Local permutation polynomials and Latin hypercubes

Jaime Gutierrez

Universidad de Cantabria

5th Pythagorean conference, Kalamata, June 2025

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 $\mathbb{F}_q^n = \mathbb{F}_q \times \cdots^{n)} \cdots \times \mathbb{F}_q$
- $\mathbb{F}_q[x_1, \ldots, x_n]$ 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 $\deg_{x_i}(f) < q$

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

Permutation and Local Permutation Polynomials

Definition (Niederreiter(1970))

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

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

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

Definition (Mullen(1981))

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

$$f(\alpha_1, \ldots, \alpha_{i-1}, x_i, \alpha_{i+1}, \ldots, \alpha_n) \in \mathbb{F}_q[x_i]$$

is a PP in $\mathbb{F}_q[x_i]$, for all choices of points of the form $(\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots \alpha_n) \in \mathbb{F}_q^{n-1}$.

- LPP $\subset$ PP.
- The opposite is not true in general ($n \geq 2$).
- If $n = 1$: LPP $=$ PP.

Latin squares

Definition (L. Euler (1707))

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

$$S_1 = \begin{pmatrix} 0 & 2 & 3 & 1 \\ 3 & 1 & 0 & 2 \\ 0 & 3 & 2 & 1 \\ 2 & 0 & 1 & 3 \end{pmatrix}, S_2 = \begin{pmatrix} 0 & 2 & 3 & 1 \\ 3 & 1 & 0 & 2 \\ 1 & 3 & 2 & 0 \\ 2 & 0 & 1 & 3 \end{pmatrix}$$

$$q = 4, \quad F = \{0, 1, 2, 3\}$$

Latin square $\implies$ square.

1. Squares of order $q = p^r \iff$ PP in $\mathbb{F}_q[x, y]$.
2. Latin squares of order $q = p^r \iff$ LPP in $\mathbb{F}_q[x, y]$ [Mullen(1981)].

Hypercubes

Definition (Ethier, Mullen, Panario, Stevens, Thomson(2012))

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 $n-1$.

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

Remark

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

Notation

- *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 $x_{i_1}, \ldots, x_{i_j}$ (W.L.O.G $x_{i_1}, \ldots, x_{i_j} = x_1, \ldots, x_j$), and for all choices of points $(\alpha_1, \ldots, \alpha_j) \in \mathbb{F}_q^j$ the equation

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

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

- 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 $(i_1, \ldots, i_q)$

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

□

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

Polynomials of separated variables

Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ be a non constant and $0 \leq j \leq n-1$.

Theorem

f is j-PP $\iff$ for all choices of j variables $(x_{i_1}, \ldots, x_{i_j} = x_1, \ldots, x_j)$, and for all choices of points $(\alpha_1, \ldots, \alpha_j) \in \mathbb{F}_q^j$

$$\sum_{(c_{j+1},\ldots,c_n)\in\mathbb{F}_q^{n-j}} \chi_b(f(\alpha_1, \ldots, \alpha_j, c_{j+1}, \ldots, c_n)) = 0$$

for all additive character χ_b of $\mathbb{F}_q$ with $b \neq 0$.

Theorem

$$f = g(x_1, \ldots, x_m) + h(x_{m+1}, \ldots, x_n).$$

1. *If g is j_1-PP and h is j_2-PP. Then f is a $j_1 + j_2 + 1$-PP.*
2. *If $\mathbb{F}_q = \mathbb{F}_p$ and f is j-PP $\implies$ for any $j_1 + j_2 = j$, with $j_1 \leq m-1$ and $j_2 \leq n-m-1$ either g is j_1-PP or h is j_2-PP.*

- $j = 0$ [Niederreiter(1970)]
- $j = n-1$, f is LPP $\iff$ g and h are LPP's.

Counting cubes and Latin hypercubes

Theorem

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

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 (https://users.cecs.anu.edu.au/~bdm/data/)

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

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

Isotopic j-Hypercubes

Definition (McKay-Wanless(2008))

Given a hypercube $A = \{(x_1, \ldots, x_{n+1})\}$ and permutations $(p_1, \ldots, p_{n+1}) \in \Sigma_q^{n+1}$ then $B = \{(p_1(x_1), \ldots, p_{n+1}(x_{n+1}))\}$ is also a hypercube, said to be isotopic to A. This is an equivalence relation(isotopy classes).

Theorem

1. *Let $g(z) \in \mathbb{F}_q[z]$ be PP. Then*
   f *is a j-PP* $\iff$ $g(f(x_1, \ldots, x_n))$ *is a j-PP.*
2. *Let $h_1(x_1), \ldots, h_n(x_n)$ be PP's. Then*
   f *is j-PP* $\iff$ $f(h_1(x_1), \ldots, h_n(x_n))$ *is a j-PP*

Problem

- *Input:* $f, \bar{f} \in \mathbb{F}_q[x_1, \ldots, x_n]$ *j-Permutation polynomials*
- *Output:* $g(z), h_1(x_1), \ldots, h_n(x_n)$ *PP's*

$$\bar{f} = g(f(h_1(x_1), \ldots, h_n(x_n))$$

Galois j-Hypercubes

Definition

Given f an $j-PP$

$$f = \sum_{k_1=0,\ldots,k_n=0}^{q-2,\ldots,q-2} c_{k_1 k_2 \ldots k_n} x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n} = \sum_{\underline{k}} c_{\underline{k}} \underline{x}^{\underline{k}},$$

then for all $\sigma \in \text{Galois}(\mathbb{F}_q/\mathbb{F}_p)$,

$$g = f^{\sigma} = \sum_{\underline{k}} \sigma(c_{\underline{k}}) \underline{x}^{\underline{k}}$$

is also a $j-PP$, said to be Galois to f.
This is an equivalence relation (Galois classes).

Problem

- *How relating other equivalence classes of hypercubes to Galois classes?*

Definition (McKay-Wanless(2008))

- *A Latin hypercube* $H[x_1, \dots, x_n] = x_{n+1}$ *is* **reduced** *if, whenever* $n-1$ *entries of a tuple* $(x_1, \dots, x_n, x_{n+1})$ *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

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

$$f = \sum_{k_1=0,\ldots,k_n=0}^{q-2,\ldots,q-2} c_{k_1 k_2 \ldots k_n} x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$$

1. *If f is a reduced LPP, then for all $\sigma \in Galois(\mathbb{F}_q/\mathbb{F}_p)$, $f^\sigma = \sum_{\underline{k}} \sigma(c_{\underline{k}}) \underline{x}^{\underline{k}}$ is a reduced LPP.*
2. *If is reduced LPP then:* $c_{00\ldots 0} = 0$
   $c_{10\ldots 0} = 1, c_{01\ldots 0} = 1, \ldots, c_{00\ldots 1} = 1$
   $c_{j0\ldots 0} = 0, c_{0j\ldots 0} = 0, \ldots, c_{00\ldots 0j} = 0, \quad \forall j = 2, \ldots, q-2$

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

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

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.

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

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

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

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

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

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

m-Orthogonal Latin hypercubes

Definition (Laywine, Mullen(2008), Ethier, Mullen, Panario, Stevens, Thomson(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 $(a_1, \ldots, a_m) \in \mathbb{F}_q^m$.

$\boxed{m \text{ hypercubes are } m\text{-orthogonal} \iff \text{the associated polynomials is an OS}}$

If $m = n$ this means that the OS $f_1, \ldots, f_n$ 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.

Problem

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

References

- J. T. Ethier, G. L. Mullen, D. Panario, B. Stevens, D. Thomson: Sets of orthogonal hypercubes of class r. J. Comb. Theory A 119(2): 430-439 (2012)
- 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.
- Y. Sato, S. Inoue, A. Suzuki, K. Nabeshima, K. Sakai: Boolean Groebner bases. J. Symb. Comput. 46(5): 622-632 (2011)