J. Korean Math. Soc. **33** (1996), No. 1, pp. 81–87

PERMUTATION POLYNOMIALS OF THE TYPE $1 + x + \cdots + x^k$

KYUNG HEE KIM*, JUNE BOK LEE* AND YOUNG H PARK

1. Introduction

Let $\mathbb{F}_q$ denote the finite field of order $q = p^n$, p a prime. A polynomial $f \in \mathbb{F}_q[x]$ is called a permutation polynomial over $\mathbb{F}_q$ if f induces a 1-1 map of $\mathbb{F}_q$ onto itself. When q is even, permutation polynomials of the type $h_k(x) = 1 + x + \cdots + x^k$ are useful in the construction of ovals in the projective plane $PG(2, \mathbb{F}_q)$ and an oval in the projective plane $PG(2, \mathbb{F}_q)$ is defined to be a set of $q + 2$ points of $PG(2, \mathbb{F}_q)$ no three of which are collinear [2]. For any $f \in \mathbb{F}_q[x]$, let $A(f) = \{(f(c), c, 1) | c \in \mathbb{F}_q\} \cup \{(1, 0, 0), (0, 1, 0)\}$. Chou [1] has shown the followings:

THEOREM 1.1. *Let $q = 2^n$ with $n > 1$. Then $A(x^{k+1})$ with $1 \leq k \leq q - 2$ is an oval in $PG(2, \mathbb{F}_q)$ if and only if $h_k(x)$ is a permutation polynomial of $\mathbb{F}_q$.* □

THEOREM 1.2. *Let $q = p^n$, p a prime. If $h_k(x) = 1 + x + \cdots + x^k$ is a permutation polynomial of $\mathbb{F}_q$, then there is a nonnegative integer m such that*

1) $k \equiv mp(p-1) + 1 \pmod{p(q-1)}$, *with* $mp(p-1) + 1 \leq q - 2$

2) $(mp(p-1)+1, q-1) = 1 = \begin{cases} (\frac{mp(p-1)}{2} + 1, \frac{q-1}{2}) & \text{if } q \text{ is odd,} \\ (m+1, q-1) & \text{if } q \text{ is even.} \end{cases}$ □

For q odd, permutation polynomials of the type $h_k(x)$ are completely determined by the following:

Received October 19, 1994. Revised June 10, 1995.
1991 AMS Subject Classification: 11T06.
Key words: Permutation polynomial, finite field.
* Research supported in part by NON DIRECTED RESEARCH FUND, Korea Research Foundation, 1993 and partially supported by BSRI-94-1423.

THEOREM 1.3 ([3]). *For q odd, $h_k(x) = 1 + x + \cdots + x^k$ is permutation polynomial over $\mathbb{F}_q$ if and only if $k \equiv 1 \pmod{p(q-1)}$.* □

Let $q = 2^n$. In this case, Theorem 1.2 is not enough to determine whether or not $h_k(x)$ is a permutation polynomial. Let $\mathbb{N}_q = \{0, 1, 2, \ldots, q-2\}$. Then Theorem 1.2 shows that we may consider only those odd $k \in \mathbb{N}_q$ such that $(k, q-1) = (k+1, q-1) = 1$ to find permutation polynomials of the type $h_k(x)$. Let

$$P_q = \{k \in \mathbb{N}_q \mid h_k(x) \text{ is a permutation polynomial over } \mathbb{F}_q\}.$$

We will show that there exists an action of the dihedral group D_3 of order 6 on P_q. Since P_q is difficult to determine, we will look at larger D_3-sets, which are easier to determine, and discuss how to get closer to P_q using the action of D_3.

2. Permutation Polynomials of $h_k(x)$ when q is even

From now on, we assume that $q = 2^n$, $n \geq 2$, unless stated otherwise. There are some classes of permutation polynomials which are easy to determine.

THEOREM 2.1. *Let $q = 2^n$ and $m < n$.*

(1) *$h_{2^m-1}(x)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $(m, n) = 1$.*
(2) *$h_5(x)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if n is odd.*

Proof. We have $h_{2^m-1}(x) = \dfrac{1 + x^{2^m}}{1 + x} = \dfrac{(1+x)^{2^m}}{1+x} = (1+x)^{2^m-1}$. Hence, $h_{2^m-1}(x)$ is a permutation polynomial of $\mathbb{F}_q$ iff $(1+x)^{2^m-1}$ is a permutation polynomial of $\mathbb{F}_q$ iff x^{2^m-1} is a permutation polynomial of $\mathbb{F}_q$ iff $(2^m - 1, 2^n - 1) = 1$ iff $(m, n) = 1$. This proves (1). To show (2), let $g_5(x, a)$ denote the Dickson polynomial [2]. Then $g_5(x+1, 1) = \sum_{j=0}^{\lfloor 5/2 \rfloor} \frac{5}{5-j}\binom{5-j}{j}(-1)^j(x+1)^{5-2j} = h_5(x)$ over $\mathbb{F}_{2^n}$. It is well known that $g_5(x+1, 1)$ is a permutation polynomial of $\mathbb{F}_{2^n}$ iff $(5, 2^{2n} - 1) = 1$ [2]. Since $(5, 2^{2n} - 1) = 1$ iff n is odd, (2) follows. □

We now discuss two theorems, which produce new permutation polynomials from known ones.

THEOREM 2.2 ([1]). *$h_k(x) = 1 + x + \cdots + x^k$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $h_{q-2-k}(x) = 1 + x + \cdots + x^{q-2-k}$ is a permutation polynomial of $\mathbb{F}_q$.* □

LEMMA 2.3 ([2]). *Let $a_0, a_1, \cdots, a_{q-1}$ be elements of $\mathbb{F}_q$, where $q = p^n$, p a prime. Then the following two conditions are equivalent:*

(1) *$a_0, a_1, \cdots, a_{q-1}$ are distinct;*

(2) $\sum_{i=0}^{q-1} a_i^t = \begin{cases} 0 & \text{for } t = 0, 1, \ldots, q-2, \\ -1 & \text{for } t = q-1. \end{cases}$ □

LEMMA 2.4. *Let $k \in \mathbb{N}_q$. If $h_k(x) = 1 + x + \cdots + x^k$ permutes $\mathbb{F}_q - \{0, 1\}$, then $h_k(x)$ is a permutation polynomial over $\mathbb{F}_q$.*

Proof. By Lemma 2.3, $\sum_{a \in \mathbb{F}_q} h_k(a) = 0$. Also we have

$$\sum_{a \in \mathbb{F}_q} h_k(a) = h_k(0) + h_k(1) + \sum_{a \in \mathbb{F}_q - \{0,1\}} h_k(a) = 1 + h_k(1) + \sum_{a \in \mathbb{F}_q - \{0,1\}} a$$
$$= 1 + h_k(1) + (-1) = h_k(1).$$

Hence, $h_k(1) = 0$. Since $h_k(0) = 1$, $h_k(x)$ is a permutation polynomial over $\mathbb{F}_q$. □

For $k \in \mathbb{N}_q$ with $(k, q-1) = 1$, denote by $k^{-1} \in \mathbb{N}_q$ the multiplicative inverse modulo $q - 1$. For $k \in \mathbb{N}_q$ with $(k+1, q-1) = 1$ denote by k^* the number in $\mathbb{N}_q$ such that $(k+1)(k^*+1) \equiv 1 \pmod{q-1}$. In other words, $k^* = (k+1)^{-1} - 1 \in \mathbb{N}_q$.

THEOREM 2.5. *$h_k(x) = 1 + x + \cdots + x^k$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $h_{k^*}(x) = 1 + x + \cdots + x^{k^*}$ is a permutation polynomial of $\mathbb{F}_q$.*

Proof. Suppose that $h_k(x)$ is a permutation polynomial of $\mathbb{F}_q$. Then k^* exists and $(k^*+1, q-1) = 1$. Thus x^{k^*+1} is a permutation polynomial of $\mathbb{F}_q$. For $a \neq 0, 1$,

$$h_{k^*}(a) = \frac{1 + a^{k^*+1}}{1 + a} = \frac{1 + a^{k^*+1}}{1 + a^{(k^*+1)(k+1)}} = \frac{1}{h_k(a^{k^*+1})}.$$

Since $h_k(x)$ and x^{k^*+1} permute $\mathbb{F}_q - \{0, 1\}$, $h_{k^*}(a)$ permutes $\mathbb{F}_q - \{0, 1\}$, also. Thus, by Lemma 2.4, $h_{k^*}(x)$ is a permutation polynomial of $\mathbb{F}_q$. The converse does hold by the same way. □

3. Orbits of permutation polynomials.

Let $R_q = \{k \in \mathbb{N}_q \mid (k, q-1) = 1 = (k+1, q-1)\}$. Define two maps $\alpha, \beta : R_q \to R_q$ by

$$\alpha(k) = q - 2 - k, \quad \beta(k) = (k+1)^{-1} - 1.$$

It is easy to check that α and β are well-defined and $\alpha^2 = \beta^2 = 1$. Let $\sigma = \alpha\beta$ and $\tau = \beta\alpha\beta$, so that

$$\sigma(k) = q - 1 - (k+1)^{-1}, \text{ and } \tau(k) = k^{-1}.$$

Then σ and τ satisfy the relations $\sigma^3 = 1$, $\tau^2 = 1$ and $\sigma\tau\sigma = \tau$. Thus the group generated by σ and τ is the dihedral group

$$G = D_3 = \{1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\},$$

and G acts on R_q in an obvious fashion. Since $\alpha = \tau\sigma$, $\beta = \sigma\tau$, and $\tau\sigma$, $\sigma\tau$ generate G, the set of numbers obtained from $k \in R_q$ by applying α and β repeatedly is the same as the orbit of k under the action of G. Explicitly, we have

PROPOSITION 3.1. *For $k \in R_q$, the orbit of k is given by*

$$G \cdot k = \{k, q-1-(k+1)^{-1}, q-2-k^{-1}, k^{-1}, q-2-k, (k+1)^{-1}-1\}.$$

If h_k is a permutation polynomial, then $h_{k'}$ is a permutation polynomial for every $k' \in G \cdot k$, and if $G \cdot k$ contains an even number, then h_k is not a permutation polynomial. □

As an example, the orbit of $9 \in R_{2^7}$ is $\{9, 38, 13, 113, 117, 88\}$, and hence h_9 is not a permutation polynomial over $\mathbb{F}_{2^7}$.

It is interesting to note that there are no two consecutive odd k's in P_q for even n, since one of k, $k+1$, $k+2$ and $k+3$ is divisible by 3 and $3 \mid 2^n - 1$. For odd n, besides the three obvious consecutive odds 1,3, and 5 in P_q, we have the following:

COROLLARY 3.2. *Assume n is odd. Then $2^{\frac{n+1}{2}} - 1$ and $2^{\frac{n+1}{2}} + 1$ are in P_q.*

Proof. Clearly $k = 2^{(n+1)/2} - 1 \in P_q$, since $(\frac{n+1}{2}, n) = 1$. By Proposition 3.1, $k^{-1} = 2^{(n+1)/2} + 1 \in P_q$. □

An orbit of any $k \in R_q$ consists of either 1,2,3 or 6 elements. We classify such possibilities.

PROPOSITION 3.3. *There is no orbit consisting of 1 element except* $q = 4$. *There is exactly one orbit consisting of 3 elements, namely* $\{1, \frac{q-2}{2}, q-3\}$ *for every* $q \neq 4$. *There exist orbits consisting of 2 elements only if* $9 \nmid q-1$ *and every prime factor of* $q-1$ *is either 3 or congruent to 1 mod 3.*

Proof. There are three subgroups (τ), $(\tau\sigma)$ and $(\tau\sigma^2)$ of order 2, and one subgroup (σ) of 3. Let $k \in R_q$ and G_k be the stabilizer of k in G. Suppose $G_k = G$. Then $k = k^{-1} = -(k+1)^{-1}$, so that $k^2 = 1$ and $k^2 + k = -1$. Hence $4 \equiv 1 \pmod{q-1}$ and thus $q = 4$. Note that $R_4 = \{1\}$. Suppose $G_k = (\tau)$. Then $k = k^{-1}$, or $(k-1)(k+1) = 0$, and thus $k = 1$ since $(k+1)^{-1}$ exists. Similarly we can show that $G_k = (\tau\sigma)$ iff $k = \frac{q-2}{2}$, and $G_k = (\tau\sigma^2)$ iff $k = q-3$. Now $q-3 = \alpha(1)$, $\frac{q-2}{2} = \beta(1)$ and thus $\{1, \frac{q-2}{2}, q-3\}$ is an orbit. Finally if $G_k = (\sigma) = (\sigma^2)$,then $k = -(k+1)^{-1}$ or $(2k+1)^2 = -3$, and hence $x^2 \equiv -3 \pmod{q-1}$ is solvable. It is easy to check that $x^2 \equiv -3$ is solvable modulo 3, but not solvable modulo 9. Let $p \neq 3$ be a prime factor of $q-1$. If $x^2 \equiv -3 \pmod{p}$ is solvable, then $x^2 \equiv -3 \pmod{p^r}$ is solvable. Furthermore, $x^2 \equiv -3 \pmod{p}$ is solvable iff $\left(\frac{-3}{p}\right) = 1$ iff $p \equiv 1 \pmod{3}$, and hence our claim follows. □

For example, if $4 \mid n$, then $5 \mid q-1$ and if $6 \mid n$, then $9 \mid q-1$. Thus, as a corollary, there is no orbit consisting of 2 elements if 4 or 6 divides n. Also an orbit containing 2 elements may or may not be in P_q. For $n = 9$, $\{81, 429\}$ is an orbit not in P_q but for $n = 5$, $\{5, 25\}$ is an orbit in P_q.

Now recall that P_q consists of odd numbers. Thus it is enough to consider

$$R'_q = \{k \in R_q \mid k \text{ is odd}\}.$$

Even though $k \in R'_q$, its orbit can contain even numbers. According to our computation, a large number of orbits of $k \in R'_q$ contain even numbers. Now $G \cdot k$ contains only odd numbers iff k is in the set

$$R''_q = \{k \in R_q \mid k, \sigma(k) \text{ and } \sigma^2(k) \text{ are odd}\}$$

The set R''_q is G-stable. A further reduction to P_q is possible by the following

PROPOSITION 3.4. *Suppose* $m \mid n$. *Let* $q_0 = 2^m$ *and let* $r = r_m : R_q \to R_{q_0}$, $k \mapsto k \pmod{q_0 - 1}$. *Then*

(1) $r(P_q) \subset P_{q_0}$.

(2) *the action of* G *commutes with* r, *and hence for* $k \in P_q$, *we have* $r(G \cdot k) = G \cdot r(k)$.

Proof. The map r is well defined, since $q_0 - 1 \mid q - 1$. Since the coefficients of h_k are in $\mathbb{F}_{q_0}$ for any k, $h_k(\mathbb{F}_{q_0}) \subset \mathbb{F}_{q_0}$, which shows (1). To prove (2), note that $kk' \equiv 1 \pmod{q-1}$ implies $r(k)r(k') \equiv 1 \pmod{q_0 - 1}$, and hence r commutes with σ and τ. □

If we let

$$R_q''' = \{k \in R_q'' \mid r_m(k) \in P_{2^m} \text{ for any } m \mid n\},$$

then we have a series of G-stable sets $R_q \supset R_q'' \supset R_q'''$.

Up to $n = 29$, the set P_q is known for some time. For $n = 3$ to 16 we list the number of orbits under $G = D_3$ of the various sets. Here N', N'', N''', N denote the number of orbits generated by $k \in R_q'$, that of R_q'', that of R_q''', and that of P_q, respectively for each $q = 2^n$.

TABLE

n	N'	N''	N'''	N
3	2	1	1	1
4	2	1	1	1
5	4	3	3	3
6	3	1	1	1
7	16	6	6	5
8	7	3	3	2
9	51	13	8	5
10	39	7	3	2
11	248	52	52	8
12	75	13	5	2
13	1189	180	180	9
14	744	114	21	3
15	3095	504	113	7
16	1675	233	52	4

References

1. W.-S. Chou, *Permutation Polynomials over Finite Fields and Combinatorial Applications*, Ph.D. Diss., the Pennsylvania State University, 1990.
2. R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl., vol. 20, Addison-Wesley, Reading, MA, 1983.
3. R. Matthews, *Permutation properties of the polynomials* $1 + x + \cdots + x^k$ *over a finite field*, Proc. Amer. Math. Soc. **120** no. 1 (1994). 47-51.

Kyung Hee Kim
Department of Mathematics
Yonsei University
Kangwondo 220-701, Korea

June Bok Lee
Department of Mathematics
Yonsei University
Seoul 120-749, Korea

Young H Park
Department of Mathematics
Kangwon National University
Chuncheon 200-701, Korea