q^*$, is absolutely irreducible over F_q if and only if k is not a power of the characteristic of F_q.*

https://doi.org/10.1017/S1446788700018346 Published online by Cambridge University Press

PROOF. We use the fact that $y^d - f(x)$ is absolutely irreducible over F_q if and only if $D = \gcd(d, d_1, \ldots, d_s) = 1$, where $d_1, \ldots, d_s$ are the multiplicities of roots of $f(x)$ (see [11], page 11, Lemma 2C). In our case $f(x) = -c(x^k - 1)/(x - 1)$. Let p be the characteristic of F_q and $k = p^t u$, $\gcd(p, u) = 1$. If $t = 0$, then $f(x)$ has only simple roots, hence $D = 1$. If $t > 0$, $u \geqslant 2$, then $f(x)$ has the root 1 of multiplicity $p^t - 1$ and $u - 1$ roots $\neq 1$ of multiplicity p^t, hence $D = \gcd(k - 1, p^t - 1, p^t, \ldots, p^t) = 1$. If $t > 0$, $u = 1$, then $f(x)$ has the root 1 of multiplicity $p^t - 1 = k - 1$, thus $D = \gcd(k - 1, k - 1) > 1$ since $k > 2$.

THEOREM 9. *Let $k > 2$. Then*: (i) *if k is not a prime power, then for all finite fields F_q with $q \geqslant (k^2 - 4k + 6)^2$ there is no permutation polynomial of F_q of the form $ax^k + bx \in F_q[x]$ with $ab \neq 0$*; (ii) *if k is a power of the prime p, then for all finite fields F_q with $q \geqslant (k^2 - 4k + 6)^2$ and characteristic $\neq p$ there is no permutation polynomial of F_q of the form $ax^k + bx \in F_q[x]$ with $ab \neq 0$.*

PROOF. If the equation (4) is absolutely irreducible, then the number N of solutions $(x_0, y_0) \in F_q \times F_q$ satisfies

$$|N - q| \leqslant (k - 2)^2 q^{1/2} \tag{5}$$

by [11, page 80]. On the other hand, the number N^* of solutions with either $x_0 = 1$ or $y_0 = 0$ satisfies $N^* \leqslant 2(k - 1)$. For $q \geqslant (k^2 - 4k + 6)^2$ we get from (5),

$$\begin{aligned} N &\geqslant q^{1/2}\left[q^{1/2} - (k - 2)^2\right] \geqslant (k^2 - 4k + 6)\left[k^2 - 4k + 6 - (k - 2)^2\right] \\ &= 2(k^2 - 4k + 6) > 2(k - 1) \geqslant N^*. \end{aligned}$$

Thus there exists a solution (x_0, y_0) of (4) with $x_0 \neq 1$ and $y_0 \neq 0$. The result follows now from Lemmas 2 and 3.

COROLLARY 2. *If k and q are as in Theorem 9, then there is no complete mapping polynomial of F_q of the form $ax^k + bx \in F_q[x]$ with $a \neq 0$.*

In the exceptional case of Theorem 9, namely when k is a power of the characteristic of F_q, one can show that the conclusion of Theorem 9 is not valid.

THEOREM 10. *For fixed $k = p^t > 2$, p prime, there are infinitely many finite fields F_q of characteristic p for which there exist complete mapping polynomials of F_q of the form $ax^k \in F_q[x]$. If $p \geqslant 3$, one can find complete mapping polynomials of this form for any F_q of characteristic p.*

https://doi.org/10.1017/S1446788700018346 Published online by Cambridge University Press

PROOF. If F_q is of characteristic p, then ax^k, $a \in F_q^*$, is always a permutation polynomial of F_q. Thus it remains to show that for infinitely many F_q there exist permutation polynomials of F_q of the form $ax^k + x$, $a \in F_q^*$. Since the mapping $c \in F_q \mapsto ac^k + c$ is a linear operator on F_q considered as a vector space over F_p, $ax^k + x$ is a permutation polynomial of F_q if and only if the polynomial only has the root 0 in F_q, or equivalently, if and only if $-a^{-1}$ is not a $(k-1)$st power of an element of F_q^*. Such an element $a \in F_q^*$ can be found precisely if $\gcd(k-1, q-1) > 1$. If $p \geqslant 3$, then $\gcd(k-1, q-1) = \gcd(p^t - 1, q-1) \geqslant p - 1$, so the condition is always satisfied. If $p = 2$, then $k = 2^t$ with $t \geqslant 2$, and one can find infinitely many powers q of 2 with $\gcd(k-1, q-1) > 1$, for example take q to be any power of k.

More generally, one can study the question of finding permutation polynomials of F_q which are binomials

$$ax^k + bx^j \in F_q[x], \qquad ab \neq 0,\ 1 \leqslant j < k. \tag{6}$$

In the same way as Lemma 2, one shows the following criterion.

LEMMA 4. *The binomial* (6) *is a permutation polynomial of F_q if and only if the equation*

$$\begin{aligned} &y^{k-j}\left(x^{j-1} + x^{j-2} + \cdots + x + 1\right) \\ &\quad + ab^{-1}\left(x^{k-1} + x^{k-2} + \cdots + x + 1\right) = 0 \end{aligned} \tag{7}$$

only has solutions $(x_0, y_0) \in F_q \times F_q$ with either $x_0 = 1$ or $y_0 = 0$.

Let $e = \gcd(k, j)$, then we can write $ax^k + bx^j = a(x^e)^{k/e} + b(x^e)^{j/e}$. Since the composition of two polynomials is a permutation polynomial if and only if each constituent is one, we get the following.

LEMMA 5. *The binomial* (6) *is a permutation polynomial of F_q if and only if* $\gcd(e, q-1) = 1$ *and $ax^{k/e} + bx^{j/e}$ is a permutation polynomial of F_q, where* $e = \gcd(k, j)$.

We can thus concentrate on the case where $\gcd(k, j) = 1$. The following auxiliary results are needed.

LEMMA 6. *Let* $\gcd(k, j) = 1$ *and* $k, j > 1$. *Then for* $f(x) = c(x^{k-1} + x^{k-2} + \cdots + x + 1) \in F_q[x]$, $c \neq 0$, *and* $g(x) = x^{j-1} + x^{j-2} + \cdots + x + 1 \in F_q[x]$ *we have*:

(i) *$f(x)$ and $g(x)$ are relatively prime*;

(ii) *if d and h are integers with $0 < h < d$, then $f(x)^h g(x)^{d-h}$ is not a dth power.*

https://doi.org/10.1017/S1446788700018346 Published online by Cambridge University Press

PROOF. Since $\gcd(k, j) = 1$, $f(x) = c(x^k - 1)/(x - 1)$ and $g(x) = (x^j - 1)/(x - 1)$ are relatively prime. Furthermore, one of k and j is not divisible by the characteristic of F_q, and so one of $f(x)$ and $g(x)$ has only simple roots. Property (ii) is then clear.

LEMMA 7. *There exists a sequence $M_3 \leqslant M_4 \leqslant \cdots$ of positive integers with the following property: for $k > 2$ and any finite field F_q with $q \geqslant M_k$, there is no permutation polynomial of F_q of the form $ax^k + bx^j \in F_q[x]$ with $ab \neq 0$, $1 < j < k$, and $\gcd(k, j) = 1$.*

PROOF. If $ab \neq 0$, $1 < j < k$, and $\gcd(k, j) = 1$, then it follows from Lemma 6 that the equation (7) satisfies the conditions of [11, page 175, Theorem 7B]. It follows from this theorem that the number N of solutions $(x_0, y_0) \in F_q \times F_q$ of (7) satisfies

$$|N - q| \leqslant C(k - 1, k - j)q^{1/2}$$

for some positive constant $C(k - 1, k - j)$ depending on $k - 1$ and $k - j$. With $C(k) = \max_j C(k - 1, k - j)$ we get

$$|N - q| \leqslant C(k)q^{1/2}.$$

Let N^* be the number of solutions with either $x_0 = 1$ or $y_0 = 0$. If $x_0 = 1$, then (7) yields $jy_0^{k-j} + kab^{-1} = 0$, and since we cannot have $j = k = 0$ in F_q because of $\gcd(k, j) = 1$, we get at most $k - j$ values for y_0. If $y_0 = 0$, we obtain at most $k - 1$ values for x_0. Altogether,

$$N^* \leqslant (k - j) + (k - 1) \leqslant 2k - 3.$$

Now choose $M_3 \leqslant M_4 \leqslant \cdots$ such that

$$q - C(k)q^{1/2} > 2k - 3 \quad \text{for all } q \geqslant M_k.$$

Then $N > N^*$ for $q \geqslant M_k$, and the result follows from Lemma 4.

THEOREM 11. *Let $e = \gcd(k, j)$. If $e = k/2$, then there is no permutation polynomial of F_q of the form* (6). *If either $e < k/2$, $e < j$, or $e < k/2$, $e = j$ and k/e is not a prime power, then there exists M_k such that for all finite fields F_q with $q \geqslant M_k$ there is no permutation polynomial of F_q of the form* (6). *If $e < k/2$, $e = j$, and k/e is a power of the prime p, then for all F_q with $q \geqslant M_k$ and characteristic $\neq p$ there is no permutation polynomial of F_q of the form* (6).

PROOF. If $e = k/2$, then $j = e$, and the resulting binomial $ax^{2e} + bx^e$ is never a permutation polynomial of F_q. If $e < k/2$ and $e < j$, then by Lemmas 5 and 7 we

will not get a permutation polynomial of F_q of the form (6) if $q \geqslant M_{k/e}$, thus a fortiori not if $q \geqslant M_k$. If $e < k/2$ and $e = j$, then by Lemma 5 and Theorem 9 we get the desired results in the remaining cases.

REMARK 6. In the case not covered by Theorem 11, namely $e < k/2$, $e = j$, and k/e a power of the characteristic p of F_q, say $k/e = p^t$, the binomials are of the form $ax^{jp^t} + bx^j \in F_q[x]$. If $\gcd(j, q-1) > 1$, no binomial of this form can be a permutation polynomial of F_q. If $\gcd(j, q-1) = 1$, then by Lemma 5 and Theorem 10 there are infinitely many F_q of characteristic p for which there exist permutation polynomials of F_q of the form $ax^{jp^t} + x^j$ with $a \in F_q^*$.

References

1. L. Carlitz, 'Some theorems on permutation polynomials,' *Bull. Amer. Math. Soc.* **68** (1962), 120–122.
2. L. Carlitz, 'Permutations in finite fields,' *Acta Sci. Math. (Szeged)* **24** (1963), 196–203.
3. J. Dénes and A. D. Keedwell, *Latin squares and their applications* (Academic Press, New York, 1974).
4. 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.* (1) **11** (1896/97), 65–120.
5. L. E. Dickson, *Linear groups* (Dover, New York, 1958).
6. M. Hall, Jr., *Combinatorial theory* (Blaisdell Publ. Co., Waltham, Mass., 1967).
7. H. Lausch and W. Nöbauer, *Algebra of polynomials* (North-Holland, Amsterdam, 1973).
8. H. B. Mann, 'The construction of orthogonal latin squares,' *Ann. Math. Statist.* **13** (1942), 418–423.
9. H. Niederreiter and K. H. Robinson, 'Bol loops of order pq,' *Math. Proc. Cambridge Philos. Soc.* **89** (1981), 241–256.
10. W. M. Schmidt, 'Zur Methode von Stepanov,' *Acta Arith.* **24** (1973), 347–367.
11. W. M. Schmidt, *Equations over finite fields* (Lecture Notes in Math., Vol. 536, Springer-Verlag, Berlin-Heidelberg-New York, 1976).

Kommission für Mathematik
Österreichische Akademie der Wissenschaften
Dr. Ignaz-Seipel-Platz 2
A-1010 Wien
Austria

Department of Mathematics
University of the West Indies
Kingston 7
Jamaica