TAIWANESE JOURNAL OF MATHEMATICS
Vol. 13, No. 5, pp. 1371-1377, October 2009
This paper is available online at http://www.tjm.nsysu.edu.tw/

ENUMERATING LOCAL PERMUTATION POLYNOMIALS OVER RESIDUE CLASS RINGS

Jiangmin Pan and Caiheng Li

Abstract. Diestelkamp, Hartke and Kenney recently studied local permutation polynomials over finite field F_s and proved that $2s-4$ is the sharp bound of their degrees when $s>3$. In this paper, we focus on local permutation polynomials over residue class rings. We prove two specific formulas computing the number and the sharp bound of degrees of local permutation polynomials modulo p^n respectively.

1. INTRODUCTION

Let R be a finite ring, and $R[x]$ be the polynomial ring with one variable over R. A polynomial $f(x)$ in $R[x]$ is called a *permutation polynomial* (PP for short) over R if $f(x)$ permutes R, that is, the induced map $a \longrightarrow f(a)$ from R to itself is a bijective. Let x, y be two commutative indeterminates, and $R[x,y]$ be the polynomial ring with two variables over R. A polynomial $f(x,y)$ in $R[x,y]$ is called a *local permutation polynomial* (LPP for short) if for any $a \in R$, $f(a,y)$ and $f(x,a)$ are permutation polynomials over R. In a special case: $R = Z_m$ is the residue class ring modulo m, PP and LPP over R are also called PP and LPP modulo m, respectively. For background material on PP and LPP, we refer to [1].

PP and LPP over finite fields and residue class rings have many nice properties (see, for example, [1]) and have important applications both in cryptography (see, for examples [2, 3]) and in Latin square which first initiated by Euler (see, for example, [4, 5].)

Recently, Diestelkamp, Hartke and Kenney studied LPP over finite field F_s, they proved that $2s-4$ is the sharp bound of their degrees in the case $s>3$, see [6]. It

Received September 17, 2006, accepted June 18, 2007.
Communicated by Wen-Fong Ke.
2000 *Mathematics Subject Classification*: 13M10, 12Y05.
Key words and phrases: Permutation polynomial, Local permutation polynomial, Residue class ring, Sharp bound.
Partially supported by a NNSF of China and an ARC Discovery Grant Project.

is natural to ask how is sharp bound of LPP over residue class rings? We focus on this subject in this paper. We prove two specific formulas computing the number of LPP modulo p^n and the sharp bound of degrees of LPP modulo p^n, respectively.

We now fix some notations which will be used throughout the paper. Let R be the residue class ring modular p^n with p a prime. Let R_n denote the ring of all polynomial functions in two commutative indeterminates x, y over Z_{p^n} and let r_n denote its cardinality. If $f(x,y) \in Z[x,y]$, it can induce a polynomial function in R_n in the natural way. It is an easy observation that every polynomial function in R_n can be obtained in this way. For the simplicity to express, when we use the notation $f(x,y)$, we will not mention whether it is being considered as a polynomial of $Z[x,y]$ or a function of R_n unless the context is ambiguous.

For nonnegative integer m, let $\pi(m)$ be the largest integer s such that $p^s \mid m!$, that is, $\pi(m)$ is the exponent of p in the standard decomposition of $m!$. It is known that $\pi(m) = \sum_{i=1}^{\infty}[\frac{m}{p^i}]$. Let ω_n be the cardinality of set $\{(i,j) \mid \pi(i)+\pi(j) \leq n-1\}$. For positive integer k, let $x^{[k]} = x(x-1)\cdots(x-k+1)$ and $x^{[0]} = 1$. Then it is easy to see that $k! \mid x^{[k]}$ and $p^{\pi(k)} \mid x^{[k]}$ for any integer x.

The main results we obtained in this paper are the following two theorems. The first presents the number of LPP modular p^n.

Theorem 1.1. *Let l_n denote the number of LPP modulo p^n. Then*

(*i*) $l_2 = p^{p^2}(p-1)^{2p^2}l_1$;

(*ii*) *if* $n > 2$, $l_n = p^{\omega_n}l_{n-1}$.

The second theorem gives rise to the sharp bound of degrees of LPP modular p^n.

Theorem 1.2. *Let d_n denote the sharp bound of degrees of LPP modulo p^n. Then*

(*i*) *if* $p = 2$ *or* 3, $d_1 = 1$;

(*ii*) *if* $p > 3$, $d_1 = 2p-4$;

(*iii*) *if* $2 \leq n \leq p$, $d_n = (n+1)p-2$.

Generally, $d_n = max\{i+j \mid \pi(i)+\pi(j) = n-1\}$ *for each* $n \geq 2$.

2. Proofs of the Main Theorems

In this section, we first collect some necessary preliminaries and propositions, and then prove Theorems 1.1 and 1.2.

The following two propositions play crucial roles in the study of LPP modulo p^n. More precisely, they reduce our consideration on LPP modulo p^n to LPP modulo p^2.

Proposition 2.1. [7]. *Let $f(x) \in Z[x]$ and $n \geq 2$. Then $f(x)$ is a PP modulo p^n if and only if $f(x)$ is a PP modulo p and $f'(a) \not\equiv 0$(mod p) for each $a \in Z$.*

Proposition 2.2. [8] or [9]. *Let $n > 2$. Then $f(x)$ is a PP modulo p^n if and only if $f(x)$ is a PP modulo p^2. Similarly, $f(x, y)$ is a LPP modulo p^n if and only if $f(x, y)$ is a LPP modulo p^2.*

The sharp bound of degrees of LPP over finite fields is already known.

Proposition 2.3. [4]. *Let $f(x, y)$ be a LPP modulo p. If $p = 2$ or 3, then $deg(f(x, y)) = 1$.*

Proposition 2.4. [6]. *Let F_s be s elements field with $s > 3$. Then the sharp bound of degrees of LPP over finite field F_s is $2s - 4$.*

Now, we prove several technical lemmas which play important roles in the proofs of Theorem 1.1 and Theorem 1.2.

Lemma 2.5. *Let $f(x, y) \in R_n$. Then $f(x, y)$ can be uniquely expressed by*

$$f(x, y) = \sum_{k+\pi(i)+\pi(j)<n} a_{ijk} p^k x^{[i]} y^{[j]} \tag{1}$$

with $0 \leq a_{ijk} \leq p - 1$ for $i, j, k \geq 0$.

Proof. First, note that the leading monomial of $cx^{[i]}y^{[j]}$ with $c \neq 0$ is $cx^i y^j$, it follows that $f(x, y)$ can be written in the form $f(x, y) = \sum_{i,j} b_{ij} x^{[i]} y^{[j]}$. Without lose of generality, we can suppose that each $b_{ij} \geq 0$ since if there is some $b_{ij} < 0$, it can be substituted by some suitable $b'_{ij} = p^n q_{ij} + b_{ij} \geq 0$ keeping $f(x, y)$ invariant.

Write $b_{ij} = \sum_k a_{ijk} p^k$ with $0 \leq a_{ijk} \leq p - 1$. If $k + \pi(i) + \pi(j) \geq n$, then $p^k x^{[i]} y^{[j]} \equiv 0(mod\, p^n)$. Therefore, $f(x, y)$ can be written in the form (1).

To prove the uniqueness of the representation, it suffices to prove that if

$$g(x, y) = \sum_{k+\pi(i)+\pi(j)<n} c_{ijk} p^k x^{[i]} y^{[j]} \equiv 0(mod\, p^n) \quad (|c_{ijk}| < p)$$

for any integers x and y, then each $c_{ijk} = 0$.

Write $d_i(y) = \sum_{k+\pi(j)<n-\pi(i)} c_{ijk} p^k y^{[j]}$. Then $g(x, y) = \sum_{\pi(i)<n} d_i(y) x^{[i]}$. We now prove

$$d_i(y) \equiv 0(mod\, p^{n-\pi(i)}) \quad (\pi(i) < n) \tag{2}$$

by using induction on i.

For $i = 0$, $d_0(y) = g(0, y) \equiv 0(mod\, p^n)$. Now, $d_i(y)i^{[i]} \equiv g(i, y) \equiv 0(mod\, p^n)$ since $d_t(y) \equiv 0(mod\, p^{n-\pi(t)})$ for $t < i$ by induction hypothesis (it implies $d_t(y)i^{[i]} \equiv 0(mod\, p^n)$) and $i^{[t]} = 0$ for $t > i$. So (2) follows.

Further, let $d_{ij} = \sum_{k<n-\pi(i)-\pi(j)} c_{ijk}p^k$, it is easily to prove that each $d_{ij} \equiv 0(mod\, p^{n-\pi(i)-\pi(j)})$ by similar discussion as above. However, since $|c_{ijk}| < p$, $|d_{ij}| < p^{n-\pi(i)-\pi(j)}$, so $d_{ij} = 0$, and then each $c_{ijk} = 0$. This completes the proof of the Lemma 2.5. ■

Lemma 2.6. *Let φ_n be the natural homomorphism from R_n onto R_{n-1} with $n \geq 2$. Then*

(*i*) $Ker(\varphi_n) = \left\{ \sum_{k+\pi(i)+\pi(j)=n-1} a_{ijk}p^k x^{[i]}y^{[j]} \mid i, j, k \geq 0, 0 \leq a_{ijk} \leq p-1 \right\}$.

(*ii*) $|Ker(\varphi_n)| = p^{\omega_n}$.

Proof. By Lemma 2.5, every polynomial function in R_n can be expressed uniquely in form (1). Then

$$\varphi_n \left(\sum_{k+\pi(i)+\pi(j)<n} a_{ijk}x^{[i]}y^{[j]} \right) = \sum_{k+\pi(i)+\pi(j)<n-1} a_{ijk}x^{[i]}y^{[j]} = 0$$

if and only if $a_{ijk} = 0$ when $k + \pi(i) + \pi(j) < n - 1$ by the uniqueness of the representation. So (i) follows.

For each pair (i, j) satisfying $\pi(i) + \pi(j) \leq n - 1$, there exists exactly one k such that $k+\pi(i)+\pi(j) = n-1$, thus $|Ker(\varphi_n)| = p^{\omega_n}$ as every a_{ijk} has exactly p choices. Lemmas 2.5 and 2.6 have the following corollary which determines the number of polynomial functions in two commutative indeterminates over the residue class ring modulo p^n. ■

Corollary 2.7. *Assume $n \geq 2$. Then*

(*i*) $|r_1| = p^{p^2}$, $|r_2| = p^{4p^2}$.

(*ii*) $|r_n| = p^{\omega_n}|r_{n-1}| = p^{4p^2}p^{\sum_{k=3}^{n}\omega_n}$.

Proof. By Lemma 2.5, we immediately have $|r_1| = p^{p^2}$. Note $\omega_2 = |\{(i, j) \mid \pi(i) + \pi(j) \leq 1\}| = 3p^2$, then the rest sesults are direct consequences of Lemma 2.6. ■

Lemma 2.8. *The number of polynomial $f(x)$ in $Z_p[x]$ satisfying $f(a) \not\equiv 0(modp)$ for each $a \in Z$ is $(p-1)^p$.*

Proof. We may assume that $f(x) \equiv \sum_{i=0}^{p-1} a_i x^{[i]} (mod\, p)$ $(0 \le a_i \le p-1)$ since $x^{[t]} \equiv 0 (mod\, p)$ when $t \ge p$. First, $a_0 \equiv f(0) \not\equiv 0 (mod\, p)$, a_0 has $p-1$ choices. When $a_0, a_1, \cdots, a_{k-1}$ $(0 \le (k-1) < p-1)$ are chosen, we have $f(k) \equiv a_0 + ka_1 + \cdots + k!a_{k-1} + k!a_k \not\equiv 0 (mod p)$, a_k also has exactly $p-1$ choices as $(k!, p) = 1$. The lemma follows. ■

We can now prove Theorems 1.1.

Proof of Theorem 1.3. By Lemma 2.6 and Corollary 2.7, the first result is obviously true.

Let $f(x, y)$ be a LPP modulo p^2. By Lemma 2.5, $f(x, y)$ can be uniquely expressed in the form $f(x, y) = g_1(x, y) + g_2(x, y) + g_3(x, y) + pg_4(x, y)$, where

$$g_1(x,y) = \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} a_{ij0} x^{[i]} y^{[j]}, \quad g_2(x,y) = \sum_{i=p}^{2p-1}\sum_{j=0}^{p-1} a_{ij0} x^{[i]} y^{[j]}$$

$$g_3(x,y) = \sum_{i=0}^{p-1}\sum_{j=p}^{2p-1} a_{ij0} x^{[i]} y^{[j]}, \quad g_4(x,y) = \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} a_{ij1} x^{[i]} y^{[j]}$$

with $0 \le a_{ij0}, a_{ij1} \le p-1$.

Obviously, $f(x, y) \equiv g_1(x, y) (mod\, p)$. Now, since

$$\begin{aligned}\frac{\partial g_2}{\partial x} &= (x^{[p]})'_x \cdot \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} a_{(p+i)j0} (x-p)^{[i]} y^{[j]} \\ &\quad + x^{[p]} \cdot (\sum_{i=p}^{p-1}\sum_{j=0}^{p-1} a_{(p+i)j0} (x-p)^{[i]} y^{[j]})'_x \\ &\equiv (x^{[p]})'_x \cdot \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} a_{(p+i)j0} x^{[i]} y^{[j]} (mod\, p),\end{aligned}$$

by Wilson's theorem, we have $(x^{[p]})'_x \equiv -1 (mod\, p)$, so

$$\frac{\partial g_2}{\partial x} \equiv -\sum_{i=0}^{p-1}\sum_{j=0}^{p-1} a_{(p+i)j0} x^{[i]} y^{[j]} (mod\, p).$$

Moreover, since $y^{[j]} \equiv 0 (mod\, p)$ when $p \le j \le 2p-1$, we have $\frac{\partial g_3}{\partial x} \equiv 0 (mod\, p)$. Hence

$$\frac{\partial f}{\partial x} \equiv \frac{\partial g_1}{\partial x} - \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} a_{(p+i)j0} x^{[i]} y^{[j]} (mod\, p).$$

Similarly, we have

$$\frac{\partial f}{\partial y} \equiv \frac{\partial g_1}{\partial y} - \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} a_{i(p+j)0}x^{[i]}y^{[j]}(mod\ p).$$

Further, by Proposition 2.1, $f(x,y)$ is a LPP modulo p^2 if and only if $g_1(x,y)$ is a LPP modulo p, and both

$$\frac{\partial g_1}{\partial x} - \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} a_{(p+i)j0}x^{[i]}y^{[j]} \equiv 0(mod\ p) \tag{3}$$

and

$$\frac{\partial g_1}{\partial y} - \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} a_{i(p+j)0}x^{[i]}y^{[j]} \equiv 0(mod\ p) \tag{4}$$

have no integer solution.

Write

$$\sum_{i=0}^{p-1}\sum_{j=0}^{p-1} a_{(p+i)j0}x^{[i]}y^{[j]} = \sum_{i=0}^{p-1} h_i(y)x^{[i]}$$

where $h_i(y) = \sum_{j=0}^{p-1} a_{(p+i)j0}y^{[j]}$ with $0 \le i \le p-1$.

For each choice of $g_1(x,y)$ (note that $g_1(x,y)$ exists since linear form $ax + by + c$ $(p \nmid a, p \nmid b)$ are LPP modulo p), using similar discussion as Lemma 2.8, it follows that each $h_i(y)$ has exactly $(p-1)^p$ choices, that is, $g_2(x,y)$ has $(p-1)^{p^2}$ choices such that (3) has no solutions.

Similarly, $g_3(x,y)$ has $(p-1)^{p^2}$ choices such that (4) has no solutions. Moreover, $g_4(x,y)$ obviously has p^{p^2} choices.

Summarizing the above observations, the second result of the theorem follows. ■

Finally, we give the proof of Theorem 1.2.

Proof of Theorem 1.4. (i), (ii) are obvious true by Proposition 2.3 and 2.4. we now prove the final result of The theorem.

First, by Lemma 2.5, we easily have $d_n \le max\{i+j \mid \pi(i)+\pi(j) = n-1\}$.

Conversely, for $n > 2$, choose $\sum_{k+\pi(i)+\pi(j)<2} a_{ijk}x^{[i]}y^{[j]}$ a LPP modulo p^2, by Proposition 2.2, for freely choices of a_{ijk} when $k + \pi(i) + \pi(j) \ge 2$, the resulting polynomial function $\sum_{k+\pi(i)+\pi(j)<n} a_{ijk}x^{[i]}y^{[j]}$ is a LPP modulo p^n. So we only need to choose $a_{ij0} = 1$ when $i+j$ equals the maximal number of set $\{i+j \mid \pi(i)+\pi(j) = n-1\}$, the resulting polynomial is a LPP modulo p^n with the degree exactly equals $max\{i+j \mid \pi(i)+\pi(j) = n-1\}$. Hence $d_n = max\{i+j \mid \pi(i)+\pi(j) = n-1\}$, that is, the final result is true.

For $n = 2$, it is not difficult to prove directly $d_2 = 3p - 2$ as in the proof of Theorem 1.1.

Finally, (iii) is a direct consequence of the final result as $max\{i + j \mid \pi(i) + \pi(j) = n - 1\} = (n + 1)p - 2$ when $2 \leq n \leq p$. ■

Remark 2.9. The results we obtained above can be generalized for any positive modulo m. Since if $m = p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}$ is the standard decomposition, then $f(x, y)$ is a PP (or LPP) modulo m if and only if $f(x, y)$ is a PP (or LPP) modulo $p_i^{r_i}$ for $i = 1, 2, \cdots, t$.

References

1. R. Lidl and H. Niederreiter, Finite fields, *Encyclopedia of Mathematics and its Applications*, Vol. 20, Addision-Wesley, Reading, MA, 1983.
2. R. Lidl and W. B. Mullen, Permutation polynomial in RSA-cryptosystems, in: *Proc. CRYPTO 83*, Plenum, New York, 1984.
3. R. L. Rivest, A. Shamir and L. M. Adleman, A method for obtaining digital signatures and public-key crytosystems, *Comm. ACM 21*, **2** (1978), 120-126.
4. G. L. Mullen, Local permutation polynomials over Z_p, *Fibonacci Quart.*, **18** (1980), 104-108.
5. W. S. Diestelkamp, The decomposability of simple orthogonal arrays on 3 symbols having t+1 rows and strength t, *J. Combin.*, **8** (2000), 442-458.
6. W. S. Diestlkamp, S. G. Hartke and R. H. Kenney, On the degree of local permutation polynomials, *Jour. Combin. Math. Comput.*, **50** (2004), 129-140.
7. G. H. Hardy and E. M. Wright, An introduction to the theory of numbers, Oxford, 1960.
8. Q. Zhang, Polynomial functions and permutation polynomials over some finite commutative rings, *Journal of Number Theory*, **105** (2004), 192-202.
9. J. Pan, Polynomials over finite fields with a given value set, *Comm. Algebra*, to appear.

Jiangmin Pan
Department of Mathematics,
Yunnan University,
Kunming 650091, P. R. China
E-mail: jmpan@ynu.edu.cn

Caiheng Li
School of Mathematics and Statistics,
University of Western Australia,
Australia
E-mail: li@maths.uwa.edu.au