Local permutation polynomials and Latin hypercubes

Jaime Gutierrez

Universidad de Cantabria

CODESCO Sevilla, July 8-12, 2024

Agenda

- Local Permutation Polynomials(LPP)
- Hypercubes
  - Hypercubes of type j and j permutation polynomials
  - Reduced Latin hypercubes.
  - The Latin hypercube algebraic variety.
- Latin Squares of order 4.
- LPP of maximum degree
- Orthogonal Latin hypercubes.
  - Orthogonal System of polynomials.
  - Mutually Orthogonal Latin Squares(MOLS) and e-Klenian polynomials
- References

Polynomials over finite fields

- Let p be a prime, $r \in \mathbb{N}$ and $q = p^r$, we denote by $\mathbb{F}_q$ the field of q elements. $\mathbb{F}_q = \{0, u^1, u^2, \ldots, u^{q-1}\}$, where u is a primitive element.
- Let $n \in \mathbb{N}$ with $n > 0$ and $\mathbb{F}_q^n = \mathbb{F}_q \times \overset{n)}{\ldots} \times \mathbb{F}_q$
- $\mathbb{F}_q[x_1, \ldots, x_n]$ the polynomial ring in variables $x_1, \ldots, x_n$

Lemma (Lagrange interpolation several variables)

If $f \in \mathbb{F}_q[x_1, \ldots, x_n]$, there exists a unique $g \in \mathbb{F}_q[x_1, \ldots, x_n]$ of degree $< q$ in each variable with $f(c_1, \ldots, c_n) = g(c_1, \ldots, c_n)$ for all $(c_1, \ldots, c_n) \in \mathbb{F}_q^n$ and

$$f \equiv g \bmod (x_1^q - x_1, \ldots, x_n^q - x_n)$$

Proof.

$$g(x_1, \ldots, x_n) = \sum_{(c_1, \ldots, c_n) \in \mathbb{F}_q^n} f(c_1, \ldots, c_n)(1 - (x_1 - c_1)^{q-1}) \cdots (1 - (x_n - c_n)^{q-1})$$

□

Identifying $f \equiv g$, f will be of degree $\deg_{x_i}(f) < q$

Permutation and Local Permutation Polynomials

Definition (Niederreiter(1975))

- $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ *is a Permutation Polynomial (or PP) if the equation*

$$f(x_1, \ldots, x_n) = a$$

has q^{n-1} *solutions in* $\mathbb{F}_q^n$ *for each* $a \in \mathbb{F}_q$.

- $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ *is a Local Permutation Polynomial (or LPP) if for each* i, $1 \leq i \leq n$,

$$f(a_1, \ldots, a_{i-1}, x_i, a_{i+1}, \ldots, a_n) \in \mathbb{F}_q[x_i]$$

is a PP in $\mathbb{F}_q[x_i]$, *for all choices of points of the form* $(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots a_n) \in \mathbb{F}_q^{n-1}$.

Remark

- *Any LPP* $\subset$ *PP.*
- *The opposite is not true in general:* $f(x_1, \ldots, x_n) = x_1^{q-1} + x_2$
- *If* $n = 1$ *: LPP =PP.*

Univariate permutation polynomials

- x^m is PP of $\mathbb{F}_q$ if and only if $\gcd(m, q-1) = 1$ and there is no PP of $\mathbb{F}_q$ with degree a divisor of $q-1$. [Hermite's Criterion]
- The transposition $(0\,1)$:$g(x) = x + \sum_{k=0}^{q-2} x^k$. permutes 1 and 0, and leave fixed any other element in $\mathbb{F}_q$.
- If u is a primitive element in $\mathbb{F}_q^*$ then: $g_q(x) = (ux-1)^{q-1} - x^{q-1} + ux$ is a PP representing a cycle of length q: $(0\,1\,u\,\ldots\,u^{q-2})$.
- The $p-$ polynomial $L(x) = \sum_{i=0}^{m} a_i x^{p^i} \in \mathbb{F}_q[x]$ is a PP of $\mathbb{F}_q$ if and only $L(x)$ only has the root 0 in $\mathbb{F}_q$
- Dickson polynomials and Chebyshev polynomials of the first kind: $T_k(x) = \cos(k \arccos x)$ are PP.
- If $t > 1$ with $\gcd(t, q-1) = 1$, s a divisor of $q-1$ and $g(x^s)$ has nonzero root in $\mathbb{F}_q$, then $x^t(g(x^s))^{(q-1)/s}$ is a PP.

Remark

Find $N_d = N_d(q)$ the number of PPs of degree d. $N_1 = q(q-1)$. $N_d = 0$ if d is a divisor of $q-1$. (Carlitz conjeture) .

[R. Lidl, H. Niederreiter, *Finite Fields* (1997)]

Some results on PP's and LPP's

Theorem

Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ be a non constant polynomial.

1. *If $f = g(x_1, \ldots, x_m) + h(x_{m+1}, \ldots, x_n), \quad 1 \leq m < n$, then f is LPP $\iff$ g and h are LPP's.*
2. *Let $g(z) \in \mathbb{F}_q[z]$ be PP. Then f is a (local) permutation polynomial $\iff$ $g(f(x_1, \ldots, x_n))$ is a (local) permutation polynomial*
3. *Let $h_1(x_1), \ldots, h_n(x_n)$ be PP's. Then f is (local) permutation polynomial $\iff$ $f(h_1(x_1), \ldots, h_n(x_n))$ is (local) permutation polynomial*
4. *$f \in \mathbb{F}_q[x_1, \ldots, x_n]$ is LPP of all finite field extensions of $\mathbb{F}_q$ $\iff$ is of the form $f = a_1 x_1^{p^{h_1}} + \cdots + a_n x_1^{p^{h_n}} + b$ where $0 \neq a_i \in \mathbb{F}_q$ and $h_i \geq 0$*
5. *Any PP has degree at most $n(q-1)-1$, and any LPP $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ is linear if $q = 2$ and $q = 3$, and has degree at most $n(q-2)$ otherwise.*

Latin squares

Definition

A square of order $q \in \mathbb{N}$ is an $q \times q$ array L with entries from a set T of size q s. t. each element of T occurs q in L. And is a latin square if each element of T occurs exact once in every row and every column of L.

$$S_1 = \begin{pmatrix} 0 & \alpha & \beta & 1 \\ \beta & 1 & 0 & \alpha \\ 1 & \beta & \alpha & 0 \\ \alpha & 0 & 1 & \beta \end{pmatrix}, S_2 = \begin{pmatrix} 0 & \alpha & \beta & 1 \\ \beta & 1 & 0 & \alpha \\ 0 & \beta & \alpha & 1 \\ \alpha & 0 & 1 & \beta \end{pmatrix}$$

$$T = \{0, 1, \alpha, \beta\}$$

Any latin square is a square, the converse is not true. S_2 is a non latin square.

Hypercubes

Definition (Laywine-Mullen(1980))

Let $n, q \in \mathbb{N}$ and F a set of q elements(symbols). An hypercube H of order q, dimension n and type j, $0 \leq j \leq n-1$ is an $n-$dimensional array $q \times \cdots \times q$ with q^n symbols, such that if whenever any j of the coordinates are fixed each of the q elements of F appears q^{n-j-1} in that subarray.
A Latin hypercube is hypercube of type $n-1$.

- If $n = 1$ (Permutation)
- If $n = 2$
  - $j = 0$ (Square)
  - $j = 1$ (Latin square)
- $n = 3$
  - $j = 0$ (Cube)
  - $j = 2$ (Latin cube)

Remark

Any hypercube H of type j is also of types $0, 1, ..., j-1$.

Notation (https://users.cecs.anu.edu.au/ bdm/data/latincubes.html)

- *The set* $F = \{0, 1, \ldots, q-1\}$
- *The* q^n *cells:* $[0, 0, ..., 0], [0, 0, ..., 1], ..., [q-1, q-1, ..., q-1]$

The hypercube is represented as a n-dimensional array H with

$$H[x_1, x_2, ..., x_n] = x_{n+1}$$

```
          C1                                        C2
0123    1032    2301    3210   ||   0123    3210    3210    3210
1032    0123    3210    2301   ||   1032    2301    2301    2301
2301    3210    0123    1032   ||   2301    1032    1032    1032
3210    2301    1032    0123   ||   3210    0123    0123    0123
(0)     (1)     (2)     (3)         (0)      (1)     (2)     (3)
For instance:
C1(1,3,0)=2,  C1(0,0,1)=1, C2(1,1,2)=3, C2(3,0,3)=0
```

$j-$Permutation polynomial

Definition

$f \in \mathbb{F}_q[x_1, \ldots, x_n]$ and $0 \leq j \leq n-1$ is a j-permutation polynomial (or j-PP) if for all choices of j variables $x_{i_1}, \ldots, x_{i_j}$ (assuming without of generality $x_{i_1}, \ldots, x_{i_j} = x_1, \ldots, x_j$), and for all choices of points $(a_1, \ldots, a_j) \in \mathbb{F}_q^j$ the equation

$$f(a_1, \ldots, a_j, x_{j+1}, \ldots, x_n) = a$$

has q^{n-j-1} solutions in $\mathbb{F}_q^{n-j}$ for each $a \in \mathbb{F}_q$.

- f is $(n-1)$-PP $\iff$ f is Local permutation polynomial
- f is $0-$PP $\iff$ f is Permutation polynomial

Remark

Any j-PP is also $k-$PP for $k = 0, 1, \ldots, j-1$

Hypercube of type j and $j-$Permutation polynomial

Theorem

There is a bijective map between $n-$dimensional hypercubes H of order a prime power q of type j $(0 \leq j \leq n-1)$ and j-PP polynomials $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ such that $\deg_{x_i}(f) < q$.

Proof.

Given H, identify the symbols to the elements of $\mathbb{F}_q = \{c_1, \ldots, c_q\}$ and, then interpolating. Conversely, given the polynomial f we construct the hypercube H as follows: given any cell indexed by $(i_1, \ldots, i_q)$

$$H(i_1, \ldots, i_q) = f(c_{i_1}, \ldots, c_{i_q})$$

□

$$C1 \longleftrightarrow X + Y + Z, \qquad C2 \longleftrightarrow X + Y + Z^3$$

Counting cubes and Latin hypercubes

Theorem

The number of PP's in $\mathbb{F}_q[x_1, \ldots, x_n]$ *is:* $N_n(q) = \frac{q^n!}{(q^{n-1})!^q}$.

Proof.

$\mathbb{F}_q = \{c_0, \ldots, c_{q-1}\}$, for $i = 0, \ldots, q-1$:

$$A_i = \{(a_1, \ldots, a_n) \in \mathbb{F}_q^n : f(a_1, \ldots, a_n) = c_i\}$$

$$A_0 \cup \ldots \cup A_{q-1} = \mathbb{F}_q^n, \quad A_i \cap A_j = \emptyset\,(i \neq j) \quad \& \quad |A_i| = q^{n-1}.$$

□

Remark (McKay-Wanless(2008))

The number of LPP's for q=2,3,4,5:

- $\mathbb{F}_q[x_1, x_2]$: $2, 12, 576, 161280$
- $\mathbb{F}_q[x_1, x_2, x_3]$: $2, 24, 55296, 2781803520$
- $\mathbb{F}_q[x_1, x_2, x_3, x_4]$: $2, 48, 36972288, 52260618977280$

Reduced Latin hypercube

Definition (McKay-Wanless(2008))

- *A Latin hypercube* $H[x_1, \ldots, x_n] = x_{n+1}$ *is reduced if, whenever* $n-1$ *entries of a tuple* $(x_1, \ldots, x_n, x_{n+1})$ *are* 0*, the other two entries are equal.*
- *The total number of Latin hypercubes of order* q *and dimension* n *is*

$$q!(q-1)!^{n-1}$$

times the number of reduced Latin hypercubes.

0123	1032	2301	3210
1032	0123	3210	2301
2301	3210	0123	1032
3210	2301	1032	0123
H(i,j,0)	H(i,j,1)	H(i,j,2)	H(i,j,3)

Reduced local permutation polynomials

$$\mathbb{F}_q = \{0, u^1, u^2, \ldots, u^{q-2}, u^{q-1} = 1\} \longleftrightarrow [0, 1, 2, \ldots, q-2, q-1]$$

Theorem

If $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ *is LPP:*

$$f = \sum_{i_1=0,\ldots,i_n=0}^{q-2,\ldots,q-2} c_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

is a reduced LPP then: $c_{00\ldots0} = 0$

$c_{10\ldots0} = 1, c_{01\ldots0} = 1, \ldots, c_{00\ldots1} = 1$

$c_{j0\ldots0} = 0, c_{0j\ldots0} = 0, \ldots, c_{00\ldots0j} = 0, \quad \forall\, j = 2, \ldots, q-2$

$\boxed{q = 5, n = 2}$

$c_{33}X^3Y^3 + c_{32}X^3Y^2 + c_{23}X^2Y^3 + c_{31}X^3Y + c_{22}X^2Y^2 + c_{13}XY^3 + c_{21}X^2Y + c_{12}XY^2 + c_{11}XY + X + Y$

$\boxed{q = 4, n = 3}$

$c_{222}X^2Y^2Z^2 + c_{221}X^2Y^2Z + c_{212}X^2YZ^2 + c_{122}XY^2Z^2 + c_{220}X^2Y^2 + c_{211}X^2YZ + c_{121}XY^2Z + c_{202}X^2Z^2 + c_{112}XYZ^2 + c_{022}Y^2Z^2 + c_{210}X^2Y + c_{120}XY^2 + c_{201}X^2Z + c_{111}XYZ + c_{021}Y^2Z + c_{102}XZ^2 + c_{012}YZ^2 + c_{110}XY + c_{101}XZ + c_{011}YZ + X + Y + Z$

The LPP's algebraic variety

Given a LPP $f \in \mathbb{F}_q[x_1, \ldots, x_n]$

$$f = \sum_{i_1=0,\ldots,i_n=0}^{q-2,\ldots,q-2} c_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$$

$$\updownarrow$$

$$(c_{0\ldots0}, c_{0\ldots01}, \ldots, c_{q-2\ldots q-2q-1}, c_{q-2\ldots q-2q-2}) \in \mathbb{F}_q^m, \quad m = (q-1)^n$$

The LPP's is an algebraic set defined by a polynomial ideal I.

$$I \lhd \mathbb{F}_q[Y_1, \ldots, Y_m]$$

$$LPP's = \mathcal{V}_{\mathbb{F}_q^m}(I) = \{\underline{c} \in \mathbb{F}_q^m : g(\underline{c}) = 0, \forall g \in I\}$$

Finding a system of generators $T = \{g_1, \ldots, g_r\}$ of the ideal I ?

$$I = (g_1, \ldots, g_r)$$

The Rabinowitsch trick

$$I = J \bigcap \mathbb{F}_q[Y_1, \ldots, Y_m]$$

$S \subset \mathbb{F}_q[Z, Y_1, \ldots, Y_m]$ and $J \lhd \mathbb{F}_q[Z, Y_1, \ldots, Y_m]$ and $J = (S \cup \{Z^{q-1} - 1\})$
Then, $h \in S$

- Choice $n-1$ variables $x_{i_1}, \ldots, x_{i_{n-1}}$ (assuming without of generality $x_{i_1}, \ldots, x_{i_{n-1}} = x_1, \ldots, x_{n-1}$)
- Choice $(a_1, \ldots, a_{n-1}) \in \mathbb{F}_q^{n-1}$
- Choice $c, b \in \mathbb{F}_q, c \neq b$:

$$h = f(a_1, \ldots, a_{n-1}, b) f(a_1, \ldots, a_{n-1}, c) Z - 1 \in S$$

- $h^{q-1} - 1 = f(a_1, \ldots, a_{n-1}, b) f(a_1, \ldots, a_{n-1}, c)^{q-1} - 1 \in T$
- $Y_j^q - Y_j \in T, \forall\, j = 1, \ldots m = (q-1)^n$

Reduced Latin squares of order 4

$$f = c_{22}X^2Y^2 + c_{21}X^2Y + c_{12}XY^2 + c_{11}XY + X + Y$$

Computing a Groebner basis of I generated by T with respect lexicografic order in the variables $c_{i,j}$

```
I=[(cc[i*(q-1)+j])**q-(cc[i*(q-1)+j]) for j in range(1,q-1) for i in
for i in range(1, len(K)):
    for j in range(1, len(K)):
        I.append((K[i]-f(X=K[i],Y=K[j]))**(q-1)-1)
ideal(I).groebner_basis()
```

```
[c_11 + c_21^2, c_12 + c_21, c_21^3 + c_22,
c_21*c_22 + c_21,  c_22^2 + c_22]
```

1. $X + Y$
2. $X^2Y^2 + uX^2Y + uXY^2 + (u+1)XY + X + Y$
3. $X^2Y^2 + (u+1)X^2Y + (u+1)XY^2 + uXY + X + Y$
4. $X^2Y^2 + X^2Y + XY^2 + XY + X + Y$

[Falcón-Morales(2007), Satoa-Inoue-Suzuk-Nabeshima-Sauto(2011)]

Theorem

Every reduced LPP in $\mathbb{F}_4[x, y]$ *is of the form*

$$a^3x^2y^2 + (a^2(x + y) + a)xy + x + y,$$

for some $a \in \mathbb{F}_4$.

0	1	u	u^2
1	$a^3 + a^2$	$(a^3 + 1)u^2 + au + a^2$	$au^2 + a^3u + u + a^2$
u	$(a^3 + 1)u^2 + au + a^2$	$au^2 + a^3u$	$a^3 + a^2 + a + 1$
u^2	$au^2 + (a^3 + 1)u + a^2$	$a^3 + a^2 + a + 1$	$a^3u^2 + au$

1. $x + y$
2. $x^2y^2 + ux^2Y + uxy^2 + (u + 1)\,xy + x + y$
3. $x^2x^2 + (u + 1)\,x^2y + (u + 1)\,xy^2 + uxy + x + y$
4. $x^2y^2 + x^2y + xy^2 + xy + x + y$

The algebraic variety of latin squares of order 4

Theorem

The set $\mathcal{LS}(4)$ is decomposed into

- *A subset $\mathcal{S}_1$ of 144 Latin squares identified with the affine variety*

$$\mathcal{V}_{\mathbb{F}_5^4}\left(\left\{a^3+b^3+1,\ c^3+d^3+1\right\}\right)$$

by means of the LPPs in $\mathbb{F}_4[x,y]$

$$a\,x^2+c\,y^2+b\,x+d\,y+e$$

- *A subset $\mathcal{S}_2$ of 432 Latin squares identified with the affine variety*

$$\mathcal{V}_{\mathbb{F}_6^4}\left(\left\{a^3+1,\ b^3+1,\ c^3+1,\ d(d+a^2b^2),\ e(e+a^2c^2)\right\}\right)$$

by means of the LPPs in $\mathbb{F}_4[x,y]$

$$a\,x^2y^2+b\,x^2y+c\,xy^2+abc\,(a\,xy+b\,x+c\,y)+d\,x^2+bcd^2\,x+e\,y^2+a^2be\,y+f.$$

Theorem

For any n, and for any $q = p^r$ there is an LPP over $\mathbb{F}_q[x_1, \ldots, x_n]$ of degree $n(q-2)$.

$g(x) = x + \sum_{k=0}^{q-2} x^k$,(transposition (0 1)) For $i = 1, \ldots, n$:

$$f_1 = x_1$$

$$f_i = f_i(x_1, \ldots, x_i) = g(f_{i-1}(x_1, \ldots, x_{i-1})^{q-2} + x_i^{q-2}) = g(f_{i-1}^{q-2} + x_i^{q-2})$$

Conjecture

$f_n(x_1, \ldots, x_n)$ is LPP of maximum degree $n(q-2)$ when $q = p^r > 3$ and $p \neq 2$

$$f_2 = g(f_1^{q-2} + x_2^{q-2}) = x_1^{q-2} + x_2^{q-2} + \sum_{k=0}^{q-2} (x_1^{q-2} + x_2^{q-2})^k.$$

$$f_3 = g(f_2^{q-2} + x_3^{q-2}) = f_2^{q-2} + x_3^{q-2} + \sum_{k=0}^{q-2} (f_2^{q-2} + x_3^{q-2})^k.$$

m-Orthogonal Latin hypercubes

Definition (Ethier-Mullen(2012))

For $n \geq 2$, a set of m $(1 \leq m \leq n)$ hypercubes of order q and dimension n is said to be m-orthogonal if when superimposed, each of the q^m order m-tuple occurs q^{n-m}.
Moreover, a set $r \geq m$ hypercubes of dimension n is mutually orthogonal if given any m hypercubes from the set, they are $m-$orthogonal.

$$q = 4, \quad r = 3, \quad m = n = 2$$

$$\left[\begin{pmatrix} 0 & 1 & 2 & 1 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 2 & 3 & 1 \\ 1 & 3 & 2 & 0 \\ 2 & 0 & 1 & 3 \\ 3 & 1 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 2 & 3 & 1 \\ 2 & 0 & 1 & 3 \\ 3 & 1 & 0 & 2 \\ 1 & 3 & 2 & 0 \end{pmatrix} \right]$$

Applications: Coding theory(MDS), finite geometries, ..

Orthogonal system of polynomials

Definition (Niederreiter(1971))

A system of polynomials $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$, $1 \leq m \leq n$, is said to be orthogonal in $\mathbb{F}_q$ if the system of equations

$$f_1(x_1, \ldots, x_n) = a_1, \ldots, f_m(x_1, \ldots, x_n) = a_m$$

has q^{n-m} solutions in $\mathbb{F}_q^n$ for each $(a_1, \ldots, a_m) \in \mathbb{F}_q^m$.

m hypercubes are m-orthogonal $\iff$ the associated polynomials is an OS

If $m = n$ this means that the OS $f_1, \ldots, f_m$ induces a permutation of $\mathbb{F}_q^n$.

Theorem (Niederreiter(1971))

There is a bijective map between orthogonal systems in $\mathbb{F}_q$ consisting of polynomials of degree $< q$ in each variable and permutation polynomials in one variable over $\mathbb{F}_{q^n}$ of degree $< q^n$

Mutually Orthogonal Latin Squares(MOLS)

Definition

- *Let $M(q)$ be the size of the largest collection of MOLS of order q, then we have $M(q) \leq q-1$ H is Complete set of MOLS if $\#(H) = M(q)$*
- *If $q = p^r$ is a power of prime p, then $M(q) = q-1$*

Theorem

1. *$f(x,y), g(x,y)$ is an OS $\iff$ $af(x,y)+bg(x,y), cf(x,y)+dg(x,y)$ is an OS, for $a,b,c,d \in \mathbb{F}_q$ such that $ad-bc \neq 0$.*
   And $\{f(x,y)+ag(x,y), a \in \mathbb{F}_q^*\}$ is a complete set of MOLS.
2. *$f(z), g(z), h_1(z), h_2(z)$ are PP's in $\mathbb{F}_q[z]$ $\iff$ for all $a,b,c,d \in \mathbb{F}_q$ s.t $ad-bc \neq 0$ $f(ah_1(x)+bh_2(y)), g(ch_1(x)+dh_2(y))$ is an OS.*
   And $\{f(x)+ah(y), a \in \mathbb{F}_q^*\}$ is complete set of MOLS.

Remark

Generalisation to LPP in $\mathbb{F}_q[x_1, \ldots, x_n]$.

$e-$Klenian polynomials

Definition

If $f \in \mathbb{F}_q[x, y]$ is PP, we say that g is a companion of f if f, g is an OS.

Question

Is it true that any LPP has a companion which is also an LPP?

Answer: Not for $q > 3$. If $q = 4$ only 144 has LPP companions of the total 576.

Definition

Let $\mathbb{F}_q = \{c_0, \ldots, c_{q-1}\}$ and $f \in \mathbb{F}_q[x, y]$ a LPP, then there exist $\gamma_i \in \Sigma_q$ such that $\gamma_i \gamma_j^{-1}$, $i \neq j$ has not fixed points for $i = 0, \ldots, q-1$ and

$$A_i = \{(a_{i,j}, b_{i,j}) : f(a_{i,j}, b_{i,j}) = c_i\} = \{(c_j, \gamma_i(c_j)) : f(c_j, \gamma_i(c_j)) = c_i\}, (j = 0, .., q-1)$$

When γ_i are defined by concrete α, β is called e−Klenian polynomial. For instance, when $\alpha = id$ and β is a cycle of lenght q ([G, Urroz(2023)] .

Orthogonal system of e-Klenian polynomials

Theorem

Let $2 \nmid q$. Every e-Klenian polynomial has a companion which is an LPP

Proof.

Let $f(x, y)$ be an e-Klenian polynomial, for each $m = 0, \ldots, q-1$ written as $m = a + bl$, for $0 \leq a \leq l-1$, $0 \leq b \leq t-1$, consider the associated partition:

$$A_m = \{(c_j, \alpha^a \beta^b(c_j)), j = 0, \ldots, q-1\}.$$

The polynomial g associated to B_m is an LPP companion of f, where

$$B_m = \{(c_k, \alpha^{a+i} \beta^{b+j}(c_k)), k = i + jl,\ 0 \leq i \leq l-1, 0 \leq j \leq t-1\}$$

□

Orthogonal system of e-Klenian polynomials in $\mathbb{F}_5$

Let $\beta = (2, 0, 1, 3, 5, 6, 4)$ the cycle of length 7, so the corresponding $e-$Klenian polynomial f is:

$$x^5 - y^5 - x^4 + y^4 + 3x^3 + 4y^3 + 2x^2 + 5y^2 + x - y + 6 \in \mathbb{F}_7[x, y]$$

and the LPP produced in the above Theorem is

$$2x^5 - y^5 + 5x^4 + y^4 - x^3 + 4y^3 + 4x^2 + 5y^2 + 2x - y + 4$$

Then, f, g is an orthogonal set.

$$\begin{pmatrix} 6 & 0 & 5 & 1 & 4 & 2 & 3 \\ 5 & 6 & 4 & 0 & 3 & 1 & 2 \\ 0 & 1 & 6 & 2 & 5 & 3 & 4 \\ 4 & 5 & 3 & 6 & 2 & 0 & 1 \\ 1 & 2 & 0 & 3 & 6 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 & 6 & 0 \\ 2 & 3 & 1 & 4 & 0 & 5 & 6 \end{pmatrix}, \quad \begin{pmatrix} 4 & 5 & 3 & 6 & 2 & 0 & 1 \\ 2 & 3 & 1 & 4 & 0 & 5 & 6 \\ 6 & 0 & 5 & 1 & 4 & 2 & 3 \\ 0 & 1 & 6 & 2 & 5 & 3 & 4 \\ 1 & 2 & 0 & 3 & 6 & 4 & 5 \\ 5 & 6 & 4 & 0 & 3 & 1 & 2 \\ 3 & 4 & 2 & 5 & 1 & 6 & 0 \end{pmatrix}$$

References

- John T. Ethier, Gary L. Mullen: Strong forms of orthogonality for sets of hypercubes. Discret. Math. 312(12-13)(2012), 2050-2061.
- Diestelkamp, W.S., Hartke, S.G., Kenney, R.H. On the degree of local permutation polynomials, *J. Comb. Math. Comb. Comput.* **50** (2004), 129–140.
- Falcon, R., Matin-Morales, J. Groebner bases and the number of Latin squares to autotopisms of order ≤ 7 . *Journal Symbolic Computation* **42** (2007) 1142-1154
- Falcón, R., Gutierrez, J., Urroz, J. An algebraic approach to Latin hypercubes by LPPs over finite fields. *Preprint(2023), Universidad de Sevilla*
- Gutierrez, J., Urroz, J. Local permutation polynomials and the action of e-Klenian groups, *Finite Fields Their Appl.* **91** (2023), paper 102261.
- McKay, B.D., Wanless, I.M. A census of small Latin hypercubes, *SIAM J. Discrete Math.* **22** (2008), 719–736.

References

- Laywine, C., Mullen, G. Discrete Mathematics Using Latin Squares, *John Wiley and Sons*, Inc., New York, 1998.
- R. Lidl, H. Niederreiter, Finite Fields, 2nd edn., Encyclopedia Math. Appl., vol.20, Cambridge University Press, Cambridge, 1997.
- H. Niederreiter, Permutation polynomials in several variables over finite fields, Proc. Jpn. Acad. 46 (1970) 1001-1005.
- H. Niederreiter, Orthogonal systems of polynomials in finite fields, Proc. Am. Math. Soc. 28 (1971) 415-422.
- Yosuke Sato, Shutaro Inoue, Akira Suzuki, Katsusuke Nabeshima, Ko Sakai: Boolean Groebner bases. J. Symb. Comput. 46(5): 622-632 (2011)