J. Austral. Math. Soc. (Series A) 38 (1985), 164–170

THE STRUCTURE OF A GROUP OF PERMUTATION POLYNOMIALS

GARY L. MULLEN and HARALD NIEDERREITER

(Received 24 November 1983; revised 31 January 1984)

Communicated by R. Lidl

Abstract

Let G_q be the group of permutations of the finite field F_q of odd order q that can be represented by polynomials of the form $ax^{(q+1)/2} + bx$ with $a, b \in F_q$. It is shown that G_q is isomorphic to the regular wreath product of two cyclic groups. The structure of G_q can also be described in terms of cyclic, dicyclic, and dihedral groups. It also turns out that G_q is isomorphic to the symmetry group of a regular complex polygon.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*): 12 C 05, 20 B 25, 20 E 22, 51 F 15

1. Introduction

Let F_q be the finite field of order q. Then every mapping from F_q into itself can be uniquely represented by a polynomial in $F_q[x]$ of degree less than q, and composition of mappings corresponds to composition of polynomials $\bmod(x^q - x)$ (see [9, Chapter 7]). In particular, every group of permutations of F_q can be represented by a set of polynomials in $F_q[x]$ of degree less than q that is closed under composition $\bmod(x^q - x)$. According to a well-known definition (see [8, Chapter 4], [9, Chapter 7]), a polynomial f over F_q for which the corresponding polynomial mapping $c \in F_q \to f(c)$ is a permutation is called a permutation polynomial of F_q. Numerous papers have been written on the structure of permutation groups represented by a given group of permutation polynomials of F_q under composition $\bmod(x^q - x)$; see for example Carlitz [1],

https://doi.org/10.1017/S1446788700023016 Published online by Cambridge University Press

Fryer [6], Lausch and Nöbauer [8, Chapter 4], Lidl and Niederreiter [9, Chapter 7], Nöbauer [12], and Wells [15], [16].

In the present paper we determine the structure of a group of permutation polynomials that was discovered recently by Niederreiter and Robinson [11]. In Remark 2 on page 205 of that paper it is pointed out that for odd q the set of polynomials in $F_q[x]$ of the form $ax^{(q+1)/2} + bx$ with $a, b \in F_q$ is closed under composition mod$(x^q - x)$. In particular, the set of permutation polynomials of F_q of this form is a group under composition mod$(x^q - x)$, and we shall denote this group by G_q. We will establish some preparatory results in Section 2. These will enable us to determine the structure of G_q in Section 3. In fact, several descriptions of the structure of G_q will be given. We are grateful to the referee for pointing out that G_q can also be described in terms of wreath products.

It is convenient to identify a polynomial over F_q with the corresponding polynomial mapping, so that an identity $f = g$ with $f, g \in F_q[x]$ means $f \equiv g$ mod$(x^q - x)$. Throughout the rest of this paper, q will be an odd prime power and n will denote the value $(q-1)/2$. The group G_q can then be described as the group of permutations of F_q of the form $ax^{n+1} + bx$ with $a, b \in F_q$.

2. Preparatory results

We determine first the order of the group G_q. We write $|G|$ for the order of a finite group G.

LEMMA 1. $|G_q| = 2n^2$.

PROOF. Let N be the number of permutations of F_q of the form $f(x) = x^{n+1} + bx$ with $b \in F_q$. Clearly, $f(x)$ is a permutation of F_q if and only if $af(x)$ is a permutation for $a \in F_q$, $a \neq 0$. If $a \neq 0$ is fixed, then the set of polynomial mappings $ax^{n+1} + bx$ with $b \in F_q$ also contains exactly N permutations. If $a = 0$, then bx is a permutation if and only if $b \neq 0$. It follows that

$$(1) \qquad |G_q| = (q-1)N + q - 1 = (q-1)(N+1) = 2n(N+1).$$

By Theorem 5 of [11], $x^{n+1} + bx$ is a permutation polynomial of F_q if and only if $\psi(b^2 - 1) = 1$, where ψ is the quadratic character defined by $\psi(0) = 0$ and $\psi(c) = 1$ or -1 depending on whether c is a nonzero square or a nonsquare in F_q.

Consequently,

$$N = \sum_{\substack{b \in F_q \\ b \neq \pm 1}} \frac{1}{2}\left[1 + \psi(b^2 - 1)\right] = -1 + \frac{1}{2} \sum_{b \in F_q} \left[1 + \psi(b^2 - 1)\right]$$
$$= \frac{q-2}{2} + \frac{1}{2} \sum_{b \in F_q} \psi(b^2 - 1) = \frac{q-3}{2} = n - 1,$$

where we used Theorem 5.48 in [9] to evaluate the character sum. The lemma follows now from (1).

In order to determine the structure of G_q, we make use of the following law of composition observed in [11, p. 205]: if $f_1(x) = ax^{n+1} + bx$ and $f_2(x) = cx^{n+1} + dx$ with $a, b, c, d \in F_q$, then

$$(2) \qquad (f_1 \circ f_2)(x) = (ae + bc)x^{n+1} + (ah + bd)x,$$

where $\circ$ denotes composition and

$$(3) \quad e = \tfrac{1}{2}(c + d)^{n+1} + \tfrac{1}{2}(d - c)^{n+1}, \qquad h = \tfrac{1}{2}(c + d)^{n+1} - \tfrac{1}{2}(d - c)^{n+1}.$$

We construct now a special element of G_q which will prove useful in the sequel. We recall that a generator of the cyclic multiplicative group of F_q is called a primitive element of F_q.

Lemma 2. *Let r be a primitive element of F_q. Then*

$$f(x) = \tfrac{1}{2}(1 - r^2)x^{n+1} + \tfrac{1}{2}(1 + r^2)x$$

is an element of G_q of order n.

Proof. For $g(x) = ax^{n+1} + bx$ with $a, b \in F_q$ we calculate $g \circ f$. The appropriate values of e and h from (3) are $e = \frac{1}{2}(1 + r^2)$ and $h = \frac{1}{2}(1 - r^2)$, so that (2) yields

$$(g \circ f)(x) = \tfrac{1}{2}\left[a(1 + r^2) + b(1 - r^2)\right]x^{n+1} + \tfrac{1}{2}\left[a(1 - r^2) + b(1 + r^2)\right]x.$$

A straightforward induction on m shows then that the m-fold composition f^m is given by

$$(4) \qquad f^m(x) = \tfrac{1}{2}(1 - r^{2m})x^{n+1} + \tfrac{1}{2}(1 + r^{2m})x.$$

It follows that f^m is the identity mapping if and only if $r^{2m} = 1$, and since the order of r is $2n$, the least positive m for which f^m is the identity mapping is $m = n$. In particular, f is a permutation of F_q and thus an element of G_q.

Let r be a fixed primitive element of F_q and let X denote the element of G_q constructed in Lemma 2. Furthermore, let Y be the element of G_q given by the linear permutation polynomial rx of F_q. This notation will be used throughout the rest of this section.

Lemma 3. *Every element of G_q can be represented uniquely in the form X^iY^j with $0 \leqslant i < n, 0 \leqslant j < 2n$.*

Proof. Since $|G_q| = 2n^2$ by Lemma 1, it suffices to show that the elements X^iY^j, $0 \leqslant i < n$, $0 \leqslant j < 2n$, are all distinct. Suppose $X^iY^j = X^kY^l$ with $0 \leqslant i$, $k < n$ and $0 \leqslant j$, $l < 2n$, where we can assume (with no loss of generality) that $i \geqslant k$. With $m = i - k$ we get then $X^m = Y^{l-j}$, so that X^m is represented by a linear polynomial. The formula for X^m in (4) shows that this is only possible if $r^{2m} = 1$. Since $0 \leqslant m < n$, it follows that $m = 0$, hence $i = k$. Then $Y^j = Y^l$, and since Y is an element of order $2n$, we get $j = l$, and the proof if complete.

The following lemma gives a set of generators and relations for the group G_q. The symbol 1 will henceforth also denote the identity element of a group. The correct interpretation of the symbol 1 will always be clear from the context.

Lemma 4. $G_q = \left\langle X, Y \mid X^n = Y^{2n} = (X^{-1}Y)^2 = 1, XY^2 = Y^2X \right\rangle$.

Proof. The fact that X and Y generate G_q follows already from Lemma 3. Now $X^n = 1$ follows from Lemma 2 and $Y^{2n} = 1$ is clearly satisfied. Moreover, $X^{-1} = X^{n-1}$ is represented by

$$\tfrac{1}{2}(1 - r^{2(n-1)})x^{n+1} + \tfrac{1}{2}(1 + r^{2(n-1)})x = \tfrac{1}{2}(1 - r^{-2})x^{n+1} + \tfrac{1}{2}(1 + r^{-2})x$$

according to (4). Hence $X^{-1}Y$ and $Y^{-1}X$ are both represented by

$$\tfrac{1}{2}(r^{-1} - r)x^{n+1} + \tfrac{1}{2}(r^{-1} + r)x$$

since $r^n = -1$. This implies $(X^{-1}Y)^2 = 1$. The remaining relation $XY^2 = Y^2X$ can be checked easily.

On the basis of the relations in Lemma 4 we can calculate the group law for G_q.

Lemma 5.

$$(5) \qquad (X^iY^j)(X^kY^l) = \begin{cases} X^{i+k}Y^{j+l} & \text{if } j \text{ is even},\\ X^{i-k}Y^{j+l+2k} & \text{if } j \text{ is odd}. \end{cases}$$

Proof. The first part of (5) is clear since Y^2 commutes with X by Lemma 4. Next we note that $(YX^{-1}Y^{-1})^{-k} = YX^kY^{-1}$, and since $YX^{-1}Y^{-1} = (YX^{-1}Y)Y^{-2} = XY^{-2}$ by the third relation in Lemma 4, we have

$$YX^k = (YX^{-1}Y^{-1})^{-k}Y = (XY^{-2})^{-k}Y = X^{-k}Y^{2k+1}.$$

The second part of (5) follows now, since for odd j we get

$$(X^iY^j)(X^kY^l) = X^iY^{j-1}YX^kY^l = (X^iY^{j-1})(X^{-k}Y^{2k+l+1})$$
$$= X^{i-k}Y^{j+l+2k},$$

where we used the first part of (5) in the last step.

3. The structure of the group

We convert now the presentation in Lemma 4 into a simpler one. It is clear that G_q is also generated by X and $R = X^{-1}Y$. From Lemma 4 we have $R^2 = 1$, and the relation $XY^2 = Y^2X$ can be rewritten as $X(XR)^2 = (XR)^2X$, or $(XR)^2 = (RX)^2$. From the fact that X commutes with $(XR)^2$, one obtains easily by induction that $(XR)^{2k} = (X^kR)^2$ for all positive integers k. In particular, the relation $Y^{2n} = 1$ in Lemma 4 follows. Hence G_q has the presentation

$$G_q = \left\langle X, R \mid X^n = R^2 = 1, (XR)^2 = (RX)^2 \right\rangle.$$

Thus G_q is the group $n[4]2$ in the notation of Coxeter and Moser [4]. More generally, for any positive integer m the group $m[4]2$ is defined by

$$m[4]2 = \left\langle X, R \mid X^m = R^2 = 1, (XR)^2 = (RX)^2 \right\rangle.$$

The relation $(XR)^2 = (RX)^2$ can also be interpreted to say that X commutes with $RXR = R^{-1}XR = X^R$. It follows now from Theorem 5 in Johnson [7, Chapter 15] that the presentation of $m[4]2$ is the same as the presentation of the regular wreath product $C_m \operatorname{wr} C_2$, where C_m denotes the cyclic group of order m. Thus we have shown the following result.

THEOREM. *The group G_q of all permutations of F_q of the form $ax^{n+1} + bx$ with a, $b \in F_q$ is isomorphic to the regular wreath product $C_n \operatorname{wr} C_2$, where $n = (q-1)/2$. More generally, the group $m[4]2$ is isomorphic to the regular wreath product $C_m \operatorname{wr} C_2$ for all positive integers m.*

The groups $m[4]2$ have been studied in the literature in connection with the theory of symmetries of regular complex polytopes (see [3]). In particular, as indicated by Shephard [13], [14], the group $m[4]2$ can be viewed as the symmetry group of the complex polygon with m^2 vertices (θ_1, θ_2), where θ_1 and θ_2 run independently through the complex mth roots of unity. Further details regarding the precise definitions of regular complex polytopes and their groups of symmetries can be found in [3]. Crowe [5] gives an alternative interpretation of $m[4]2$ as a group of equivalence classes of quaternion transformations. The groups $m[4]2$ belong also to the family of complex reflection groups; see the paper of Cohen [2] in which the notation $G(m,1,2)$ is used for $m[4]2$.

For odd m the group $m[4]2$ has the direct product form $D_m \times C_m$, where D_m is the dihedral group of order $2m$; see [4, p. 78]. This fact can also be deduced from the description of $m[4]2$ as the regular wreath product $C_m \operatorname{wr} C_2$. Indeed, Theorem

https://doi.org/10.1017/S1446788700023016 Published online by Cambridge University Press

7.1 of Neumann [10] shows that $C_m \operatorname{wr} C_2$ has a nontrivial direct product decomposition. An inspection of the proof of this theorem yields a direct factor Q isomorphic to $C_m = \langle \alpha \rangle$ and a direct factor P consisting of all pairs (b, f) with $b \in C_2 = \langle \beta \rangle$ and $f\colon C_2 \to C_m$ being a mapping satisfying $f(1)f(\beta) = 1$. Now P is generated by $S = (\beta, f_0)$ and $T = (1, f_1)$, where $f_0(1) = f_0(\beta) = 1$, $f_1(1) = \alpha$, $f_1(\beta) = \alpha^{-1}$, and S and T satisfy the relations $S^2 = T^m = (ST)^2 = 1$, so that P is isomorphic to D_m. If $m[4]2$ is given by the presentation in Lemma 4 (with n replaced by m), then the direct factors P and Q can be identified explicitly. Using the group law in Lemma 5, one verifies that $P = \{X^{-j}Y^j\colon 0 \leqslant j < 2m\}$ is a normal subgroup of $m[4]2$ with generators $S = X^{-1}Y$ and $T = X^{-2}Y^2$ and relations $S^2 = T^m = (ST)^2 = 1$, so that P is isomorphic to D_m. Furthermore, $Q = \langle Y^2 \rangle$ is a normal cyclic subgroup of $m[4]2$ of order m, and $P \cap Q = \{1\}$ since m is odd. Moreover, $|PQ| = |P|\,|Q| = 2m^2$, the order of $m[4]2$, hence $m[4]2$ is isomorphic to $P \times Q$. In particular, G_q is isomorphic to $D_n \times C_n$ with $n = (q-1)/2$ provided that $q \equiv 3 \pmod 4$.

For even m the group $m[4]2$ can also be described in terms of cyclic and dicyclic groups. Let $C_{2m} = \langle \gamma \rangle$ be an abstract cyclic group of order $2m$, and let

$$E_m = \left\langle \delta, \varepsilon \,|\, \delta^m = \varepsilon^2 = (\delta\varepsilon)^2 \right\rangle$$

be an abstract dicyclic group of order $4m$ with generators δ and ε of orders $2m$ and 4, respectively (compare with [4]). Then C_{2m} has the subgroup $C_m = \langle \gamma^2 \rangle$ of index 2, and E_m contains the dicyclic group

$$E_{m/2} = \left\langle \delta^2, \varepsilon \,|\, (\delta^2)^{m/2} = \varepsilon^2 = (\delta^2\varepsilon)^2 \right\rangle$$

as a subgroup of index 2. Hence $C_m \times E_{m/2}$ is a normal subgroup of $C_{2m} \times E_m$, and $H_m = L_m(C_m \times E_{m/2})$ is a subgroup of $C_{2m} \times E_m$, where L_m is the cyclic subgroup of $C_{2m} \times E_m$ generated by (γ, δ^{-1}). The elements of H_m can be represented uniquely in the form $(\gamma^{2a+d}, \delta^{2b-d}\varepsilon^c)$ with $0 \leqslant a < m$, $0 \leqslant b < m$, $0 \leqslant c < 2$, $0 \leqslant d < 2$. One constructs a mapping $\varphi\colon H_m \to m[4]2$ by using the presentation of $m[4]2$ in Lemma 4 (with n replaced by m) and setting

$$\varphi\left(\gamma^{2a+d}, \delta^{2b-d}\varepsilon^c\right) = X^{-2b+d+mc/2-c}Y^{2a+2b+c}.$$

By an elementary but lengthy calculation based on the group law in Lemma 5 one shows that φ is an epimorphism with kernel $K_m = \langle (\gamma^m, \delta^m) \rangle$. Therefore, $m[4]2$ is isomorphic to H_m/K_m. This description of $m[4]2$ for even m is more explicit than the one given in Crowe [5].

References

[1] L. Carlitz, 'Permutations in a finite field', *Proc. Amer. Math. Soc.* **4** (1953), 538.
[2] A. M. Cohen, 'Finite complex reflection groups', *Ann. Sci. Ecole Norm. Sup.* (4) **9** (1976), 379–436.
[3] H. S. M. Coxeter, *Regular complex polytopes* (Cambridge Univ. Press, London, 1974).
[4] H. S. M. Coxeter and W. O. J. Moser, *Generators and relations for discrete groups* (3rd ed., Springer-Verlag, Berlin-Heidelberg-New York, 1972).
[5] D. W. Crowe, 'The groups of regular complex polygons', *Canad. J. Math.* **13** (1961), 149–156.
[6] K. D. Fryer, 'Note on permutations in a finite field', *Proc. Amer. Math. Soc.* **6** (1955), 1–2.
[7] D. L. Johnson, *Presentation of groups* (London Math. Soc. Lecture Note Series, Vol. 22, Cambridge Univ. Press, Cambridge, 1976).
[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] P. M. Neumann, 'On the structure of standard wreath products of groups', *Math. Z.* **84** (1964), 343–373.
[11] H. Niederreiter and K. H. Robinson, 'Complete mappings of finite fields', *J. Austral. Math. Soc.* (*Ser. A*) **33** (1982), 197–212.
[12] W. Nöbauer, 'Über eine Klasse von Permutationspolynomen und die dadurch dargestellten Gruppen', *J. Reine Angew. Math.* **231** (1968), 215–219.
[13] G. C. Shephard, 'Regular complex polytopes', *Proc. London Math. Soc.* (3) **2** (1952), 82–97.
[14] G. C. Shephard, 'Unitary groups generated by reflections', *Canad. J. Math.* **5** (1953), 364–383.
[15] C. Wells, 'Groups of permutation polynomials', *Monatsh. Math.* **71** (1967), 248–262.
[16] C. Wells, 'Generators for groups of permutation polynomials over finite fields', *Acta Sci. Math. Szeged* **29** (1968), 167–176.

Department of Mathematics
The Pennsylvania State University
University Park, Pennsylvania 16802
U.S.A.

Mathematical Institute
Austrian Academy of Sciences
Dr. Ignaz-Seipel-Platz 2
A-1010 Vienna
Austria