On the degree of local permutation polynomials*

Wiebke S. Diestelkamp
Department of Mathematics
University of Dayton
Dayton, OH 45469-2316
wiebke@udayton.edu

Stephen G. Hartke†
Department of Mathematics
Rutgers University
Hill Center - Busch Campus
110 Frelinghuysen Road
Piscataway, NJ 08854-8019
hartke@math.rutgers.edu

Rachael H. Kenney
Department of Mathematics
North Carolina State University
Box 8205
Raleigh, NC 27695-0001
rhkenney@unity.ncsu.edu

Abstract

Every Latin square of prime or prime power order s corresponds to a polynomial in 2 variables over the finite field on s elements, called the local permutation polynomial. What characterizes this polynomial is that its restrictions to one variable are permutations. We discuss the general form of local permutation polynomials and prove that their total degree is at most $2s-4$, and that this bound is sharp. We also show that the degree of the local permutation polynomial for Latin squares having a particular form is at most $s-2$. This implies that circulant Latin squares of prime order p correspond to local permutation polynomials having degree at most $p-2$. Finally, we discuss a special case of circulant Latin squares whose local permutation polynomial is linear in both variables.

*Journal of Combinatorial Mathematics and Combinatorial Computing, Vol. 50 (2004), 129-140
†Supported by a National Defense Science and Engineering Graduate Fellowship.

1 Introduction

Every Latin square can be represented by a function of two variables. In this paper we focus on Latin squares of prime and prime power order. Latin squares of order two and three have already been examined by Mullen [5] and Diestelkamp [2], both of whom found that any Latin square of order 3 can be fit to a unique polynomial $f(x, y)$ that is linear in x and y.

We provide a construction formula for the local permutation polynomials of Latin squares of prime and prime power order s. We also prove that the degree of these polynomials is at most $2s - 4$. We provide explicit examples to illustrate that there exist Latin squares of every order $s > 3$ for which this bound is attained. We show that circulant Latin squares of prime order p correspond to local permutation polynomials of degree at most $p - 2$ and provide examples where this degree is attained. Further, we show that circulant Latin squares whose first row has a specific form correspond to linear local permutation polynomials.

Throughout the paper, p is a prime, and if $s = p^n$ for some positive integer n, then $\mathbb{F}_s$ denotes the finite field with s elements. When $s = p$, we use $\mathbb{F}_p = \mathbb{Z}_p$, the field of integers modulo p. The set of nonzero elements of $\mathbb{F}_s$ is denoted by $\mathbb{F}_s^*$. The characteristic of a finite field F is denoted by $\mathrm{char}(F)$.

We use the usual definition for the degree of a polynomial in two variables: The degree of a nonzero monomial in two variables $ax^{k_1}y^{k_2}$ is k_1+k_2. The degree of $f(x, y) = \sum_{j=0}^{m}\sum_{i=0}^{m} a_{ij}x^iy^j$ is the maximum of the degrees of $a_{ij}x^iy^j$ such that $a_{ij} \neq 0$.

2 Representation of Latin squares by functions

Definition 2.1. *A Latin square of order s is an $s \times s$ matrix L with entries from a set S of size s such that each element of S occurs exactly once in every row and every column of L.*

By indexing the cells of L by $S \times S$, we have the following:

Lemma 2.2. *An $s \times s$ matrix L with entries a_{ij} is a Latin square if and only if there exists a function $f : S \times S \to S$ such that $f(i, j) = a_{ij}$ $\forall i, j \in S$. Moreover,*

(i) $x, y, z \in S$ *and* $y \neq z \Rightarrow f(x, y) \neq f(x, z)$,

(ii) $x, y, z \in S$ *and* $x \neq z \Rightarrow f(x, y) \neq f(z, y)$.

Example 2.3. *Let $S = \{0, 1, 2, 3\}$. The following is a Latin square of order 4 on S: (Note that S is an arbitrary 4-element set.)*

$$\begin{bmatrix} 0 & 2 & 1 & 3 \\ 3 & 0 & 2 & 1 \\ 2 & 1 & 3 & 0 \\ 1 & 3 & 0 & 2 \end{bmatrix}$$

Here, $f(0,0) = 0, f(0,1) = 2, f(1,3) = 1$ *etc.*

The definition of a Latin square does not impose a structure on the set S.

For the remainder of this paper, we consider only Latin squares of prime or prime power order. The underlying set S is chosen to be $\mathbb{F}_s$ or $\mathbb{Z}_p$. This allows us to exploit the algebraic properties of finite fields to study these functions.

Consider the following well-known result from the theory of finite fields (see, for example, [1] or [4]):

Theorem 2.4. *If* $f : (\mathbb{F}_s)^n \to \mathbb{F}_s$*, then* f *is a polynomial in* n *variables. If we mandate that no exponent is greater than* $s-1$*, then the polynomial* f *is unique.*

Theorem 2.4 implies that any function $f : \mathbb{F}_s \times \mathbb{F}_s \to \mathbb{F}_s$ can be expressed as a polynomial in two variables of the form

$$f(x,y) = \sum_{j=0}^{s-1} \sum_{i=0}^{s-1} a_{ij} x^i y^j. \tag{1}$$

Throughout this paper, we identify all functions $f : (\mathbb{F}_s)^n \to \mathbb{F}_s$ with polynomials for which every exponent is less than s.

3 Permutations of $\mathbb{F}_s$

In this section, we discuss results regarding permutations of $\mathbb{F}_s$ that are needed later on. Recall that a permutation of $\mathbb{F}_s$ is a bijection of $\mathbb{F}_s$. The polynomial corresponding to a permutation is called a *permutation polynomial*.

Proposition 3.1. *If* $d > 1$ *is a divisor of* $s-1$*, then there exists no permutation polynomial of* $\mathbb{F}_s$ *of degree* d*.*

The proof of Proposition 3.1 is given in [4, p. 349].

Now, let $g : \mathbb{F}_s \to \mathbb{F}_s$ be a permutation. By Propositions 2.4 and 3.1, g is a polynomial in one variable and has degree at most $s-2$. We will now provide an explicit construction of g.

Define

$$h_\alpha(x) = \prod_{\substack{\gamma \in \mathbb{F}_s \\ \gamma \neq \alpha}} (x - \gamma). \tag{2}$$

Then set

$$f(x) = \sum_{\alpha \in \mathbb{F}_s} \big(-g(\alpha)\big) h_\alpha(x). \tag{3}$$

This is essentially Lagrange's Interpolation Formula (cf. [4]).

Lemma 3.2. *Let* $f : \mathbb{F}_s \to \mathbb{F}_s$ *be defined as in (3). Then* $f(x) = g(x)$ *for all* $x \in \mathbb{F}_s$*.*

Proof. By Lemma 4.5 below,

$$h_\alpha(x) = \begin{cases} 0, & \text{if } x \neq \alpha, \\ -1, & \text{if } x = \alpha. \end{cases}$$

Thus,

$$f(\alpha) = \big(-g(\alpha)\big)(-1) = g(\alpha).$$

□

Now, by Lemma 3.1, the degree of f is at most $s-2$. In fact, this upper bound on the degree of a permutation is sharp:

Proposition 3.3. *For $s \neq 2$, there exists a permutation of $\mathbb{F}_s$ whose degree is $s-2$.*

Proof. Since $x^{s-1} = 1$ for $x \neq 0$, x^{s-2} is a permutation of $\mathbb{F}_s$. □

4 Local permutation polynomials for Latin squares of prime and prime power order

Definition 4.1. (Mullen [6]) *A polynomial $f : \mathbb{F}_s \times \mathbb{F}_s \to \mathbb{F}_s$ that gives rise to a Latin square (i.e. satisfies the conditions of Lemma 2.2) is called a* local permutation polynomial *(or* LPP*).*

It is already known what kind of polynomials can arise as local permutation polynomials over $\mathbb{Z}_2$ and $\mathbb{Z}_3$:

Proposition 4.2. *Let $f : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$ be a local permutation polynomial. If $p = 2$ or $p = 3$, then f is linear.*

The proof can be found in [5] or [2].

Proposition 4.3. *Assume $s > 3$. Let $f : \mathbb{F}_s \times \mathbb{F}_s \to \mathbb{F}_s$ be a local permutation polynomial. Then the degree of f is at most $2s-4$.*

Proof. Let $a, b \in \mathbb{F}_s$. By definition of f as an LPP, the polynomials $f(\cdot, a)$ and $f(b, \cdot)$ are permutations of $\mathbb{F}_s$. By Proposition 3.1, these polynomials have degree at most $s-2$. Thus f has degree at most $2(s-2) = 2s-4$. □

Our main result is to prove that the bound on the degree of a local permutation polynomial given in Proposition 4.3 is sharp. We utilize the following:

Lemma 4.4. *Let G be a group (written multiplicatively) with identity 1. Then*

$$\prod_{g \in G} g = \begin{cases} a, & \textit{if } a \textit{ is the unique element of order } 2, \\ 1, & \textit{otherwise.} \end{cases}$$

Applying Lemma 4.4 to the additive and multiplicative groups of the field $\mathbb{F}_s$, we have

Lemma 4.5. *If $s > 2$, then $\sum_{g \in \mathbb{F}_s} g = 0$ and $\prod_{g \in \mathbb{F}_s^*} g = -1$.*

Proof. The second statement follows from the fact that the equation $x^2 - 1 = 0$ over $\mathbb{F}_s$ has only the two solutions ± 1 (note that $-1 = 1$ if $\mathrm{char}(\mathbb{F}_s) = 2$). □

Now, to show that the bound on the degree of an LPP over $\mathbb{F}_s$ given in Proposition 4.3 is the best possible, we use the following construction:

Let $g : \mathbb{F}_s \times \mathbb{F}_s \to \mathbb{F}_s$ be a local permutation polynomial over $\mathbb{F}_s$. Define $f_\beta(y)$ to be the polynomial representing the permutation in the β^{th} row. This means that $f_\beta(y) = g(\beta, y)$ as a function. Let h_α be defined as in (3). Then

$$f_\beta(y) = \sum_{\alpha \in \mathbb{F}_s} \big(-g(\beta, \alpha)\big) h_\alpha(y).$$

Let

$$f(x, y) = \sum_{\beta \in \mathbb{F}_s} -h_\beta(x) f_\beta(y). \tag{4}$$

Then we have

Lemma 4.6. *For all $y, x \in \mathbb{F}_s$, $f(x, y) = g(x, y)$.*

Proof.

$$f(\gamma, \delta) = -(-1) f_\gamma(\delta) = f_\gamma(\delta) = g(\gamma, \delta).$$

□

We are now ready to prove our main result.

Theorem 4.7. *If s is a prime power, and $s > 3$, then there exists a $s \times s$ Latin square whose local permutation polynomial has degree $2s - 4$.*

Proof. For $s = 4$, let ξ be a root of the irreducible polynomial $x^2 + x + 1$ over $\mathbb{F}_2$. Then $\mathbb{F}_4 = \mathbb{F}_2[\xi]$. The LPP for the Latin square

$$\begin{bmatrix} 0 & 1 & \xi & \xi+1 \\ 1 & 0 & \xi+1 & \xi \\ \xi & \xi+1 & 1 & 0 \\ \xi+1 & \xi & 0 & 1 \end{bmatrix},$$

where the rows and columns are indexed by $(0, 1, \xi, \xi + 1)$, is given by the function $x^2y^2 + x^2y + xy^2 + xy + x + y$. This polynomial has degree $2(4) - 4 = 4$ as desired.

For $s > 4$, let ϕ and π be permutations of $\mathbb{F}_s$ with $\phi(\alpha) \neq \pi(\alpha)$ for all $\alpha \in \mathbb{F}_s$. Denote the polynomials corresponding to ϕ and π by $f^\phi(x)$ and $f^\pi(x)$, respectively. Suppose

that $f^\phi(x)$ and $f^\pi(x)$ are of degree $s-2$ with different leading coefficients. (We show at the end of the proof that there always exist such permutations by providing explicit constructions for ϕ and π.) Construct a partial $s \times s$ Latin square M' with ϕ as the first row ($\beta = 0$) and π as the second row ($\beta = 1$). M' can be extended to a full Latin square M (see [3]). We claim that either the LPP of M has degree $2s-4$, or the Latin square $\widehat{M}$ formed by switching the two first rows of M has an LPP with degree $2s-4$.

Let $f(x,y)$ be the LPP for M and $\widehat{f}(x,y)$ the LPP for $\widehat{M}$. Then both f and $\widehat{f}$ can be written in the form given in (4). As we have already shown in the proof of Proposition 3.3, the coefficient of x^{s-2} in the polynomial $h_\beta(x)$ is $\sum_{\substack{\gamma \in \mathbb{F}_s \\ \gamma \neq \beta}} (-\gamma) = \beta$. Thus the coefficient of $y^{s-2}x^{s-2}$ in f is $\sum_{\beta \in \mathbb{F}_s} -\beta\ell_\beta$, where ℓ_β is the coefficient of y^{s-2} in $f_\beta(y)$. Now, if the coefficients of $y^{s-2}x^{s-2}$ for M and $\widehat{M}$ are the same, then

$$\sum_{\beta \in \mathbb{F}_s} -\beta\ell_\beta = \sum_{\beta \in \mathbb{F}_s} -\beta\widehat{\ell}_\beta,$$

where the $\widehat{\ell}_\beta$ are the coefficients from $\widehat{M}$. By construction, $\ell_\beta = \widehat{\ell}_\beta$ for $\beta \neq 0, 1$. Therefore, $0\ell_0 - 1\ell_1 = 0\widehat{\ell}_0 - 1\widehat{\ell}_1$, so $\ell_1 = \widehat{\ell}_1$. But ℓ_1 is the leading coefficient of the polynomial representing ϕ, and $\widehat{\ell}_1$ for π, which are distinct. Thus the coefficients of $y^{s-2}x^{s-2}$ for M and $\widehat{M}$ are different, and so at least one of M and $\widehat{M}$ has degree $2s-4$.

We now show that it is always possible to find two permutations ϕ and π of degree $s-2$ such that $\phi(x) \neq \pi(x)$ for all $x \in \mathbb{F}_s$ by providing explicit examples.

First, note the following: If g is any any permutation of $\mathbb{F}_s$, and f is defined as in (3), then consider the coefficient of x^{s-2} in f. The coefficient of x^{s-2} in $h_\alpha(x)$ is given by

$$\sum_{\substack{\gamma \in \mathbb{F}_s \\ \gamma \neq \alpha}} (-\gamma) = -\sum_{\substack{\gamma \in \mathbb{F}_s \\ \gamma \neq \alpha}} \gamma = -(-\alpha) = \alpha,$$

and so the coefficient of x^{s-2} in $f(x)$ is

$$\sum_{\alpha \in \mathbb{F}_s} \left(\big(-g(\alpha)\big) \sum_{\substack{\gamma \in \mathbb{F}_s \\ \gamma \neq \alpha}} (-\gamma) \right) = \sum_{\alpha \in \mathbb{F}_s} \big(-g(\alpha)\big)(\alpha) = \sum_{\alpha \in \mathbb{F}_s} -\alpha g(\alpha). \tag{5}$$

Now let

$$\sigma(\alpha) := \begin{cases} -\alpha^{-1}, & \text{if } \alpha \neq 0, \\ 0, & \text{if } \alpha = 0. \end{cases} \tag{6}$$

Using (5), the coefficient of x^{s-2} in the polynomial for σ is given by

$$\sum_{\alpha \in \mathbb{F}_s} -\alpha\sigma(\alpha) = \sum_{\alpha \in \mathbb{F}_s^*} 1 = -1.$$

If $s = p^n$ for $p > 3$, consider the permutation

$$\rho(\alpha) = \begin{cases} \alpha^{-1}, & \text{if } \alpha \neq 0, -1, \\ -1, & \text{if } \alpha = 0, \\ 0, & \text{if } \alpha = -1. \end{cases}$$

Then

$$\sum_{\alpha \in \mathbb{F}_s} -\alpha\rho(\alpha) = \sum_{\substack{\alpha \in \mathbb{F}_s^* \\ \alpha \neq -1}} -1 = 2.$$

Therefore σ and ρ are both of degree $s-2$ and have distinct leading coefficients. Thus we can use σ and ρ as the permutations ϕ and π, respectively.

If $s = 2^n, n > 2$, let ξ be a primitive element of $\mathbb{F}_s$ (i.e., ξ generates the multiplicative group of $\mathbb{F}_s$). Since $\mathbb{F}_s$ has characteristic 2, the map $x \mapsto x^2$ is an automorphism of $\mathbb{F}_s$ that fixes $\mathbb{Z}_2$, and hence every element has a square root. Since $-x = x$, the square root is unique.

Define[1] μ as

$$\mu(\alpha) := \begin{cases} \alpha, & \text{if } \alpha \neq 0, 1, \xi, \xi^{1/2}, \\ 1, & \text{if } \alpha = 0, \\ 0, & \text{if } \alpha = 1, \\ \xi^{1/2}, & \text{if } \alpha = \xi, \\ \xi, & \text{if } \alpha = \xi^{1/2}. \end{cases}$$

Recall the permutation σ defined in (6). For $\alpha = 0, 1, \xi, \xi^{1/2}$, $\sigma(\alpha) \neq \mu(\alpha)$. For $\alpha \neq 0, 1, \xi, \xi^{1/2}$, $\sigma(\alpha) = \mu(\alpha)$ implies $\alpha^{-1} = \alpha$, which implies that $\alpha = 1$, a contradiction. Thus, $\sigma(\alpha) \neq \mu(\alpha)$ for all $\alpha \in \mathbb{F}_s$. Now, as shown in the proof of Proposition 3.3 the coefficient of x^{s-2} in the polynomial corresponding to μ is

$$\begin{aligned} \sum_{\alpha \in \mathbb{F}_s} -\alpha\mu(\alpha) &= \sum_{\alpha \in \mathbb{F}_s} \alpha\mu(\alpha), \quad \text{since } \mathbb{F}_s \text{ has characteristic 2,} \\ &= \left(\sum_{\substack{\alpha \in \mathbb{F}_s \\ \alpha \neq 0,1,\xi,\xi^{1/2}}} \alpha^2 \right) + \xi^{1/2}(\xi) + \xi(\xi^{1/2}) \\ &= \sum_{\substack{\alpha \in \mathbb{F}_s \\ \alpha \neq 0,1,\xi,\xi^2}} \alpha, \quad \text{since } x \mapsto x^2 \text{ is an automorphism of } \mathbb{F}_s, \\ &= 0 - (0 + 1 + \xi + \xi^2), \quad \text{by Lemma 4.5} \\ &= 1 + \xi + \xi^2. \end{aligned}$$

[1]We thank Pieter Blue for suggesting this permutation.

Since the powers $\xi^0, \xi, \xi^2, \ldots, \xi^{n-1}$ form a basis for $\mathbb{F}_s$ as an n-dimensional vector space over $\mathbb{F}_2$, $1 + \xi + \xi^2$ is neither 0 nor 1. Thus σ and μ have distinct leading coefficients (and are of degree $s-2$), and so can be used as the permutations ϕ and π, respectively.

When $s = 3^n$ for $n > 1$, let $\xi \in \mathbb{F}_s$ with $\xi \neq 0, 1, -1$. Since $s > 3$, there exists such an element in $\mathbb{F}_s$. Let

$$\tau(\alpha) = \begin{cases} \xi\alpha^{-1}, & \alpha \neq 0, -1, \\ -\xi, & \alpha = 0, \\ 0, & \alpha = -1, \end{cases}$$

Then $\sigma(\alpha) \neq \tau(\alpha)$ for all $\alpha \in \mathbb{F}_s$. Now, the coefficient of x^{s-2} in the polynomial that corresponds to τ is

$$\begin{aligned} \sum_{\alpha} -\alpha\tau(\alpha) &= \sum_{\alpha \neq 0, -1} -\alpha(\xi\alpha^{-1}) \\ &= -\sum_{\alpha \neq 0, -1} \xi = -(3^n - 2)\xi = 2\xi = -\xi \neq -1 \end{aligned}$$

Thus σ and τ have distinct leading coefficients (and are of degree $s-2$), and so can be used when $p = 3$, $n > 1$ and $s = 3^n$ as the permutations ϕ and π, respectively.

□

5 Circulant Latin squares and other special cases

Definition 5.1. *Let L be a Latin square of order t, and let $m \in \{1, ..., t-1\}$. L is* m-circulant *if each row is obtained by cyclically shifting every entry in the previous row m places to the right.*

Note that this definition does not require the order of L to be a prime or prime power. However, m-circulant Latin squares of order t exist only if m is relatively prime to t. Thus there exist m-circulant Latin squares of order p for all $m \in \{1, ..., p-1\}$.

Example 5.2.

$$L = \begin{bmatrix} 1 & 0 & 2 & 4 & 3 \\ 2 & 4 & 3 & 1 & 0 \\ 3 & 1 & 0 & 2 & 4 \\ 0 & 2 & 4 & 3 & 1 \\ 4 & 3 & 1 & 0 & 2 \end{bmatrix}$$

is a 3-circulant Latin square of order 5.

If we label the rows and columns $0, 1, ..., 4$, we find that 1 occurs in cells $(0,0)$, $(1,3)$, $(2,1)$, $(3,4)$ and $(4,2)$. Thus if g is the LPP for this Latin square, we have $1 = g(0,0) = g(1,3) = g(2,1) = g(3,4) = g(4,2)$.

In general, we have the following:

Lemma 5.3. *If $g : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$ is the local permutation polynomial of an m-circulant Latin square L of order p, then*

$$g(i,j) = g(i+1, j+m) \text{ for all } i,j \in \mathbb{Z}_p.$$

We may characterize an m-circulant Latin square of prime order by the permutation that determines its first row:

Lemma 5.4. *Let $g : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$ be the LPP of an m-circulant Latin square L of order p, and let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be the permutation in the first row of L. Then*

$$g(x,y) = g(0, y+mx) = f(y+mx) \ \ \forall\, x,y \in \mathbb{Z}_p.$$

Proposition 5.5. *An m-circulant Latin square of order p can be represented as a polynomial in two variables of degree at most $p-2$. Further, there exist m-circulant Latin squares whose local permutation polynomials achieve this bound.*

Proof. Let $g : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$ represent an m-circulant Latin square with LPP g whose first row is given by a polynomial f. Then the degree of f is at most $p-2$, and by Lemma 5.4, $g(x,y) = g(0, y+mx) = f(y+mx)$. Thus, g can be represented as a polynomial in two variables of degree at most $p-2$.

Using the construction of σ given in (6), we will construct a Latin square whose polynomial attains this degree bound. Let $g(0,y)$ be the permutation σ, which then extends to the rest of the Latin square. Since the coefficient of y^{p-2} of σ is nonzero, the two-variable polynomial g has degree $p-2$. □

Example 5.6. *The local permutation polynomials for m-circulant Latin squares of order 5 and 7, respectively, are given below. Here, the first row of the Latin square is given by $[a_0, a_1, ..., a_{p-1}]$ for $p = 5, 7$.*

$$\begin{aligned} g_5(x,y) \;=\; & (a_0 + 2a_1 + 3a_2 + 4a_3)m^3x^3 + (2a_0 + 4a_1 + a_2 + 3a_3)m^2x^2y \\ & +(3a_0 + a_1 + 4a_2 + 2a_3)mxy^2 + (4a_0 + 3a_1 + 2a_2 + a_3)y^3 \\ & +(a_0 + 2a_2 + 2a_3)m^2x^2 + (3a_0 + a_2 + a_3)mxy \\ & +(a_0 + 2a_2 + 2a_3)y^2 + (a_0 + 2a_1 + 4a_2 + 3a_3)mx \\ & +(4a_0 + 3a_1 + a_2 + 2a_3)y + a_0, \end{aligned}$$

$$
\begin{aligned}
g_7(x,y) \;=\;& (a_0+2a_1+3a_2+4a_3+5a_4+6a_5)m^5x^5 \\
&+(2a_0+4a_1+6a_2+a_3+3a_4+5a_5)m^4x^4y \\
&+(3a_0+6a_1+2a_2+5a_3+a_4+4a_5)m^3x^3y^2 \\
&+(4a_0+a_1+5a_2+2a_3+6a_4+3a_5)m^2x^2y^3 \\
&+(5a_0+3a_1+a_2+6a_3+4a_4+2a_5)mxy^4 \\
&+(6a_0+5a_1+4a_2+3a_3+2a_4+a_5)y^5 \\
&+(a_0+4a_2+6a_3+6a_4+4a_5)x^4+(3a_0+5a_2+4a_3+4a_4+5a_5)m^3x^3y \\
&+(6a_0+3a_2+a_3+a_4+3a_5)m^2x^2y^2+(3a_0+5a_2+4a_3+4a_4+5a_5)mxy^3 \\
&+(a_0+4a_2+6a_3+6a_4+4a_5)y^4+(a_0+2a_1+2a_2+2a_4)m^3x^3 \\
&+(4a_0+a_1+a_2+a_4)m^2x^2y+(3a_0+6a_1+6a_2+6a_4)mxy^2 \\
&+(6a_0+5a_1+5a_2+5a_4)y^3+(a_0+6a_2+4a_3+4a_4+6a_5)m^2x^2 \\
&+(5a_0+2a_2+6a_3+6a_4+2a_5)mxy+(a_0+6a_2+4a_3+4a_4+6a_5)y^2 \\
&+(a_0+2a_1+5a_2+6a_3+3a_4+4a_5)mx \\
&+(6a_0+5a_2+2a_2+a_3+4a_4+3a_5)y+a_0.
\end{aligned}
$$

Proposition 5.7. *Let $g:\mathbb{Z}_p\times\mathbb{Z}_p\to\mathbb{Z}_p$ be the LPP for an m-circulant Latin square of order p whose first row is given by $[\alpha,\alpha+k,...,\alpha+(p-1)k]$ for some $0<k<p$. Then g is linear and is given by*

$$g(x,y)=(p-1)mkx+ky+\alpha. \tag{7}$$

Proof. Define $g:\mathbb{Z}_p\times\mathbb{Z}_p\to\mathbb{Z}_p$ by $g(x,y)=(p-1)mkx+ky+\alpha$ for $0<m<p-1$. Then

$$g(0,n)=\alpha+nk$$

and

$$
\begin{aligned}
g(x+1,y+m) &= (p-1)mk(x+1)+k(y+m)+\alpha \\
&= (p-1)mkx+(p-1)mk+ky+mk+\alpha \\
&= (p-1)mkx+ky+\alpha \\
&= g(x,y)
\end{aligned}
$$

Thus g is the LPP for an m-circulant Latin square with first row $[\alpha,\alpha+k,...,\alpha+(p-1)k]$. Moreover, there are exactly as many different functions of form (7) as there are m-circulant Latin squares whose first row is given by $[\alpha,\alpha+k,...,\alpha+(p-1)k]$. □

Now consider the case of a Latin square of order $s=p^n$. While it is straightforward to check that any polynomial $g:\mathbb{F}_s\times\mathbb{F}_s\to\mathbb{F}_s$ that satisfies the condition in Lemma 5.4 (with m being any nonzero element of $\mathbb{F}_s$) is an LPP, the resulting Latin square may not be circulant if s is a prime power. However, we still have the following:

Proposition 5.8. *Let $g:\mathbb{F}_s\times\mathbb{F}_s\to\mathbb{F}_s$ be the LPP of a Latin square L of order s, and suppose*

$$g(x,y)=g(0,y+mx)=f(y+mx)\ \ \forall\, x,y\in\mathbb{F}_s,$$

where $f : \mathbb{F}_s \to \mathbb{F}_s$ denotes the permutation in the first row of L and $m \in \mathbb{F}_s^*$. Then the degree of g is at most $s-2$, and there exist Latin squares of order s whose local permutation polynomials achieve this bound.

References

[1] Leonard E. Dickson. The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. *Ann. of Math.*, 11:65–120, 161–183, 1897.

[2] Wiebke S. Diestelkamp. The decomposability of simple orthogonal arrays on 3 symbols having $t+1$ rows and strength t. *J. Combin. Des.*, 8:442–458, 2000.

[3] Marshall Hall. An existence theorem for Latin squares. *Bull. Amer. Math. Soc.*, 51:387–388, 1945.

[4] Rudolf Lidl and Harald Niederreiter. *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and Its Applications*. Addison-Wesley Publishing Company, Reading, MA, 1983.

[5] Gary L. Mullen. Local permutation polynomials over $\mathbf{Z}_p$. *Fibonacci Quart.*, 18:104–108, 1980.

[6] Gary L. Mullen. Local permutation polynomials over a finite field. *Det Kong. Norske Vid. Selskab, Series Skrifter*, 1:1–4, 1981.