Comm. Korean Math. Soc. 9 (1994), No. 3, pp. 539–545

LOCAL PERMUTATION POLYNOMIALS OVER FINITE FIELDS

JUNE BOK LEE* AND HYOUNG JUNE KO

Let $q = p^r$, where p is a prime. A polynomial $f(x) \in GF(q)[x]$ is called a *permutation polynomial* (PP) over $GF(q)$ if the numbers $f(a)$ where $a \in GF(q)$ are a permutation of the a's. In other words, the equation $f(x) = a$ has a unique solution in $GF(q)$ for each $a \in GF(q)$. More generally, $f(x_1, \ldots, x_n)$ is a PP in n variables if $f(x_1, \ldots, x_n) = \alpha$ has exactly q^{n-1} solutions in $GF(q)^n$ for each $\alpha \in GF(q)$. Mullen ([3], [4], [5]) has studied the concepts of *local permutation polynomials* (LPP's) over finite fields. A polynomial $f(x_1, x_2, \ldots, x_n) \in GF(q)[x_1, \ldots, x_n]$ is called a LPP if for each $i = 1, \ldots, n$, $f(a_1, \ldots, a_{i-1}, x_i, a_{i+1}, \ldots, a_n)$ is a PP in x_i for all $a_j \in GF(q)$, $j \neq i$. Mullen ([3], [4]) found a set of necessary and sufficient conditions on the coefficients of a polynomial f in two and three variables over $GF(q)$ in order that f be a LPP. As examples, there are 12 LPP's over $GF(3)$ in two indeterminates ; $f(x_1, x_2) = a_{10}x_1 + a_{01}x_2 + a_{00}$ where $a_{10} = 1$ or 2, $a_{01} = 1$ or 2, $a_{00} = 0,1$, or 2. There are 24 LPP's over $GF(3)$ of three indeterminates ; $f(x_1, x_2, x_3) = ax_1 + bx_2 + cx_3 + d$ where a, b and $c = 1$ or 2, $d = 0,1$, or 2.

A feedback shift register (FSR) is a physical device which generates sequences $x_0, x_1, \ldots$ satisfying a feedback equation $x_{t+n} = f(x_t, \ldots, x_{t+n-1})$ for $t = 0, 1, \ldots$. An FSR is *nonsingular* if the map $(x_0, \ldots, x_{n-1}) \rightarrow (x_1, \ldots, x_n)$ is bijective. We call it a *nonsingular feedback function* (NSFF). In [6], Mullen found a necessary and sufficient condition for nonsingularity of a feedback shift register of degree at most two over a finite field. In fact, he proved the following Theorem using the fact that $f(x_1, \ldots, x_n)$ is a NSFF over $GF(q)$ if and only if $g(x_1) = f(x_1, a_2, \ldots, a_n)$ is a PP of $GF(q)$ for all $a_2, \ldots, a_n \in GF(q)$, i.e., if and only if $g(x_1)$ is a 1-1 mapping from $GF(q)$ onto itself for all $a_2, \ldots, a_n \in GF(q)$.

Received May 16, 1994.

* This work was supported by Yonsei Academic Research Grant, 1993.

THEOREM 1. (1) *If q is odd and $n \geq 2$, then $f(x_1, \ldots, x_n)$ of degree at most two is an NSFF iff $f(x_1, \ldots, x_n) = cx_1 + f_0(x_2, \ldots, x_n)$ where $f_0(x_2, \ldots, x_n)$ is any polynomial in the variables $x_2, \ldots, x_n$ of degree at most two over $GF(q)$, $c \in GF(q)^*$.*

(2) *If q is even and $n \geq 2$, then $f(x_1, \ldots, x_n)$ of degree at most two is an NSFF iff $f(x_1, \ldots, x_n) = cx_1 + f_0(x_2, \ldots, x_n)$ or $f(x_1, \ldots, x_n) = cx_1^2 + f_0(x_2, \ldots, x_n)$ where $f_0(x_2, \ldots, x_n)$ is any polynomial in the variables $x_2, \ldots, x_n$ of degree at most two over $GF(q)$, $c \in GF(q)^*$.*

THEOREM 2. (1) *Every LPP in n variables is an n-stage NSFF over $GF(q)$.*

(2) *Every n-stage NSFF is a PP in n variables over $GF(q)$.*

Using the above two Theorems we have the following property of LPP:

PROPOSITION 3. (1) *If q is odd and $n \geq 2$ then $f(x_1, \ldots, x_n)$ of degree at most two is a LPP iff $f(x_1, \ldots, x_n) = c_1x_1 + c_2x_2 + \cdots + c_nx_n + c$ where $c_i \in GF(q)^*$, $c \in GF(q)$.*

(2) *If q is even and $n \geq 2$ then $f(x_1, \ldots, x_n)$ of degree at most two is a LPP iff $f(x_1, \ldots, x_n) = c_1f_1(x_1) + c_2f_2(x_2) + \cdots + c_nf_n(x_n) + c$ where $c_i \in GF(q)^*$, $c \in GF(q)$ and $f_i(x_i) = x_i$ or x_i^2 for $i = 1, \ldots, n$.*

Proof. (1) Sufficiency is clear. Suppose that $f(x_1, \ldots, x_n)$ of degree at most two is a LPP then $f(x_1, \ldots, x_n)$ is a NSFF. Hence, $f(x_1, \ldots, x_n) = c_1x_1 + f_0(x_2, \ldots, x_n)$ where $c_1 \in GF(q)^*$ and $f_0(x_2, \ldots, x_n)$ is a polynomial of degree at most two over $GF(q)$. Since $f(x_1, \ldots, x_n)$ is a LPP, $f_0(x_2, \ldots, x_n)$ is a LPP. Thus, by induction $f(x_1, \ldots, x_n) = c_1x_1 + c_2x_2 + \cdots c_nx_n + c$ where $c_i \in GF(q)^*$, $c \in GF(q)$.

(2) Sufficiency is clear. Suppose that $f(x_1, \ldots, x_n)$ of degree at most two is a LPP. Then $f(x_1, \ldots, x_n)$ is a NSFF. Hence, $f(x_1, \ldots, x_n) = c_1x_1 + f_0(x_2, \ldots, x_n)$ or $f(x_1, \ldots, x_n) = c_1x_1^2 + f_0(x_2, \ldots, x_n)$ where $c_1 \in GF(q)^*$ and $f_0(x_2, \ldots, x_n)$ is a polynomial of degree at most two over $GF(q)$. Since $f(x_1, \ldots, x_n)$ is a LPP, $f_0(x_2, \ldots, x_n)$ is a LPP. Thus, $f_0(x_2, \ldots, x_n) = c_2x_2 + f_1(x_3, \ldots, x_n)$ or $f_0(x_2, \ldots, x_n) = c_2x_2^2 + f_1(x_3, \ldots, x_n)$ where $c_2 \in GF(q)^*$ and $f_1(x_3, \ldots, x_n)$ is a polynomial of degree at most two over $GF(q)$. Thus, by induction $f(x_1, \ldots, x_n) = c_1f_1(x_1) + c_2f_2(x_2) + \cdots + c_nf_n(x_n) + c$ where $c_1 \in GF(q)^*$, $c \in GF(q)$, $f_i(x_i) = x_1$ or x_i^2 for $i = 1, \ldots, n$.

Now, one might ask if any LPP $f(x_1, \ldots, x_n)$ over $GF(q)$ has the following form:

$$f(x_1, \ldots, x_n) = f_1(x_1) + f_2(x_2) + \cdots + f_n(x_n) + c \tag{1}$$

where $f_i(x_i)$ is a PP for all $i = 1, \ldots, n$ and $c \in GF(q)$. Proposition 3 implies that every LPP being of degree at most two has the form (1). However, Proposition 3 cannot be applied to a LPP $f(x_1, \ldots, x_n)$ of degree more than two. For example, $(x + y)^3$ is clearly a LPP over $GF(5)$ but it is not of the form (1). Note that if $f(x_1, \ldots, x_n)$ is a LPP over $GF(q)$ then so is $af(x_1, \ldots, x_n) + b$ for all $a \neq 0, b \in GF(q)$. Thus, we may consider a LPP $f(x_1, \ldots, x_n)$ as a polynomial $f(x_1, \ldots, x_n)$ with $f(0, \ldots, 0) = 0$. So, we may assume that (1) has the following form:

$$f(x_1, \ldots, x_n) = f_1(x_1) + f_2(x_2) + \cdots + f_n(x_n) \tag{1'}$$

where $f_i(x_i)$ is a PP and $f_i(0) = 0$ for all $i = 1, \ldots, n$. In [5], Mullen has established some classes of LPP's. In that paper, he proved the following:

THEOREM 4. *Suppose $f_1(x)$ and $f_2(y)$ are PP's. Then $f(x, y)$ is a LPP if and only if $f(f_1(x), f_2(y))$ is a LPP.*

THEOREM 5. *Suppose $g(x)$ is a PP. Then $f(x, y)$ is a LPP if and only if $g(f(x, y))$ is a LPP.*

Note that these two Theorems could be extended to an arbitrary number of variables. Theorem 4 and Theorem 5 can be used to construct classes of LPP's. For example, if $f(x_1, \ldots, x_n)$ is a LPP of the form (1'), then $\{f_1(x_1) + f_2(x_2) + \cdots + f_n(x_n)\}^k$ is a LPP where $(k, q-1) = 1$. Also, we can find a polynomial $f(x_1, \ldots, x_n)$ such that it is a LPP over all finite extensions of $GF(q)$. Namely, we have

THEOREM 6. *A polynomial $f(x_1, \ldots, x_n)$ is a LPP of all finite extensions of $GF(q)$ if and only if it is of the form $f(x_1, \ldots, x_n) = a_1 x_1^{p^{h_1}} + a_2 x_2^{p^{h_2}} + \cdots + a_n x_n^{p^{h_n}} + b$ where $a_i \neq 0$ and h_i is a nonnegative integer for $i = 1, \ldots, n$.*

Proof. It is clear from Theorem 7.14 in Lidl and Niederreiter [2], that is, a polynomial $f \in GF(q)[x]$ is a PP of all finite extensions of $GF(q)$

if and only if it is of the form $f(x) = ax^{p^h} + b$, where $a \neq 0$, p is the characteristic of $GF(q)$, and h is a nonnegative integer.

Now, we consider an analogue of Theorem 4, namely, given the condition that $f(x,y), g(x,y)$ and $h(x,y)$ are LPP's, we ask whether or not $f(g(x,y), h(x,y))$ is also a LPP. It is not in general true that $f(g(x,y), h(x,y))$ is a LPP. For example, $f(x,y) = g(x,y) = h(x,y) = x + y^3$ is a LPP over $GF(5)$ but $f(g(x,y), h(x,y)) = (x + y^3) + (x + y^3)^3$ is not a LPP over $GF(5)$.

First, we determine that $f(g(x,y), h(x,y))$ is a LPP when $f(x,y)$, $g(x,y)$ and $h(x,y)$ are of degree at most two. In this case, we have already determined that $f(x,y), g(x,y)$ and $h(x,y)$ are of the form $(1')$ so that

$$f(x,y) = a_1x + b_1y \text{ or } a_1x^2 + b_1y^2 \text{ where } a_1, b_1 \in GF(q)^*,$$
$$g(x,y) = a_2x + b_2y \text{ or } a_2x^2 + b_2y^2 \text{ where } a_2, b_2 \in GF(q)^*,$$
$$f(x,y) = a_3x + b_3y \text{ or } a_3x^2 + b_3y^2 \text{ where } a_3, b_3 \in GF(q)^*.$$

If $f(x,y) = a_1x + b_1y$ then $g(x,y) = a_2x + b_2y, h(x,y) = a_3x + b_3y$ or $g(x,y) = a_2x^2 + b_2y^2, h(x,y) = a_3x^2 + b_3y^2$ where $a_1a_2 + b_1a_3 \not\equiv 0 \pmod q$, $a_1b_2 + b_1b_3 \not\equiv 0 \pmod q$ in order that $f(g(x,y), h(x,y))$ be a LPP.

If $f(x,y) = a_1x^2 + b_1y^2$ then $g(x,y) = a_2x + b_2y, h(x,y) = a_3x + b_3y$ where $a_1a_2 + b_1a_3 \not\equiv 0 \pmod q$, $a_1b_2 + b_1b_3 \not\equiv 0 \pmod q$ in order that $f(g(x,y), h(x,y))$ be a LPP(Note that $q \cong 0 \pmod 2$ in this case).

Next, consider the case assuming that $f(x,y), g(x,y)$ and $h(x,y)$ are of the form $(1')$. Then, we have

$$f(x,y) = f_1(x) + f_2(y) \text{ where } f_1(x) \text{ and } f_2(y) \text{ are } PP's,$$
$$g(x,y) = g_1(x) + g_2(y) \text{ where } g_1(x) \text{ and } g_2(y) \text{ are } PP's,$$
$$h(x,y) = h_1(x) + h_2(y) \text{ where } h_1(x) \text{ and } h_2(y) \text{ are } PP's,$$

so that

$$(2) \qquad f(g(x,y), h(x,y)) = f_1(g(x,y)) + f_2(h(x,y))$$
$$(3) \qquad = f_1(g_1(x) + g_2(y)) + f_2(h_1(x) + h_2(y)).$$

By Theorem 5, $f_1(g(x,y))$ and $f_2(h(x,y))$ are LPP's. The trivial case for $f(g(x,y),h(x,y))$ being a LPP is that if $f_2(h(x,y)) = \alpha f_1(g(x,y))$, $\alpha \in GF(q)^*$ and $1+\alpha \not\cong 0 (\mathrm{mod}\, q)$, then $f(g(x,y),h(x,y))$ is a LPP. For example, $x^k + y^k$ is a LPP over $GF(q)$ if $(k, q-1) = 1$. Take $g(x,y) = h(x,y)$ as any LPP. Then $f(g(x,y),h(x,y)) = 2(g(x,y))^k$ is a LPP over $GF(q)$ where q is odd.

Suppose that $f(x,y)$ is of degree at most two. Then, $f(x,y) = a_1x + b_1y$ or $a_2x^2 + b_2y^2$, where $a_1, a_2, b_1, b_2 \in GF(q)^*$. If $f(x,y) = a_1x + b_1y$, then

$$\begin{aligned} f(g(x,y),h(x,y)) &= a_1 g(x,y) + b_1 h(x,y) \\ &= a_1 g_1(x) + a_1 g_2(y) + b_1 h_1(x) + b_1 h_2(y) \\ &= [a_1 g_1(x) + b_1 h_1(x)] + [a_1 g_2(y) + b_1 h_2(y)]. \end{aligned}$$

If $f(x,y) = a_2x^2 + b_2y^2$, then

$$\begin{aligned} f(g(x,y),h(x,y)) &= a_2 g(x,y)^2 + b_2 h(x,y)^2 \\ &\cong a_2 g_1(x) + a_2 g_2(y) + b_2 h_1(x) + b_2 h_2(y) \\ &= [a_2 g_1(x) + b_2 h_1(x)] + [a_2 g_2(y) + b_2 h_2(y)] \end{aligned}$$

since $q \cong 0 (\mathrm{mod}\, 2)$ in this case. For either cases, we may let

$$f(g(x,y),h(x,y)) \cong \alpha g_1 \cdot h_1^{-1}(x) + x + \beta g_2 \cdot h_2^{-1}(y) + y$$

where $\alpha, \beta \in GF(q)^*$ and we replace x(resp. y) by the polynomial representing $h_1^{-1}(x)$(resp. $h_2^{-1}(y)$). Thus, $f(g(x,y),h(x,y))$ is a LPP if and only if $\alpha g_1 \cdot h_1^{-1}(x) + x$ and $\beta g_2 \cdot h_2^{-1}(y) + y$ are PP's. In other words, $f(g(x,y),h(x,y))$ is a LPP if and only if $\alpha g_1 \cdot h_1^{-1}(x)$ and $\beta g_2 \cdot h_2^{-1}(y)$ are complete mapping polynomials over $GF(q)$. Recall that $f(x) \in GF(q)[x]$ is *a complete mapping polynomial* (CMP) of $GF(q)$ if both $f(x)$ and $f(x) + x$ are PP's of $GF(q)$. For example, $g(x,y) = x^3 - ay$ where a is not a square in $GF(q)$, $q \cong 0 (\mathrm{mod}\, 3)$, and $h(x,y) = -ax + y^3$. Then, clearly $g(x,y)$ and $h(x,y)$ are LPP's and $f(g(x,y),h(x,y)) = (x^3 - ay) + (-ax + y^3) = (x^3 - ax) + (y^3 - ay)$ is a LPP.

This idea can be extended to $f(x,y)$ being of degree more than two. Then, from (3) we have

$$f(g(x,y),h(x,y)) = f_1(g_1(x) + g_2(y)) + f_2(h_1(x) + h_2(y)).$$

In order that $f(g(x,y),h(x,y))$ be a LPP, $f_1(g_1(x)+g_2(\beta))+f_2(h_1(x)+h_2(\beta))$ and $f_1(g_1(\alpha)+g_2(y))+f_2(h_1(\alpha)+h_2(y))$ must be PP's for any $\alpha,\beta \in GF(q)$. In particular, $f_1(g_1(x))+f_2(h_1(x))$ and $f_1(g_2(y))+f_2(h_2(y))$ must be PP's. Since $f_2(h_1(x))$ and $f_2(h_2(y))$ are PP's if we replace x (resp. y) by the polynomial representing $(f_2 \cdot h_1)^{-1}(x)$(resp. $(f_2 \cdot h_2)^{-1}(y)$), we have

$$\begin{aligned} f_1(g_1(x))+f_2(h_1(x)) &= (f_1 \cdot g_1)(f_2 \cdot h_1)^{-1}(x)+x \\ &= k_1(x)+x \text{ where } k_1(x) \text{ is a PP}, \\ f_1(g_2(y))+f_2(h_2(y)) &= (f_1 \cdot g_2)(f_2 \cdot h_2)^{-1}(y)+y \\ &= k_2(y)+y \text{ where } k_2(y) \text{ is a PP}. \end{aligned}$$

Thus, in order that $f(g(x,y),h(x,y))$ is a LPP, $k_1(x)$ and $k_2(y)$ are CMP's of $GF(q)$ and we have the following result which is immediate from Theorem 1 in Cohen [1]. Namely, if $f(x)$ is a polynomial with integral coefficients and degree $n \geq 2$ then, for any prime $p > (n^2-3n+4)^2$ for which $f(x)$ is a PP of degree n of $GF(p)$, there is no integer c with $1 \leq c < p$ for which $f(x)+cx$ is also a PP of $GF(p)$.

THEOREM 7. *Let* $\deg k_1(x) = n_1 \geq 2$, $\deg k_2(y) = n_2 \geq 2$ *and* $n = \min(n_1, n_2)$. *Then for any prime* $p > (n^2-3n+4)^2$, $f(g(x,y),h(x,y))$ *is not a LPP of* $GF(p)$.

Note that if $p \nmid |n_1$ or $p \nmid |n_2$, then this can be extended to general finite field $GF(q)$. If $f(x,y)$ is of the form $(1')$, then the condition that $f(g(x,y),h(x,y))$ is a LPP depends on the PP's (such as $k_1(x)$ and $k_2(y)$ above) determined by $f(g(x,y),h(x,y))$. By the above discussion it seems difficult to find a necessary and sufficient condition that $f(g(x,y),h(x,y))$ is a LPP generally. However, when $h(x,y) = bg(x,y)$ we have the following result:

THEOREM 8. *If* $f(x,y)$, $g(x,y)$ *and* $h(x,y)$ *(not necessarily of the form* $(1')$*) are polynomials in 2 variables and* $h(x,y) = bg(x,y)$ *where* $b \in GF(q)^*$, *then* $f(g(x,y),h(x,y))$ *is a LPP over* $GF(q)$ *if and only if* $f(x,bx)$ *is a PP over* $GF(q)$.

Proof. Let $f(x,y) = \Sigma_{j=0}^{k}\Sigma_{i=0}^{m} a_{ij}x^iy^j$, where $a_{ij} \in GF(q)$. Then we

have

$$f(g(x,y),h(x,y)) = \Sigma_{j=0}^{k}\Sigma_{i=0}^{m}a_{ij}g(x,y)^i(bg(x,y))^j$$
$$= \Sigma_{j=0}^{k}\Sigma_{i=0}^{m}a_{ij}b^j g(x,y)^{i+j}.$$

On the other hand, $f(x,bx) = \Sigma_{j=0}^{k}\Sigma_{i=0}^{m}a_{ij}b^j x^{i+j}$ (say $= \overline{f}(x)$). Hence, we have $f(g(x,y),h(x,y)) = \overline{f}(g(x,y))$. If $\overline{f}(x)$ is a PP then $\overline{f}(g(x,y)) = f(g(x,y),h(x,y))$ is a LPP by Theorem 5. Conversely, $\overline{f}(g(x,y))$ is a LPP then $\overline{f}(g(x,\alpha))$ is a PP for any $\alpha \in GF(q)$ and $g(x,\alpha)$ is a PP. Thus, $\overline{f}(x)$ is a PP.

Using Theorem 5, we could construct classes of LPP's such as $f(x,y) = k_f(\overline{f}(x,y))$, $g(x,y) = k_g(\overline{g}(x,y))$ and $h(x,y) = k_h(\overline{h}(x,y))$ where k_f, k_g and k_h are PP's, and $\overline{f}(x,y)$, $\overline{g}(x,y)$, and $\overline{h}(x,y)$ are of the form (1'). The above relationship between the LPP of $f(g(x,y),h(x,y))$ and CMP's can be extended to this construction of LPP's.

We conclude this paper with the following Problem:

PROBLEM. Does there exist a LPP $f(x,y)$ which can not be obtained from the form (1') and the construction of LPP's by Theorem 4 and 5?

References

1. S. D. Cohen, *Proof of a conjecture of Chowla and Zassenhaus on Permutation Polynomials*, Canad. Math. Bull. **33** (1990), 230–234.
2. R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and Applications, **20** Addison-Wesley Reading, MA: 1983.
3. G. L. Mullen, *Local Permutation Polynomials over* $\mathbf{Z}_p$, Fibonacci Quart **18** (1980), 104–108.
4. ———, *Local Permutation Polynomials in three variables over* $\mathbf{Z}_p$, Fibonacci Quart **18** (1980), 208–214.
5. ———, *Local Permutation Polynomials over a Finite Field*, Norske. Vid. Selsk. Skrifter **1** (1981), 1–4.
6. ———, *Permutation Polynomials and Nonsingular Feedback Shift Registers over Finite Fields*, IEEE Trans. Infor. Th. **35** (1989), 900–902.
7. Herald Niederreiter and Karl H. Robinson, *Complete mappings of finite fields*, J. Austral. Math. Soc. Series A **33** (1982), 197–212.

Department of Mathematics
Yonsei University
Seoul 120-749, Korea