43. A Note on Polynomials of the Form $x^d+a_ex^e+\cdots+a_1x+a_0$ over Finite Fields

By Javier GOMEZ-CALDERON

Department of Mathematics, New Kensington Campus, The Pennsylvania State University, U. S. A.

(Communicated by Shokichi IYANAGA, M. J. A., June 7, 1994)

Abstract: Let F_q denote the finite field of order q where q is a prime power. A polynomial $f(x)$ over F_q is called a permutation polynomial of F_q if $f(x)$ induces a 1-1 map of F_q onto itself. In this note we will show that unless q is small relative to $d = deg(f)$, then there is no permutation polynomials of the form

$$xd + a_ex^e + \cdots + a_1x + a_0$$

with $(d, q) = 1$, $a_e \neq 0$, and $1 \leq e \leq D = [(d-1)/2]$ where $[w]$ denote the greatest integer $\leq w$.

1. Introduction. Let F_q denote the finite field of order q where q is a prime power. A polynomial $f(x)$ over F_q is called a *permutation polynomial* (PP) of F_q if $f(x)$ induces a 1-1 map of F_q onto itself. Many properties of PPs can be found in Lidl and Niederreiter [3, Ch. 7] and the recent surveys Lidl and Mullen [1] and [2], and Mullen [4].

H. Niederreiter and K. H. Robinson [5] showed that unless q is small relative to $d = deg(f(x))$, then there is no PP of F_q of the form $x^d + bx$ unless d is a power of the characteristic of F_q. In this note we will generalize Niederreiter and Robinson's result for polynomials of the form

$$x^d + a_ex^e + \cdots + a_1x + a_0$$

with $(d, q) = 1$, $a_e \neq 0$, and $1 \leq e \leq D = [(d-1)/2]$ where $[w]$ denote the greatest integer $\leq w$. More precisely, we will prove the following

Theorem 1. *Let F_q denote the finite field of order q. Let $f(x)$ be a polynomial over F_q of the form*

$$x^d + a_ex^e + \cdots + a_1x + a_0$$

with $(d, q) = 1$, $a_e \neq 0$, and $1 \leq e \leq D = [(d-1)/2]$ where $[w]$ denotes the greatest integer $\leq w$. Then, $f(x)$ is not a permutation polynomial of F_q unless q is small relative to d.

2. Proof of the Theorem. The proof of the Theorem will need the following lemmas.

Lemma 2. *Let $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0$ denote a monic polynomial over F_q of degree d prime to q. Let the irreducible factorization of $f^*(x, y) = f(x) - f(y)$ be given by*

$$f^*(x, y) = \prod_{i=1}^{s} f_i(x, y).$$

Let

$$f_i(x, y) = \sum_{j=0}^{n_i} g_{ij}(x, y)$$

be the homogeneous decomposition of $f_i(x, y)$ *so that* $n_i = deg(f_i(x))$ *and* $g_{ij}(x, y)$ *is homogeneous of degree* j. *Assume* $a_{d-1} = a_{d-2} = \cdots = a_{d-r} = 0$ for some $r \geq 1$. *Then,*

$$g_{i,n-1}(x, y) = g_{i,n-2}(x, y) = \cdots = g_{i,R_i}(x, y) = 0$$

where

$$R = \begin{cases} n_i - r & \text{if } n_i \geq r \\ 0 & \text{if } n_i \leq r \end{cases}.$$

Proof. Let e_i denote the second highest degree of $f_i(x, y)$ defined by

$$e_i = \begin{cases} deg(f_i(x, y) - g_{in_i}(x, y)) & \text{if } f_i(x, y) \neq g_{in_i}(x, y) \\ -\infty & \text{if } f_i(x, y) = g_{in_i}(x, y) \end{cases}.$$

Then we assume, WLOG, that $n_1 - e_1 \leq n_2 - e_2 \leq \ldots \leq n_s - e_s$. Let i_0 denote the largest integer i such that $N = n_1 - e_1 = n_2 - e_2 = \ldots = n_i - e_i$. Our goal is to show that $N > r$. So, we assume that N is finite. Hence, $g_{ie_i}(x, y) \neq 0$ for all i, $1 \leq i \leq i_0$ and

$$a_{d-N}(x^{d-N} - y^{d-N}) = \sum_{i=1}^{i_0} g_{ie_i}(x, y) \prod_{\substack{j=1 \\ j\neq i}}^{s} g_{jn_i}(x, y).$$

Now, on the other hand, we have

$$x^d - y^d = \prod_{j=1}^{s} g_{jn_i}(x, y).$$

Therefore,

$$a_{d-N}\frac{x^{d-N} - y^{d-N}}{x^d - y^d} = \sum_{i=1}^{i_0} \frac{g_{ie_i}(x, y)}{g_{in_i}(x, y)}.$$

As $(d, q) = 1$, $x^d - y^d$ has no multiple divisor in the algebraic closure of F_q, so that the denominators in the right hand side of the above formula are relatively prime to each other, and if the denominator and nominator of each summand have common factor, if can be cancelled out. Therefore the right-hand side of the above formula does not vanish. Thus $a_{d-N} \neq 0$ and consequently $d - N < d - r$. Thus, $N > r$ and the proof of the lemma is complete.

Lemma 3. Let $f(x)$ be a monic polynomial over F_q of degree d prime to q. Let N denote the number of linear factors of $f^*(x, y) = f(x) - f(y)$ over F_q. Then, there exists a constant b in F_q such that

$$f(x) = g((x + b)^N)$$

for some polynomial $g(x)$ over F_q.

Proof. Since $(d, q) = 1$ we can choose a constant a in F_q such that $f(x - a) = F(x) = x^d + a_{d-2}x^{d-2} + \ldots + a_1x + a_0$. So, by Lemma 2, all linear factors of $F^*(x, y) = F(x) - F(y)$ have the form $x - a_iy$ for $i = 1,2, \ldots ,N$. Thus, $F(a_ix) = F(x)$ for all i, and consequently $F(a_ia_jx) = F(a_jx) = F(x)$ for all i and j. Therfore, $a_1, a_2, \ldots, a_N$ form a multiplicative group of order N.

Now write

$$F(x) = f_0(x) + f_1(x)x^N + f_2(x)x^{2N} + \ldots + f_m(x)x^{mN}$$

with $deg(f_1(x)) < N$. This decomposition is clearly unique. So, $F(x) =$

$F(a_i x)$ for $i = 1,2,\ldots,N$ implies

$$\begin{aligned} F(x) &= f_0(x) + f_1(x)x^N + f_2(x)x^{2N} + \ldots + f_m(x)x^{mN} \\ &= f_0(a_i x) + f_1(a_i x)(a_i x)^N + f_2(a_i x)(a_i x)^{2N} + \ldots + f_m(a_i x)(a_i x)^{mN} \\ &= f_0(ax) + f_1(a_i x)x^N + f_2(a_i x)x^{2N} + \ldots + f(a_i x)x^{mN} \end{aligned}$$

for $i = 1,2,\ldots,N$. Therefore, $f_i(x) = c_i$ and

$$F(x) = \sum_{i=1}^{m} c_i x^i = g(x^N)$$

where $g(x) = \sum_{i=1}^m c_i x^i \in F_q[x]$.

This completes the proof of the lemma.

We are ready to prove Theorem 1.

Proof of Theorem 1. Let $f_{d,e}(x)$ denote a permutation polynomial over F_q of the form

$$x^d + a_e x^e + \ldots + a_1 x + a_0$$

where $(d, q) = 1$, $a_e \neq 0$, $1 \leq e \leq D = [(d-1)/2]$, and q is large relative to d. Thus, by [5], $f_{3,e}(x)$ is not a PP. Now, to apply induction on d, assume that $f_{i,e}(x)$ is not a PP for $3 \leq i \leq d-1$. We also assume that $f_{d,e}(x)$ is a PP. Then, by [3, Th. 7.29], $f_{d,e}{}^{**}(x, y) = (f_{d,e}(x) - f_{d,e}(y))/(x-y)$ has no absolutely irreducible factors over F_q. Therefore, $f_{d,e}{}^{**}(x, y)$ has at least one factor $h(x, y)$ over $\bar{F}_q$ (the algebraic closure of F_q) of degree r (on both x and y) such that $1 \leq r \leq [(d-1)/2]$. So,

$$f_{d,e}(x) - f_{d,e}(y) = (x-y)h(x, y) \prod_{i=1}^{s} f_i(x, y) \tag{1}$$

for some irreducible polynomials $f_1(x, y), f_2(x, y), \ldots, f_s(x, y)$ over $\bar{F}_q$. Thus, by Lemma 2, $h(x, y)$ is homogeneous of degree r. Then, comparing the highest degree terms in (1), we conclude that $h(x, y)$ divides $x^d - y^d$. Therefore, since $(d, q) = 1$, $h(x, y)$ is a product of linear homogeneous factors and we obtain

$$f_{d,e}(x) = g(x^N)$$

for some integer $N \geq r + 1 \geq 2$ and some polynomial $g(x)$ in $F_q[x]$. Therefore, $g(x)$ is a PP over F_q of the form

$$g(x) = x^{d/N} + a_{m/N} x^{m/N} + \ldots + a_1 x + a_0,$$

where $3 \leq d/N < d$ and $m/N \leq [(d/N - 1)/2]$, a contradiction to our earlier assumptions. Therefore, $f_{d,e}(x)$ is not a PP and, by induction, the proof of the theorem has been completed.

References

[1] R. Lidl and G. L. Mullen: When does a polynomial over a finite field permute the elements of the field?. Amer. Math. Mon., **95**, 243–246 (1988).

[2] ——: ditto., II. ibid., **100**, 71–74 (1993).

[3] R. Lidl and H. Niederreiter: Finite Fields. Encyclo. Math. and Appls. vol. 20, Addison-Wesley, Reading MA (1983) (Now distributed by Camb. Univ. Press).

[4] G. L. Mullen: Permutations over finite fields. Finite Fields and Coding Theory, and Advances in Communications and Computing (Proc. of the Las Vegas Conference of the same title, Aug. 1991) (eds. G. L. Mullen and P. L. -S. Shiue). Lect. Notes in Pure and Applied Mathematics, vol. 141, Marcel Dekker, pp. 131–151 (1993).

[5] H. Niederreiter and K. H. Robinson: Complete mappings of finite fields. J. Austral. Math. Soc., ser. A, **33** (1982).