Study of symmetries of Latin squares by local permutation polynomials

Raúl M. Falcón

Department of Applied Mathematics I.
Universidad de Sevilla.
rafalgan@us.es

Joint work with: Jaime Gutiérrez-Gutiérrez and Jorge Jiménez-Urroz.

Latin squares

Ruth **Moufang** (1935)

A **quasigroup** (Q, f) of order q is formed by
- a finite set Q of q elements, and
- a binary operation f such that, for all $a, b, c \in Q$:

$$\begin{cases} f(a,b) \neq f(a,c) \text{ if } b \neq c, \\ f(a,b) \neq f(c,b) \text{ if } a \neq c. \end{cases}$$

Its Cayley table L_f is a **Latin square** of order q.

0	1	2
1	2	0
2	0	1

Two quasigroups (Q, f) and (Q, g) are **isotopic** if there exist three permutations π_1, π_2, π_3 in the symmetric group $\mathcal{S}_Q$ on Q such that

$$g(\pi_1(a), \pi_2(b)) = \pi_3(f(a, b))$$

for all $a, b \in Q$. Then, $L_f^{(\pi_1,\pi_2,\pi_3)} = L_g$.

π_1 (rows); π_2 (columns); π_3 (symbols).

$$\begin{cases} L \equiv \begin{array}{|c|c|c|c|}\hline 1&2&3&4\\\hline 2&3&4&1\\\hline 3&4&1&2\\\hline 4&1&2&3\\\hline\end{array} \\ \Theta = ((1\ 2)(3\ 4), (2\ 3), \mathrm{Id}) \end{cases} \Rightarrow L^{\Theta} \equiv \begin{array}{|c|c|c|c|}\hline 2&4&3&1\\\hline 1&3&2&4\\\hline 4&2&1&3\\\hline 3&1&4&2\\\hline\end{array}$$

- **Isotopism**: $\Theta = (\pi_1, \pi_2, \pi_3)$.
- $\pi_1 = \pi_2 = \pi_3 \Rightarrow$ **Isomorphic**.
- $f = g \Rightarrow$ **Autotopism / Automorphism**.

$\mathcal{S}_3$: The symmetric group on $\{1, 2, 3\}$.

Two quasigroups (Q, f) and (Q, g) are π-**conjugate**, with $\pi \in \mathcal{S}_3$, if

$$g(a_{\pi(1)}, a_{\pi(2)}) = a_{\pi(3)} \Leftrightarrow f(a_1, a_2) = a_3$$

for all $a_1, a_2, a_3 \in Q$. Then, $L_f^\pi := L_g$.

$L = L^{(12)} \equiv$

1	2	3	4
2	3	4	1
3	4	1	2
4	1	2	3

$\Rightarrow$

$L^{(13)} = L^{(23)} \equiv$

1	2	3	4
4	1	2	3
3	4	1	2
2	3	4	1

$L^{(123)} = L^{(132)} \equiv$

1	4	3	2
2	1	4	3
3	2	1	4
4	3	2	1

A quasigroup (Q, f) is **totally symmetric** if $L_f^\pi = L_f$ for all $\pi \in \mathcal{S}_3$.

Local permutation polynomials

A polynomial

$$f(x) := \sum_{i=0}^{q-1} c_i x^i \in \mathbb{F}_q[x]$$

with q a prime power, is a **permutation polynomial** (**PP**) if the equation $f(x) = a$ has one solution in $\mathbb{F}_q$ for each $a \in \mathbb{F}_q$.

Each polynomial $f \in \mathrm{PP}(q)$ is identified with the zeros of

$$\left\{ \frac{f(i)^q - f(i) - f(j)^q + f(j)}{f(i) - f(j)} = 0 \colon\ i < j \right\}$$

$$\mathrm{PP}(2) = \bigcup_{a \in \mathbb{F}_2} \{x + a\} \qquad \mathrm{PP}(3) = \bigcup_{a,b \in \mathbb{F}_3} \{ax + b \colon\ a^2 = 1\}$$

$$\mathrm{PP}(4) = \bigcup_{a,b,c \in \mathbb{F}_4} \{ax^2 + bx + c \colon\ ab = 0 = a^3 + b^3 + 1\}$$

A polynomial

$$f(x,y) := \sum_{i,j=0}^{q-1} c_{ij} x^i y^j \in \mathbb{F}_q[x,y]$$

with q a prime power, is a **local permutation polynomial** (**LPP**) if

1. $f(x,y) = a$ has q solutions for all $a \in \mathbb{F}_q$.
2. Both $f(a,x)$, $f(x,a) \in \mathbb{F}_q[x]$ are **permutation polynomials** (**PP**) for all $a \in \mathbb{F}_q$.

$$\mathrm{LPP}(q) := \{ \text{ LPPs in } \mathbb{F}_q[x,y] \}$$

$$\mathcal{L}(q) := \{ \text{ Latin squares of order } q \text{ with entries in } \mathbb{F}_q \}.$$

Theorem (Mullen, 1980)

$$f \in \mathrm{LPP}(q) \Leftrightarrow L_f := (f(a,b))_{a,b\in\mathbb{F}_q} \in \mathcal{L}(q).$$

$$L \in \mathcal{L}(q) \Rightarrow \sum_{a,b\in\mathbb{F}_q} L[a,b] \prod_{c\neq a} \frac{x-c}{a-c} \prod_{d\neq b} \frac{y-d}{b-d} \in \mathrm{LPP}(q)$$

4	2	1	0	3
3	4	2	1	0
0	3	4	2	1
1	0	3	4	2
2	1	0	3	4

$$x^3 + 2x^2y - 2xy^2 - y^3 + x^2 - 2xy + y^2 + 2x - 2y - 1$$

Theorem (Mullen, 1980)

Every polynomial in $\mathrm{LPP}(2)$ *and* $\mathrm{LPP}(3)$ *is linear.*

$q = 2$:

0 1 1 0	1 0 0 1
$x + y$	$x + y + 1$

$q = 3$:

0 1 2 1 2 0 2 0 1	1 2 0 2 0 1 0 1 2	2 0 1 0 1 2 1 2 0	0 1 2 2 0 1 1 2 0	1 2 0 0 1 2 2 0 1	2 0 1 1 2 0 0 1 2
$x + y$	$x + y + 1$	$x + y - 1$	$-x + y$	$-x + y + 1$	$-x + y - 1$
0 2 1 1 0 2 2 1 0	1 0 2 2 1 0 0 2 1	2 1 0 0 2 1 1 0 2	0 2 1 2 1 0 1 0 2	1 0 2 0 2 1 2 1 0	2 1 0 1 0 2 0 2 1
$x - y$	$x - y + 1$	$x - y - 1$	$-x - y$	$-x - y + 1$	$-x - y - 1$

Theorem (Diestelkamp, Hartke, Kenney, 04)

For $q > 3$, if $f \in \mathrm{LPP}(q)$, then $\deg(f) \leq 2q - 4$. This upper bound is sharp.

Example: In $\mathbb{F}_4$, let u be a root of the irreducible polynomial $x^2 + x + 1$ over $\mathbb{Z}_2$. Then:

0	1	u	$u+1$
1	0	$u+1$	u
u	$u+1$	0	1
$u+1$	u	1	0

$$x^2y^2 + x^2y + xy^2 + xy + x + y$$

Lemma (Mullen, 1980)

The set of coefficients of a generic polynomial

$$f(x,y) = \sum_{\substack{i,j=0 \\ i+j \leq 2q-4}}^{q-1} c_{ij} x^i y^j \in \mathrm{LPP}(q)$$

describes an affine variety.

Each polynomial $f \in \mathrm{LPP}(q)$ is identified with the zeros of

$$\begin{cases} \frac{f(i,j)^q - f(i,j) - f(i,k)^q + f(i,k)}{f(i,j) - f(i,k)}, & \text{for all } i,j,k \in \mathbb{F}_q, \text{ with } j \neq k, \\ \frac{f(i,j)^q - f(i,j) - f(k,j)^q + f(k,j)}{f(i,j) - f(k,j)}, & \text{for all } i,j,k \in \mathbb{F}_q, \text{ with } j \neq i. \end{cases}$$

Theorem (F, Gutiérrez, Jiménez, 25+)

$$\mathcal{L}(2) \equiv \begin{array}{|c|c|}\hline a & 1+a \\ \hline 1+a & a \\ \hline \end{array}$$

$$\mathrm{LPP}(2) = \{x + y + a \colon\ a \in \mathbb{Z}_2\}.$$

$$\mathcal{L}(3) \equiv \begin{array}{|r|r|r|}\hline c & b+c & -b+c \\ \hline a+c & a+b+c & a-b+c \\ \hline -a+c & -a+b+c & -a-b+c \\ \hline \end{array}$$

$$\mathrm{LPP}(3) = \{ax + by + c \colon\ a, b \neq 0\}$$

Theorem (F, Gutiérrez, Jiménez, 25+)

Every polynomial in $\mathrm{LPP}(4)$ *is of the form*

$$(a^2b^2 + c^2bd)x^2y^2 + (a^2bd + c^2d^2)x^2y + bxy^2 + ex^2 + ay^2 + dxy + fx + cy + g$$

where

$$\begin{cases} ac = 0, \\ ef = 0, \\ a^3 + c^3 = 1, \\ e^3 + f^3 = 1, \\ b^3 = d^3, \\ bf = d^2f^3, \\ de + b^2c^2d + a^2bdf + a^2d^3 + c^2d^2f = 0, \\ be + a^2bd^2 + bc^2df + c^2d^3 + a^2df^2 = 0. \end{cases}$$

Theorem (F, Gutiérrez, Jiménez, 25+)

$\mathrm{LPP}(4) = S_1 \sqcup S_2$, *where*

$$S_1 := \{a\,x^2 + c\,y^2 + b\,x + d\,y + e\colon\ a^3 + b^3 + 1 = 0,\ c^3 + d^3 + 1 = 0\}$$

and

$$S_2 := \{(xy + abc)\,(axy + bx + cy) + dx^2 + bcd^2x + ey^2 + a^2bey + f\colon$$

$$a, b, c \neq 0,\ d(d + a^2b^2) = 0,\ e(e + a^2c^2) = 0\}$$

In particular, $|S_1| = 144$ *and* $|S_2| = 432$.

Do they correspond to the two isotopic classes of $\mathcal{L}(4)$?

Symmetries of Latin squares by LPPs

$f, g \in \mathrm{LPP}(q)$ are **isotopic** if there exist $\pi_1, \pi_2, \pi_3 \in \mathrm{PP}(q)$ such that

$$g(\pi_1(x), \pi_2(y)) = \pi_3(f(x, y)).$$

$\Theta := (\pi_1, \pi_2, \pi_3)$ is an **isotopism** such that $f^\Theta = g$. (An **isomorphism** if $\pi_1 = \pi_2 = \pi_3$.) (An **autotopism** if $f = g$.)

Lemma

Every polynomial $f \in \mathrm{LPP}(q)$ is isotopic to $g(x, y) \cdot xy + x + y$ for some $g(x, y) \in \mathbb{F}_q[x, y]$.

If $g = 0$, then we call f **isolinear**.

Theorem (F, Gutiérrez, Jiménez, 25+)

Every polynomial in $\mathrm{LPP}(2)$ and $\mathrm{LPP}(3)$ is isolinear. Furthermore, a polynomial in $\mathrm{LPP}(4)$ is isolinear if and only if it belongs to S_1.

$$\mathrm{Isot}(q) := \mathrm{PP}(q) \times \mathrm{PP}(q) \times \mathrm{PP}(q)$$

$$\mathrm{Atop}(f) := \{\Theta \in \mathrm{Isot}(q) \colon\ f^{\Theta} = f\}.$$

$$\Theta \in \mathrm{Isot}(q) \Rightarrow \mathrm{LPP}(\Theta) := \{f \in \mathrm{LPP}(q) \colon\ \Theta \in \mathrm{Atop}(f)\}.$$

Lemma

If $\Theta \in \mathrm{Isot}(q)$ is trivial, then $\mathrm{LPP}(\Theta) = \mathrm{LPP}(q)$.

Theorem (F, Gutiérrez, Jiménez, 25+)

$\sharp\mathrm{LPP}(\Theta)$ only depends on the conjugacy class of Θ.

- $q = 2$:

$$\mathrm{LPP}((x+1, x+1, x)) = \{-x + y + a \colon\ a \in \mathbb{Z}_2\} \xrightarrow{\sharp} 2$$

- $q = 3$:

$$\mathrm{LPP}((x+1, x+1, x+1)) = \{-x + 2y + a \colon\ a \neq 0\} \xrightarrow{\sharp} 3$$

$$\mathrm{LPP}((x+1, x+1, x)) = \{ax - ay + b \colon\ b \neq 0\} \xrightarrow{\sharp} 6$$

$$\mathrm{LPP}((2x, 2x, 2x)) = \{ax + by \colon\ a, b \neq 0\} \xrightarrow{\sharp} 4$$

Two LPPs $f, g \in \mathbb{F}_q[x, y]$ are **conjugate** if one of the following six identities holds.

1. $g(x, y) = f(x, y)$.
2. $g(x, y) = f(y, x)$.
3. $g(x, f(x, y)) = y$.
4. $g(f(x, y), x) = y$.
5. $g(f(x, y), y) = x$.
6. $g(y, f(x, y), x) = x$.

If all the six identities hold for $f = g$, then f is **totally symmetric**.

Theorem (F, Gutiérrez, Jiménez, 25+)

- *Every polynomial in* $\mathrm{LPP}(2)$ *is totally symmetric.*
- *Every totally symmetric polynomial in* $\mathrm{LPP}(3)$ *is of the form*

$$2(x+y)+a$$

- *There are four totally symmetric polynomials in* $\mathrm{LPP}(4)$ *of the form*

$$x+y+a$$

and 12 *of the form*

$$x^2y^2+a(x^2y+xy^2)+a^2(xy+a(x+y))+b(x^2+y^2)+ab(x+y)+c$$

where $a\neq 0$, $b(b+a^2)=0$ *and* $a^2+ac+b+c^2=0$.

Work in progress

- High orders and high dimensions (hypercubes).
- Latin transversals.
- Critical sets.
- Autotopism group.

REFERENCES

- WS Diestelkamp, SG Hartke, RH Kenney, *On the degree of local permutation polynomials*, J. Comb. Math. Comb. Comput. **50** (2004), 129–140.
- RM Falcón, J Gutiérrez-Gutiérrez, J Jiménez-Urroz, *An algebraic approach to Latin hypercubes by local permutation polynomials over finite fields*, in preparation.
- J Gutiérrez-Gutiérrez, J Jiménez-Urroz, *Local permutation polynomials and the action of e-Klenian groups*, Finite Fields Their Appl. **91** (2023), paper 102261.
- GL Mullen. *Local permutation polynomials over* $\mathbb{Z}_p$, Fibonacci Quart. **18** (1980), 104–108.

Thank you for your attention!