LOCAL MINIMAL POLYNOMIALS OVER FINITE FIELDS

Maria T. Acosta-de-Orozco

Department of Mathematics, Southwest Texas State University, San Marcos, TX 78666

Javier Gomez-Calderon

Department of Mathematics, Penn State University, New Kensington Campus, New Kensington, PA 15068

(*Submitted June 1994*)

1. INTRODUCTION

Let F_q denote the finite field of order $q = p^e$, where q is an odd prime. If $f(x)$ is a polynomial of degree $d \geq 1$ over F_q, then it is clear that

$$\left[\frac{q-1}{d}\right] + 1 \leq V(f) = \left| \{f(x) : x \in F_q\} \right| \leq q,$$

where $[w]$ denotes the greatest integer less than or equal to w. We say that $f(x)$ permutation polynomial if $V(f) = q$, and $f(x)$ is a minimal value set polynomial if

$$V(f) = \left[\frac{q-1}{d}\right] + 1.$$

A polynomial $f(x, y)$ with coefficients in F_q is a local permutation (minimal value set) polynomial over F_q if $f(a, x)$ and $f(x, b)$ are permutation (minimal value set) polynomials in x for all a and b in F_q. Local permutation polynomials have been studied by Mullen in [5] and [6].

In this note we will consider local minimal polynomials of small degree ($< \sqrt{q}$) on both x and y. We will show that there are only five classes of local minimal polynomials. Namely,

(a) $f(x, y) = aX^mY^n + bX^m + cY^n + d, m, n|(q-1)$,

(b) $f(x, y) = (aX + bY + c)^m + d, m|(q-1)$,

(c) $f(x, y) = aX^2Y^n + bX^2 + cX + dY^n + e, n|(q-1)$,

(d) $f(x, y) = aX^mY^2 + bY^2 + cY + dX^m + e, m|(q-1)$, and

(e) $f(x, y) = aX^2Y^2 + bX^2 + cY^2 + dX + eY + gXY + h$.

where $X = (x - x_0)$ and $Y = (y - y_0)$ with x_0, y_0 in F_q.

2. THEOREM AND PROOF

Minimal value set polynomials have been studied by several authors. L. Carlitz, D. J. Lewis, W. H. Mills, and E. Strauss [2] showed that, when q is a prime and $d = \deg(f) < q$, all minimal value set polynomials with $V(f) \geq 3$ have the form $f(x) = a(x+b)^d + c$ with d dividing $q - 1$. Later, W. H. Mills [4] gave a complete characterization of minimal value set polynomials over arbitrary finite fields with $d < \sqrt{q}$. A weakened form of Mills's results can be stated as follows:

Lemma 1 (Mills): If F_q is a finite field with q elements and $f(x)$ is a monic polynomial over F_q of degree d prime to q, then

$$d < \sqrt{q} \quad \text{and} \quad V(f) = \left[\frac{q-1}{d}\right] + 1$$

imply

$$d \mid (q-1) \quad \text{and} \quad f(x) = (x+b)^d + c.$$

For other related results, see [1] and [3]. We are now ready for our result.

Theorem 2: Let F_q denote a finite field of order $q = p^e$, where p is an odd prime. Let

$$f(x, y) = \sum_{i=0}^{n} a_i(x) y^i = \sum_{j=0}^{m} b_j(y) x^j$$

denote a polynomial with coefficients in F_q. Assume that m, n, $n-1$, and $m-1$ are relatively prime to q and $1 < m, n < \sqrt{q}$. Assume $a_n(x) b_m(y) \neq 0$ for all x, y in F_q. Then $f(x, y)$ is a local minimal polynomial if and only if $f(x, y)$ has one of the following forms:

(a) $f(x, y) = aX^m Y^n + bX^m + cY^n + d, m, n \mid (q-1)$,

(b) $f(x, y) = (aX + bY + c)^m + d, m \mid (q-1)$,

(c) $f(x, y) = aX^2 Y^n + bX^2 + cX + dY^n + e, n \mid (q-1)$,

(d) $f(x, y) = aX^m Y^2 + bY^2 + cY + dX^m + e, m \mid (q-1)$, and

(e) $f(x, y) = aX^2 Y^2 + bX^2 + cY^2 + dX + eY + gXY + h$.

where $X = (x - x_0)$ and $Y = (y - y_0)$ with x_0, y_0 in F_q.

Proof: If $f(x, y)$ is one of the forms (a)–(e), then it is easy to see that $f(x, y)$ is a local minimal value set polynomial. Now, let

$$f(x, y) = \sum_{i=0}^{n} a_i(x) y^i = \sum_{j=0}^{m} b_j(y) x^j$$

denote a local minimal value set polynomial over F_q satisfying:

(i) $1 < m, n < \sqrt{q}$,

(ii) $(mn(m-1)(n-1), q) = 1$,

(iii) $a_n(x) b_m(y) \neq 0$ for all x, y in F_q.

Also, and without loss of generality, assume that $m \le n$ and $n \ge 3$ [$n = 2$ gives form (e)]. Then, by Lemma 1,

$$f(x, y) = a_n(x)\left(y + \frac{a_{n-1}(x)}{n a_n(x)}\right)^n + a_0(x) - \frac{a_{n-1}^n(x)}{n^n a_n^{n-1}(x)}, \tag{1}$$

$$= b_m(y)\left(x + \frac{b_{m-1}(y)}{m b_m(y)}\right)^m + b_0(y) - \frac{b_{m-1}^m(y)}{m^m b_m^{m-1}(y)}, \tag{2}$$

for all x, y in F_q and $m, n|(q-1)$. Hence,

$$b_m^{m-1}(y)\left[\left(a_n(x)y+\frac{a_{n-1}(x)}{n}\right)^n+a_0(x)a_n^{n-1}(x)-\frac{a_{n-1}^n(x)}{n^n}\right]$$
$$=a_n^{n-1}(x)\left[\left(b_m(y)x+\frac{b_{m-1}(y)}{m}\right)^m+b_0(y)b_m^{m-1}(y)-\frac{b_{m-1}^m(y)}{m^m}\right] \tag{3}$$

for all x, y in F_q. Further, since $1<m\le n<\sqrt{q}$, equation (3) also establishes the equality of the polynomials. Therefore,

$$b_m^{m-2}(y)\left[a_n^{n-1}(x)y^n+a_n^{n-2}(x)a_{n-1}(x)y^{n-1}+\cdots+\frac{a_{n-1}^{n-1}(x)}{n^{n-2}}y+a_0(x)a_n^{n-2}(x)\right]$$
$$=a_n^{n-2}(x)\left[b_m^{m-1}(y)x^m+b_m^{m-2}(y)b_{m-1}(y)x^{m-1}+\cdots+\frac{b_{m-1}^{m-1}(y)}{m^{m-2}}x+b_0(y)b_m^{m-2}(y)\right].$$

Hence,

$$a_n^{n-2}(x)\text{ divides }\binom{n}{2}\frac{a_n^{n-3}(x)a_{n-1}^2(x)}{n^2}y^{n-3}+\cdots+\frac{a_{n-1}^{n-1}(x)}{n^{n-2}}$$

and, consequently, $a_n^{n-2}(x)$ divides $a_{n-1}^{n-1}(x)$. Now, if $g(x)$ is an irreducible factor of $a_n(x)$ so that $g^c(x)|a_n(x)$ but $g^{c+1}(x)\nmid a_n(x)$, then $g^e(x)$ divides $a_{n-1}(x)$ for some integer e such that $1< c(n-2)\le(n-1)e$. Therefore, since $\deg(g(x))\ge 2$, $e\le c-1$ implies $c(n-2)\le(n-1)(c-1)$ or $n-1\le c\le\frac{m}{2}\le\frac{n}{2}$, a contradiction. Thus, $a_n(x)$ divides $a_{n-1}(x)$.

Case 1. $a_{n-1}(x)=0$. Then, by (1),

$$f(x,y)=a_n(x)y^n+a_0(x)=\left(\sum_{i=0}^m a_{ni}x^i\right)y^n+\sum_{i=0}^m a_{0i}x^i=\sum_{i=0}^m(a_{ni}y^n+a_{0i})x^i$$
$$=(a_{nm}y^n+a_{0m})\left(x+\frac{a_{nm-1}y^n+a_{0m-1}}{m(a_{nm}y^n+a_{0m})}\right)^m+a_{n0}y^n+a_{00}-\frac{(a_{nm-1}y^n+a_{0m-1})^m}{m^m(a_{nm}y^n+a_{0m})^{m-1}}.$$

Hence, $f(x,y)$ has the form (c) or $m\ge 3$ and

$$(a_{nm}y^n+a_{0m})\binom{m}{i}\left(\frac{a_{nm-1}y^n+a_{0m-1}}{m(a_{nm}y^n+a_{0m})}\right)^{m-i}=a_{ni}y^n+a_{0i}$$

or

$$\binom{m}{i}\left(\frac{a_{nm-1}y^n+a_{0m-1}}{m}\right)^{m-i}=(a_{nm}y^n+a_{0m})^{m-i-1}(a_{ni}y^n+a_{0i}) \tag{4}$$

for all y in F_q and $i=1,2,\ldots,m$. So, if $a_{nm}=0$, then $a_{nm-1}=0$ and we obtain

$$f(x,y)=a_{0m}\left(x+\frac{a_{0m-1}}{ma_{0m}}\right)^m+a_{n0}y^n+a_{00}-\left(\frac{a_{0m-1}}{ma_{0m}}\right)^m a_{0m},$$

where $a_{0m}a_{n0} \neq 0$. On the other hand, if $a_{nm} \neq 0$, then, again by (4),

$$\frac{a_{0m}}{a_{nm}} = \frac{a_{0m-1}}{a_{nm-1}}.$$

Therefore, either $f(x, y)$ has the form (c) or

$$f(x,y) = (a_{nm}y^n + a_{0m})\left(x + \frac{a_{nm-1}y^n + a_{0m-1}}{m(a_{nm}y^n + a_{om})}\right)^m + a_{n0}y^n + a_{00} - \frac{(a_{nm-1}y^n + a_{0m-1})^m}{m^m(a_{nm}y^n + a_{0m})^{m-1}}$$

$$= (a_{nm}y^n + a_{0m})\left(x + \frac{a_{nm-1}}{ma_{nm}}\right)^m + a_{n0}y^n + a_{00} - \left(\frac{a_{nm-1}}{ma_{nm}}\right)^m (a_{nm}y^n + a_{0m})$$

and $f(x, y)$ has the form (a).

Case 2. $a_n(x) | a_{n-1}(x) \neq 0$. Then, by (1),

$$\deg(a_n(x)) + (n-1)\deg\left(\frac{a_{n-1}(x)}{a_n(x)}\right) \leq m.$$

Hence, either $\deg(\frac{a_{n-1}(x)}{a_n(x)}) = 0$ or $\deg(\frac{a_{n-1}(x)}{a_n(x)}) = 1$ and $\deg(a_n(x)) = 0$. First, we assume that $\deg(\frac{a_{n-1}(x)}{a_n(x)}) = 1$ and $\deg(a_n(x)) = 0$. Thus, $n-1 \leq m \leq n$ and

$$f(x, y) = A_1(y + a_1x + c_1)^n + g(x),$$

where $A_1a_1 \neq 0$ and $g(x)$ denotes a polynomial of degree less than or equal to n. Now, $m = n-1$ gives $b_m(y) = b_{n-1}(y) = na_1^{n-1}(y + c_1) + c_2$, a contradiction to (iii). Thus, $b_m(y) = b_n(y)$ is a constant polynomial, $\deg(\frac{b_{m-1}(y)}{b_m(y)}) = 1$ and

$$f(x, y) = A_2(x + a_2y + c_2)^m + h(y),$$

where $A_2a_2 \neq 0$ and $h(y)$ denotes a polynomial of degree less than or equal to $n = m$. Therefore, there exist constants A_3, a_3, and c_3 such that

$$A_3(x + a_3y + c_3)^n + \sum_{i=0}^{n} r_ix^i = A_2(x + a_2y + c_2)^n + \sum_{i=0}^{n} s_iy^i, \tag{5}$$

where $g(x) = \sum_{i=0}^{n} r_ix^i$ and $h(y) = \sum_{i=0}^{n} s_iy^i$. Now we compare the coefficients of $x^{n-i}y^i$ in (5) to obtain

$$A_3\binom{n}{i}a_3^i = A_2\binom{n}{i}a_2^i$$

for $i = 1, \ldots, n-1$. Since $(n-1, q) = 1$, it follows that $A_2 = A_3$ and $a_2 = a_3$. Thus, comparing the coefficients of $x^{n-2}y$, $c_2 = c_3$. Therefore, $g(x) = h(y) = d$ for some constant *d*, and

$$f(x, y) = A(x + ay + c)^n + d$$

which has the form (b).

Now we assume that $\deg(\frac{a_{n-1}(x)}{a_n(x)}) = 0$. Then

$$f(x, y) = a_n(x)(y + \alpha)^n + g(x)$$

for some $\alpha \in F_q$. Therefore, $f(x, y-\alpha) = a_n(x)y^n + g(x)$, which is a polynomial already considered in Case 1. This completes Case 2 and the proof for $m \le n$. If $n < m$, then a similar argument will provide form (d).

The next example illustrates the necessity of the condition $(n-1, q) = 1$.

Example: For a in F_{81}, let $f(x, y)$ denote the polynomial

$$f(x,y) = 2x^4 + x^3y + xy^3 + y^4 + 2ax^3 + ay^3 + 2a^3x + a^3y.$$

Then

$$\begin{aligned} f(x,y) &= (x+y+a)^4 + x^4 + ax^3 + a^3x + 2a^4 \\ &= 2(x+2y+a)^4 + 2y^4 + a^4. \end{aligned}$$

Therefore, since $4|80$, $f(x, y)$ is a local minimal polynomial that is not in the list (a)–(e).

REFERENCES

1. M. Acosta-de-Orozco & J. Gomez-Calderon. "Polynomials with Minimal Value Set over Galois Rings." *International Journal of Mathematics and Mathematical Science* **14** (1991): 471-74.
2. L. Carlitz, D. J. Lewis, W. H. Mills, & E. G. Strauss. "Polynomials Over Finite Fields with Minimal Value Set." *Mathematika* **8** (1961):121-30.
3. J. Gomez-Calderon. "A Note on Polynomials with Minimal Value Set Over Finite Fields." *Mathematika* **35** (1988):144-48.
4. W. H. Mills. "Polynomials with Minimal Value Sets." *Pacific Journal of Mathematics* **14** (1964):225-41.
5. G. L. Mullen. "Local Permutation Polynomials Over Z_p." *The Fibonacci Quarterly* **18.2** (1980):104-08.
6. G. L. Mullen. "Local Permutation Polynomials in Three Variables Over Z_p." *The Fibonacci Quarterly* **18.3** (1980):208-14.

AMS Classification Numbers: 11T06, 12E10