Latin Squares and Orthogonal Arrays

Lucia Moura
School of Electrical Engineering and Computer Science
University of Ottawa
lucia@eecs.uottawa.ca

Winter 2017

Latin squares

Definition

A *Latin square* of order n is an $n \times n$ array, with symbols in $\{1, \ldots, n\}$, such that each row and each column contains each of the symbols in $\{1, \ldots, n\}$ exactly once.

1	2	3
3	1	2
2	3	1

1	3	2
3	2	1
2	1	3

	Week 1	Week 2	Week 3	Week 4
Volunteer 1	A	B	C	D
Volunteer 2	C	D	A	B
Volunteer 3	D	C	B	A
Volunteer 4	B	A	D	C

8			4		6			7
						4		
	1					6	5	
5		9		3		7	8	
				7				
	4	8		2		1		3
	5	2					9	
		1						
3			9		2			5

Orthogonal Latin Squares

Definition (Orthogonal Latin Squares)

Two Latin squares L_1 and L_2 of order n are said to be *orthogonal* if for every pair of symbols $(a, b) \in \{1, \ldots, n\} \times \{1, \ldots, n\}$ there exist a unique cell (i, j) with $L_1(i, j) = a$ and $L_2(i, j) = b$.

Example of orthogonal Latin squares of order 3:

$$L_1 = \begin{array}{|c|c|c|} \hline 1 & 2 & 3 \\ \hline 3 & 1 & 2 \\ \hline 2 & 3 & 1 \\ \hline \end{array} \qquad L_2 = \begin{array}{|c|c|c|} \hline 1 & 3 & 2 \\ \hline 3 & 2 & 1 \\ \hline 2 & 1 & 3 \\ \hline \end{array}$$

(1,1)	(2,3)	(3,2)
(3,3)	(1,2)	(2,1)
(2,2)	(3,1)	(1,3)

Orthogonal Latin squares of order 5 and 7

(sewn by Prof. Karen Meagher)

Euler's 36 officers problem

1. Leonhard Euler's Puzzle of the 36 Officers

Une question fort curieuse is the way Euler introduces this puzzle. It involves 36 officers from six regiments. In this illustration we will distinguish the regiments by their colors: black, red, blue, green, purple and brown. Each regiment is represented by officers of six different ranks, which here we will characterize as King, Queen, Rook, Bishop, Knight, Pawn. Here they are (set in Eric Bentzen's Chess Alpha):

Ther problem is to line them up in a six by six array so that each row and each column holds one officer of each rank and one officer from each regiment.

Reference: `http://www.ams.org/samplings/feature-column/fcarc-latinii1`

Euler's conjecture

Extracted from wikipedia:

Euler's conjecture and disproof [edit]

Orthogonal Latin squares were studied in detail by Leonhard Euler, who took the two sets to be $S = \{A, B, C, \ldots\}$, the first n upper-case letters from the Latin alphabet, and $T = \{\alpha, \beta, \gamma, \ldots\}$, the first n lower-case letters from the Greek alphabet—hence the name Graeco-Latin square.

In the 1780s Euler demonstrated methods for constructing Graeco-Latin squares where n is odd or a multiple of 4.[3] Observing that no order-2 square exists and being unable to construct an order-6 square (see thirty-six officers problem), he conjectured that none exist for any oddly even number $n \equiv 2 \pmod 4$. The non-existence of order-6 squares was confirmed in 1901 by Gaston Tarry through a proof by exhaustion. However, Euler's conjecture resisted solution until the late 1950s.

In 1959, R.C. Bose and S. S. Shrikhande constructed some counterexamples (dubbed the *Euler spoilers*) of order 22 using mathematical insights. Then E. T. Parker found a counterexample of order 10 using a one-hour computer search on a UNIVAC 1206 Military Computer while working at the UNIVAC division of Remington Rand (this was one of the earliest combinatorics problems solved on a digital computer).

In April 1959, Parker, Bose, and Shrikhande presented their paper showing Euler's conjecture to be false for all $n \geq 10$. Thus, Graeco-Latin squares exist for all orders $n \geq 3$ except $n = 6$.

Euler's conjecture disproved

In Chapter 6 of Stinson (2004), you can find various constructions leading to the dispoof of Euler's conjecture:

Theorem

Let n be a positive integer and $n \neq 2$ or 6. Then there exist 2 orthogonal Latin squares of order n.

Orthogonal Latin squares of odd order

Construction

Let $n > 1$ be odd. We build two orthogonal Latin squares of order n, L_1 and L_2, as follows:

$$\begin{aligned} L_1(i,j) &= (i+j) \bmod n \\ L_2(i,j) &= (i-j) \bmod n \end{aligned}$$

Proving these are orthogonal Latin squares:
They are Latin squares, since if we fix i (or j) and vary j (or i) we run through all distinct elements of $\mathbb{Z}_n$.
Let $(a,b) \in \mathbb{Z}_n \times \mathbb{Z}_n$. We must show there exist a unique cell i,j such that $L_1(i,j) = a$ and $L_2(i,j) = b$; in other words, this system of equations has a unique solution i,j:

$$(i+j) \equiv a \pmod{n},$$
$$(i-j) \equiv b \pmod{n}.$$

continuing verification

Verify that this system has a unique solution:

$$(i + j) \equiv a \pmod{n},$$
$$(i - j) \equiv b \pmod{n}.$$

We get

$$2i \equiv a + b \pmod{n},$$
$$2j \equiv a - b \pmod{n}.$$

And since 2 has an inverse in $\mathbb{Z}_n$ for n odd, namely $\frac{n+1}{2}$, we get

$$i \equiv \frac{n+1}{2}(a + b) \pmod{n},$$
$$j \equiv \frac{n+1}{2}(a - b) \pmod{n}.$$

Example of the construction for $n = 5$

$$L_1 = \begin{array}{|c|c|c|c|c|} \hline 0 & 1 & 2 & 3 & 4 \\ \hline 1 & 2 & 3 & 4 & 0 \\ \hline 2 & 3 & 4 & 0 & 1 \\ \hline 3 & 4 & 0 & 1 & 2 \\ \hline 4 & 0 & 1 & 2 & 3 \\ \hline \end{array} \qquad L_2 = \begin{array}{|c|c|c|c|c|} \hline 0 & 4 & 3 & 2 & 1 \\ \hline 1 & 0 & 4 & 3 & 2 \\ \hline 2 & 1 & 0 & 4 & 3 \\ \hline 3 & 2 & 1 & 0 & 4 \\ \hline 4 & 3 & 2 & 1 & 0 \\ \hline \end{array}$$

Direct product of Latin squares

The direct product of two Latin squares L and M of order n and m (respectively) is an $nm \times nm$ array given by

$$(L \times M)((i_1, i_2), (j_1, j_2)) = (L(i_1, j_1), M(i_2, j_2)).$$

Example:

$$L = \begin{array}{|c|c|c|}\hline 3 & 1 & 2 \\ \hline 2 & 3 & 1 \\ \hline 1 & 2 & 3 \\ \hline \end{array}, \quad M = \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 2 & 1 \\ \hline \end{array}.$$

$L \times M =$

(3,1)	(1,1)	(2,1)	(3,2)	(1,2)	(2,2)
(2,1)	(3,1)	(1,1)	(2,2)	(3,2)	(1,2)
(1,1)	(2,1)	(3,1)	(1,2)	(2,2)	(3,2)
(3,2)	(1,2)	(2,2)	(3,1)	(1,1)	(2,1)
(2,2)	(3,2)	(1,2)	(2,1)	(3,1)	(1,1)
(1,2)	(2,2)	(3,2)	(1,1)	(2,1)	(3,1)

.

Direct product of Latin squares

Lemma

If L is a Latin square of order n and M is a Latin square of order m, then $L \times M$ is a Latin square of order $n \times m$.

Proof: Consider a row (i_1, i_2) of $L \times M$. Let $1 \leq x, y \leq n$, we will show how to find the symbol (x, y) in row (i_1, i_2). Since L is a Latin square, there exists a unique column j_1 such that $L(i_1, j_1) = x$. Since M is a Latin square, there exists a unique column j_2 such that $L(i_2, j_2) = y$. Then $(L \times M)((i_1, i_2)(j_1, j_2) = (x, y)$. $\square$

Direct product construction

Theorem (Direct Product)

If there exist orthogonal Latin squares of orders n and m, then there exist orthogonal Latin squares of order nm.

Proof: Suppose L_1 and L_2 are orthogonal Latin squares of order n and M_1 and M_2 are orthogonal Latin squares of order m. We will show that $L_1 \times M_1$ and $L_2 \times M_2$ are orthogonal Latin squares of order nm. The previous Lemma shows they are Latin squares. We must show that they are orthogonal. Take an ordered pair of symbols $((x_1, y_1), (x_2, y_2))$, we must find a unique cell $((i_1, i_2), (j_1, j_2))$ such that $(L_1 \times M_1)((i_1, i_2), (j_1, j_2)) = (x_1, y_1)$ and $(L_2 \times M_2)((i_1, i_2), (j_1, j_2)) = (x_2, y_2)$. In other words, we need to show $L_1(i_1, j_1) = x_1$, $M_1(i_2, j_2) = y_1$, $L_2(i_1, j_1) = x_2$, $M_2(i_2, j_2) = y_2$, First and third, comes from L_1 and L_2 orthogonal. Second and fourth, follows from M_1 and M_2 orthogonal. $\square$

Direct product construction: example

We take L_1 and L_2 orthogonal Latin squares of order 3, and M_1 and M_2 orthogonal Latin squares of order 4.
We build $L_1 \times M_1$ and $L_2 \times M_2$ orthogonal Latin squares of order 12.

(1,1)(1,3)(1,4)(1,2)(2,1)(2,3)(2,4)(2,2)(3,1)(3,3)(3,4)(3,2)	(1,1)(1,4)(1,2)(1,3)(3,1)(3,4)(3,2)(3,3)(2,1)(2,4)(2,2)(2,3)
(1,4)(1,2)(1,1)(1,3)(2,4)(2,2)(2,1)(2,3)(3,4)(3,2)(3,1)(3,3)	(1,3)(1,2)(1,1)(1,4)(3,3)(3,2)(3,1)(3,4)(2,3)(2,2)(2,1)(2,4)
(1,2)(1,4)(1,3)(1,1)(2,2)(2,4)(2,3)(2,1)(3,2)(3,4)(3,3)(3,1)	(1,4)(1,1)(1,3)(1,2)(3,4)(3,1)(3,3)(3,2)(2,4)(2,1)(2,3)(2,2)
(1,3)(1,1)(1,2)(1,4)(2,3)(2,1)(2,2)(2,4)(3,3)(3,1)(3,2)(3,4)	(1,2)(1,3)(1,1)(1,4)(3,2)(3,3)(3,1)(3,4)(2,2)(2,3)(2,1)(2,4)
(2,1)(2,3)(2,4)(2,2)(3,1)(3,3)(3,4)(3,2)(1,1)(1,3)(1,4)(1,2)	(2,1)(2,4)(2,2)(2,3)(1,1)(1,4)(1,2)(1,3)(3,1)(3,4)(3,2)(3,3)
(2,4)(2,2)(2,1)(2,3)(3,4)(3,2)(3,1)(3,3)(1,4)(1,2)(1,1)(1,3)	(2,3)(2,2)(2,1)(2,4)(1,3)(1,2)(1,1)(1,4)(3,3)(3,2)(3,1)(3,4)
(2,2)(2,4)(2,3)(2,1)(3,2)(3,4)(3,3)(3,1)(1,2)(1,4)(1,3)(1,1)	(2,4)(2,1)(2,3)(2,2)(1,4)(1,1)(1,3)(1,2)(3,4)(3,1)(3,3)(3,2)
(2,3)(2,1)(2,2)(2,4)(3,3)(3,1)(3,2)(3,4)(1,3)(1,1)(1,2)(1,4)	(2,2)(2,3)(2,1)(2,4)(1,2)(1,3)(1,1)(1,4)(3,2)(3,3)(3,1)(3,4)
(3,1)(3,3)(3,4)(3,2)(1,1)(1,3)(1,4)(1,2)(2,1)(2,3)(2,4)(2,2)	(3,1)(3,4)(3,2)(3,3)(2,1)(2,4)(2,2)(2,3)(1,1)(1,4)(1,2)(1,3)
(3,4)(3,2)(3,1)(3,3)(1,4)(1,2)(1,1)(1,3)(2,4)(2,2)(2,1)(2,3)	(3,3)(3,2)(3,1)(3,4)(2,3)(2,2)(2,1)(2,4)(1,3)(1,2)(1,1)(1,4)
(3,2)(3,4)(3,3)(3,1)(1,2)(1,4)(1,3)(1,1)(2,2)(2,4)(2,3)(2,1)	(3,4)(3,1)(3,3)(3,2)(2,4)(2,1)(2,3)(2,2)(1,4)(1,1)(1,3)(1,2)
(3,3)(3,1)(3,2)(3,4)(1,3)(1,1)(1,2)(1,4)(2,3)(2,1)(2,2)(2,4)	(3,2)(3,3)(3,1)(3,4)(2,2)(2,3)(2,1)(2,4)(1,2)(1,3)(1,1)(1,4)

Sufficient condition for orthogonal Latin squares

Theorem

If $n \not\equiv 2 \pmod 4$, then there exist orthogonal Latin squares of order n

Proof: If n is odd, apply the odd construction seen a few pages before.
If $n \geq 2$ is a power of two, say $n = 2^i$, for $i \geq 2$, then we apply a recursive construction. Cases $i = 2, 3$ $(n = 4, 8)$ can be build directly. Then any $n = 2^i$, $i \geq 4$ can be build by induction from $n_1 = 4$ and $n_2 = 2^{i-2}$ using the product construction.
Finally, suppose that n is even, $n \not\equiv 2 \pmod 4$ and not a power of two. We can write $n = 2^i n'$ where $i \geq 2$ and n' is odd. In this case, apply the known constructions for $n_1 = 2^i$, $n_2 = n'$ and combine them using the product construction. $\square$

Mutually Orthogonal Latin Squares

Definition (MOLS)

A set of s Latin squares $L_1, \ldots, L_s$, of order n of order are *mutually orthogonal* if L_i and L_j are orthogonal for all $1 \le i < j \le s$. A set of s MOLS of order n is denoted s MOLS(n).

One important problem is to determine the maximum number of MOLS of order n, denoted $N(n)$.

The case $n = 1$ is not interesting as $N(1) = \infty$.

We have the following upper bound on $N(n)$.

Theorem

If $n > 1$ then $N(n) \le n - 1$.

Theorem

If $n > 1$ then $N(n) \leq n - 1$.

proof. Suppose $L_1, \ldots, L_s$ are s MOLS(n). Assume wlog that the first row of each of these squares is $(1, 2, \ldots, n)$. Note that $L_1(2,1), \ldots, L_s(2,1)$ must be all distinct since any pair of the form (x, x) already appeared in the first row of the superpositions of any two squares. Furthermore $L_i(2,1) \neq 1$ since $L_i(1,1) = 1$. Therefore, $L_1(2,1), \ldots, L_s(2,1)$ are s distinct elements of $\{2, \ldots, n\}$, so $s \leq n - 1$. □

The extreme case is interesting since $n - 1$ MOLS(n) correspond to an affine plane of order n!

MOLS and affine planes

Let $(X, \mathcal{A})$ be an affine plane of order n, i.e. a $(n^2, n, 1)$-BIBD.
We will show how to build $n-1$ MOLS(n) from it.
An affine plane has $n+1$ paralell classes, each with n blocks.
Example:

$X = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$\mathcal{A} = \{123, 456, 789, 147, 258, 369, 159, 267, 348, 168, 249, 357\}$

$A_{1,1}, A_{1,2}, A_{1,3}, A_{2,1}, A_{2,2}, A_{2,3}, A_{3,1}, A_{3,2}, A_{3,3}, A_{4,1}, A_{4,2}, A_{4,3}$

Define $L_x(i,j) = k$ if and only if $A_{n,i} \cap A_{n+1,j} \in A_{x,k}$

$$(1,1) : 1,\ (1,2) : 9,\ (1,3) : 5,$$
$$(2,1) : 6,\ (2,2) : 2,\ (2,3) : 7,$$
$$(3,1) : 8,\ (3,2) : 4,\ (3,3) : 3.$$

$L_1 =$

1	3	2
2	1	3
3	2	1

$L_2 =$

1	3	2
2	1	3
3	2	1

Remember $L_x(i,j) = k$ if and only if $A_{n,i} \cap A_{n+1,j} \in A_{x,k}$

$$(1,1):1,\ (1,2):9,\ (1,3):5,$$
$$(2,1):6,\ (2,2):2,\ (2,3):7,$$
$$(3,1):8,\ (3,2):4,\ (3,3):3.$$

$$L_1 = \begin{array}{|c|c|c|}\hline 1 & 3 & 2 \\ \hline 2 & 1 & 3 \\ \hline 3 & 2 & 1 \\ \hline \end{array} \quad L_2 = \begin{array}{|c|c|c|}\hline 1 & 3 & 2 \\ \hline 2 & 1 & 3 \\ \hline 3 & 2 & 1 \\ \hline \end{array}$$

Justification:

• L_x is a Latin square because row i cannot contain two equal symbols, since they come from different blocks in the same paralel class and the same is true for any column.

• Lets now prove that L_x and L_y are orthogonal. Consider k, ℓ; we need to find i, j such that $L_x(i,j) = k$ and $L_y(i,j) = \ell$. Now, there is a unique $z \in A_{x,k} \cap A_{y,\ell}$, since blocks in different parallel classes must intersect. There is a unique i such that $z \in A_{n,i}$ since these blocks form a parallel class; similarly there is a unique j such that $z \in A_{n+1,j}$. Thus,$L_x(i,j) = k$ and $L_x(i,j) = \ell$.

The construction can be reversed. Starting from $n-1$ MOLS(n), $L_1, \ldots, L_{n-1}$.
Build an affine plane with point set $X = \{1, \ldots, n\} \times \{1, \ldots, n\}$.
For $1 \leq x \leq n-1$ and $1 \leq k \leq n$

$$A_{x,k} = \{(i,j) : L_x(i,j) = k\}.$$

Define also

$$A_{n,k} = \{(k,j) : 1 \leq j \leq n\},$$
$$A_{n+1,k} = \{(i,k) : 1 \leq i \leq n\}.$$

We need to show this is a $(n^2, n, 1)$-BIBD. Clearly $|X| = n^2$ and each block has n points. Also the number of blocks is $n(n+1)$, so it is enough to show that every pair of points does not occur in more than one block. Suppose $\{(i_1, j_1), (i_2, j_2)\} \subseteq A_{x_1,k_1}$ and $\{(i_1, j_1), (i_2, j_2)\} \subseteq A_{x_2,k_2}$.
This means $L_{x_1}(i_1, j_1) = k_1$, $L_{x_1}(i_2, j_2) = k_1$, $L_{x_2}(i_1, j_1) = k_2$, $L_{x_2}(i_2, j_2) = k_2$. Because the Latin square are orthogonal we must have $x_1 = x_2$.

Equivalence: $n-1$ MOLS, projective and affine planes

Using the equivalence between $n-1$ MOLS and affine planes and a known equivalence between affine planes and projective planes, we get the following theorem.

Theorem

Let $n \geq 2$. The existence of one of the following designs implies the existence of the other two designs:

1. $n-1$ *MOLS*(n)
2. *an affine plane of order* n
3. *a projective plane of order* n

MOLS(n) for non prime power n

Theorem

If there exist s MOLS(n_i), $1 \leq i \leq \ell$, then there exist s MOLS(n), where $n = n_1 \times n_2 \times \ldots \times n_\ell$.

Proof. Generalize the direct product construction to deal with s MOLS and generalize the direct product to combine ℓ Latin squares. Then observe that the direct product preserves orthogonality. $\square$

MOLS(n) for non prime power n (continued)

Theorem (MacNeish's Theorem)

Suppose that n has prime power factorization $n = p_1^{e_1} \cdots p_\ell^{e_\ell}$, where p_i are different primes and $e_i \geq 1$ for $1 \leq i \leq \ell$. Let

$$s = \min\{p_i^{e_i} - 1 : 1 \leq i \leq \ell\}.$$

Then, there exists s MOLS(n).

Proof. There exist an affine plane of order $p_i^{e_i}$, for $1 \leq i \leq \ell$. So there exist $p_i^{e_i} - 1$ MOLS($p_i^{e_i}$). So there are s MOLS($p_i^{e_i}$) for $1 \leq i \leq \ell$. Apply the previous theorem to combine these MOLS. □

Orthogonal arrays and MOLS

Definition

An orthogonal array OA(t, k, n) is a $n^t \times k$ array with entries from a set of n symbols such that any subarray defined by t of its columns has every t-tuple of points in exactly one row.

0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

We'll show that OA$(2, k = s + 2, n)$ are equivalent to s MOLS(n).

Equivalence between OAs with $t = 2$ and MOLS

Take s MOLS(n): $L_1, \ldots, L_s$.
For each $1 \leq i, j, \leq n$, create a row $(i, j, L_1(i,j), \ldots, L_s(i,j))$, forming a $n^2 \times (s+2)$ array A
We need to show that in any two columns $1 \leq x < y \leq s+2$, each pair of symbols (a, b) occur in a row in those columns.
Case 1: $x = 1, y = 2$: Obvious by construction.
Case 2: $x = 1, y \geq 3$: Since L_y is a Latin square, there exist some j such that $L_y(a, j) = b$.
Case 3: $x = 2, y \geq 3$: Since L_y is a Latin square, there exist some i such that $L_y(i, a) = b$.
Case 4: $y > x \geq 3$: Since L_x and L_y are orthogonal, there exist unique i, j such that $L_x(i, j) = a$ and $L_y(i, j) = b$.
Therefore, A is an OA$(2, k, n)$. $\square$

Equivalence between OAs with $t = 2$ and MOLS (reversed)

We can reverse the construction to build MOLS from an OA.
Take A an OA$(2, k, n)$.
We build $s = k - 2$ MOLS as follows.
Use the first two columns as the index of rows and columns of the MOLS; each Latin square correspond to one of the columns $3, \ldots k$, and is defined as follows. For every row $1 \leq r \leq n^2$, of the OA and $1 \leq c \leq s$, take

$$L_c(A(r, 1), A(r, 2)) = A(r, c + 2).$$

We will show $L_1, \ldots, L_s$ form a set of s MOLS(n).
• L_c is a Latin square because of the orthogonal property of columns $(1, c)$ and $(2, c)$.
• L_c is orthogonal to L_d because of the orthogonality property of columns (c, d).
□

Equivalence between OAs with $t = 2$ and MOLS

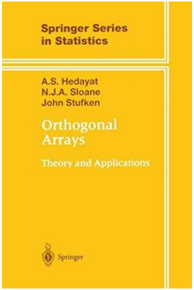
2 MOLS(3) equivalent to OA$(2, 4, 3)$:

A construction for OA$(t, q+1, q)$ for q prime power

Theorem (Bush (1952))

For $q \geq 2$ a prime power and $q \geq t-1 \geq 0$. Then there exists an $OA(t, q+1, q)$.

reference book on OAs:



Bush's construction

- Associate to each row a polynomial: $f(x) = a_0 + a_1x + \ldots a_{t-1}x^{t-1}$, for each possible tuple $(a_0, a_1, \cdots, a_{t-1}) \in F_q^t$.
- Associate to each of the first q columns a distinct element $\alpha \in F_q$.
- In the array position indexed by row $(a_0, a_1, \cdots, a_{t-1})$ and column α put the value $f(\alpha) = a_0 + a_1\alpha + \ldots a_{t-1}\alpha^{t-1}$.
- In the last row, put the value a_{t-1}.

Bush's construction: example for $q = 3$ and $t = 3$

	0	1	2	*
$0x^2 + 0x + 0$	0	0	0	0
$0x^2 + 0x + 1$	1	1	1	0
$0x^2 + 0x + 2$	2	2	2	0
$0x^2 + 1x + 0$	0	1	2	0
$0x^2 + 1x + 1$	1	2	0	0
$0x^2 + 1x + 2$	2	0	1	0
$0x^2 + 2x + 0$	0	2	1	0
$0x^2 + 2x + 1$	1	0	2	0
$0x^2 + 2x + 2$	2	1	0	0
$1x^2 + 0x + 0$	0	1	1	1
$1x^2 + 0x + 1$	1	2	2	1
$1x^2 + 0x + 2$	2	0	0	1
$1x^2 + 1x + 0$	0	1	0	1
$1x^2 + 1x + 1$	1	2	1	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

	0	1	2	*
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$1x^2 + 1x + 2$	2	0	2	1
$1x^2 + 2x + 0$	0	0	2	1
$1x^2 + 2x + 1$	1	1	0	1
$1x^2 + 2x + 2$	2	2	1	1
$2x^2 + 0x + 0$	0	2	1	2
$2x^2 + 0x + 1$	1	0	2	2
$2x^2 + 0x + 2$	2	1	0	2
$2x^2 + 1x + 0$	0	0	1	2
$2x^2 + 1x + 1$	1	1	2	2
$2x^2 + 1x + 2$	2	2	0	2
$2x^2 + 2x + 0$	0	1	0	2
$2x^2 + 2x + 1$	1	2	1	2
$2x^2 + 2x + 2$	2	0	2	2

Bush's construction: verification

We take a t-set of columns, consider the subarray determined by those columns. We need to verify that each t-tuple in F_q^t does not get repeated as a row.

If the t columns $c_1, \ldots, c_t$ are among the first q columns, consider tuple $(b_{c_1}, b_{c_2}, \ldots, b_{c_t})$.

We know that there is a unique polynomial p_i of degree $t-1$ such that $p_i(\alpha_{c_1}) = b_{c_1}, p_i(\alpha_{c_2}) = b_{c_2}, \ldots,$ and $p_i(\alpha_{c_t}) = b_{c_t}$.

Thus $(b_{c_1}, b_{c_2}, \ldots, b_{c_t})$ appears in a unique row i.

If $t-1$ columns $c_1, \ldots, c_{t-1}$ are among the first q columns, together with the last column. If there were two polynomials p_{i_1} and p_{i_2}, we get that $p = p_{i_1} - p_{i_2}$ has degree $t-2$ and $p(\alpha_{c_1}) = 0, \ldots, p(\alpha_{c_{t-1}}) = 0$. This is only possible of p is the identically null polynomial, and so $p_{i_1} = p_{i_2}$.

□

References

- HEDAYAT, SLOANE, STUFKEN, Orthogonal Arrays,
- STINSON, Combinatorial Designs: Constructions and Analysis, 2004.