Class-r hypercubes and related arrays

David Thomson

Carleton University, Ottawa ON

joint work with John Ethier, Melissa Huggan
Gary L. Mullen, Daniel Panario and Brett Stevens

Table of Contents

Latin squares

Latin squares

Definition. Let n be a positive integer. A Latin square of order n is an $n \times n$ array on n distinct symbols such that every symbol appears exactly once in every row and column.

$$\begin{array}{ccc} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{array}$$

Orthogonal Latin squares

Definition. Two Latin squares are orthogonal if, when superimposed, each of the n^2 distinct symbols appear exactly once.

$$L_1 = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix}, \; L_2 = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{pmatrix} \rightarrow$$

Orthogonal Latin squares

Definition. Two Latin squares are orthogonal if, when superimposed, each of the n^2 distinct symbols appear exactly once.

$$L_1 = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix},\ L_2 = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{pmatrix} \to \begin{pmatrix} (0,0) & (1,1) & (2,2) \\ (1,2) & (2,0) & (0,1) \\ (2,1) & (0,2) & (1,0) \end{pmatrix}$$

Sets of orthogonal Latin squares

A set $\{\mathcal{H}_1, \mathcal{H}_2, \ldots, \mathcal{H}_s\}$ of Latin squares is mutually orthogonal if $\mathcal{H}_i$ and $\mathcal{H}_j$ are orthogonal for any $1 \leq i < j \leq s$.

A set of mutually orthogonal Latin squares is called a set of MOLS.

Theorem. The maximum number of MOLS of order n is $n - 1$

Proof.

$$\begin{array}{ccc} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{array} \qquad \begin{array}{ccc} 0 & 1 & 2 \\ & & \\ & & \end{array}$$

Sets of orthogonal Latin squares

A set $\{\mathcal{H}_1, \mathcal{H}_2, \ldots, \mathcal{H}_s\}$ of Latin squares is mutually orthogonal if $\mathcal{H}_i$ and $\mathcal{H}_j$ are orthogonal for any $1 \leq i < j \leq s$.

A set of mutually orthogonal Latin squares is called a set of MOLS.

Theorem. The maximum number of MOLS of order n is $n - 1$

Proof.

0	1	2		0	1	2
1	2	0		2	0	1
2	0	1		1	2	0

We call a set of $n - 1$ MOLS complete.

MOLS of non-prime power order

Euler's conjecture (1782). (36 Officers problem): If $n \equiv 2 \pmod 4$, there is no pair of MOLS of order n.

Theorem. (Tarry - 1900 using "distributed computing") There is no pair of MOLS of order 6.

Theorem. If $n \neq 2, 6$, there are at least 2 MOLS of order n.

1. Bose and Shrikhande (1959) for some values of $n \geq 22$,
2. Parker (1959) $n = 10$,
3. Bose, Parker and Shrikhande (1960) for all $n > 6$.

Conjecture (Prime power conjecture for finite projective planes).
There exist a set of $n-1$ MOLS if and only if n is a prime power.

Two open questions.

Remark. The non-existence of a finite projective plane of order 10 was shown by Lam (using IDA computers). This was verified locally about 20 years later).

Question 1. Does there exist a triplet of MOLS of order 10? There does exist a pair of MOLS of order 10 along with a third Latin square that is orthogonal up to a 2×2 block.

Question 2. Prove or disprove there is a complete set of MOLS (equivalently, a finite projective plane) of your favourite non-prime-power order greater than 10 – prove this with or without a computer.

Constructing a complete set of MOLS

Theorem. There exist a complete set of MOLS of order n when n is a prime power.

Proof. Suppose n is a prime power and let $\mathbb{F}_n$ be the finite field of order n. For any $a \in \mathbb{F}_n^*$, construct

	$\cdots$	y	$\cdots$	
$\vdots$				
x		$ax + y$		
$\vdots$				

1. Row/column constraint is clear.
2. $(ax_1 + y_1, bx_1 + y_1) = (ax_2 + y_2, bx_2 + y_2)$ implies $a = b$.

Sudoku squares

Sudoku squares

Definition. An $n^2 \times n^2$ Sudoku square is a Latin square of order n^2 where the $n \times n$ subsquares at regular intervals also contain all n^2 symbols.

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

Linear construction of Sudoku squares

1. Order the elements of $\mathbb{F}_9$ in lexicographical order:

$$(0, 1, 2, \alpha, \alpha + 1, \alpha + 2, 2\alpha, 2\alpha + 1, 2\alpha + 2)$$

2. For any $a \in \mathbb{F}_9 \setminus \mathbb{F}_3$; i.e., $a = a_1\alpha + a_2, a_1 \neq 0$,

$a \cdot 0 + 0$	$a \cdot 0 + 1$	$a \cdot 0 + 2$						
$a \cdot 1 + 0$	$a \cdot 1 + 1$	$a \cdot 1 + 2$						
$a \cdot 2 + 0$	$a \cdot 2 + 1$	$a \cdot 2 + 2$						
$a \cdot (\alpha + 0)$	$\ddots$							
$a \cdot (\alpha + 1)$								
$a \cdot (\alpha + 2)$								
$a \cdot (2\alpha + 0)$								
$a \cdot (2\alpha + 1)$								
$a \cdot (2\alpha + 2)$								

From Latin squares to class r hypercubes

Extending Latin Squares

Natural extensions

What does it mean to be "Latin"?

Definition. Let d, n be non-negative integers. A hypercube of dimension d and order n is a $n \times n \times \cdots \times n$ array on n symbols such that each symbol occurs exactly once in each "hyper-row".

More natural than calling something a "hyper-row" is to say "each symbol occurs exactly once when fixing all but one coordinate".

Natural extensions

What does it mean to be "Latin"?

Definition. Let d, n be non-negative integers. A hypercube of dimension d and order n is a $n \times n \times \cdots \times n$ array on n symbols such that each symbol occurs exactly once in each "hyper-row".

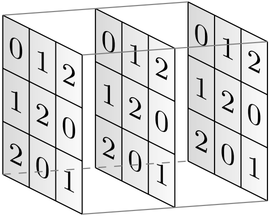
More natural than calling something a "hyper-row" is to say "each symbol occurs exactly once when fixing all but one coordinate".

Extending "Latin" to "type":

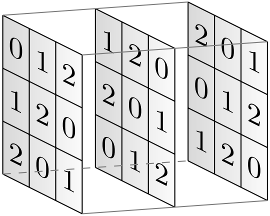
Definition. Let d, n, t be non-negative integers. A (d, n, t)-hypercube (of dimension d, order n and type t) is a $n \times n \times \cdots \times n$ array on n symbols such that, when fixing any t coordinates and allowing $d - t$ to vary, each symbol repeats exactly n^{d-t-1} times.

More results on these can be found in "Discrete Math using Latin Squares" by Laywine and Mullen.

Illustrating the type of a hypercube



has type 1.



has type 2.

Extending Sudoku squares - Class r hypercubes

Looking deeply at Sudoku

Recall. An $n^2 \times n^2$ Sudoku square is a Latin square of order n^2 where the $n \times n$ subsquares at regular intervals also contain all n^2 symbols.

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

Gary: What about hypercubes with alphabet size different from the order?

Definition. Let d, n, r, t be non-negative integers, $d, n, r > 0$. A (d, n, r, t)-hypercube (of dimension d, order n, *class* r and type t) is an $n \times n \times \cdots \times n$ (d-times) array on n^r distinct symbols such that, when fixing any t coordinates, each symbol repeats exactly n^{d-t}/n^r times.

Examples.

1. Latin squares are the

Definition. Let d, n, r, t be non-negative integers, $d, n, r > 0$. A (d, n, r, t)-hypercube (of dimension d, order n, *class* r and type t) is an $n \times n \times \cdots \times n$ (d-times) array on n^r distinct symbols such that, when fixing any t coordinates, each symbol repeats exactly n^{d-t}/n^r times.

Examples.

1. Latin squares are the $(2, n, 1, 1)$-hypercubes.
2. Sudoku squares are the

From the mind of Gary Mullen: high-class hypercubes

Definition. Let d, n, r, t be non-negative integers, $d, n, r > 0$. A (d, n, r, t)-hypercube (of dimension d, order n, *class* r and type t) is an $n \times n \times \cdots \times n$ (d-times) array on n^r distinct symbols such that, when fixing any t coordinates, each symbol repeats exactly n^{d-t}/n^r times.

Examples.

1. Latin squares are the $(2, n, 1, 1)$-hypercubes.
2. Sudoku squares are the $(2, 9, 1, 1)$-hypercubes containing 9 $(2, 3, 2, 0)$-hypercubes.

Two hypercubes are orthogonal if, when superimposed, each of the n^{2r} symbols appears exactly n^{d-2r} times.

A $(3, 3, 2, 1)$-hypercube

0	1	2	|	4	5	3	|	8	6	7
3	4	5	|	7	8	6	|	2	0	1
6	7	8	|	1	2	0	|	5	3	4

Our familiar construction using linear forms

Lemma. Let n be a power of a prime, let d, r be positive integers with $d \geq 2r$ and let $q = n^r$. Consider $\mathbb{F}_q$ as a vector space over $\mathbb{F}_n$ and define $c_j \in \mathbb{F}_q$ over $\mathbb{F}_n$, $j = 1, 2, \ldots, d$, such that any $t \leq r$ of them form a linearly independent set in $\mathbb{F}_q$ over $\mathbb{F}_n$. The hypercube constructed from the form $c_0x_0 + c_1x_1 + \cdots + c_{d-1}x_{d-1}$ is a (d, n, r, t)-hypercube.

Sketch. Count the number of solutions to the subsystems of

$$\begin{bmatrix} c_{00} & c_{01} & \cdots & c_{0,d-1} \\ c_{10} & c_{11} & \cdots & c_{1,d-1} \\ \vdots & & & \\ c_{r-1,0} & c_{r-1,1} & \cdots & c_{r-1,d-1} \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{d-1} \end{bmatrix} = \lambda \in \mathbb{F}_q,$$

where $c_i = \sum_{j=0}^{r-1} c_{ij}\alpha_j$ for some basis $\{\alpha_0, \ldots, \alpha_{r-1}\}$ for $\mathbb{F}_q$ over $\mathbb{F}_n$.

Connection to coding theory

Let H be an $r \times d$ matrix over $\mathbb{F}_n$ such that any t columns are linearly independent.

- H is the parity-check matrix of a linear code C over $\mathbb{F}_n$, that is $C = \mathrm{null}(H)$.
- C has minimum distance $t + 1$,
- $|C| = n^{d-t}$.

Moreover, when $d = 2r = 2t$, H is the parity check matrix of an MDS (maximum-distance separable) code.

Conjecture. All linear MDS codes are known, most of them are Reed-Solomon codes.

Orthogonal hypercubes of dimension $d = 2r$

Pairs of orthogonal hypercubes

Remark. Let H_1, H_2 be parity-check matrices of linear $[2r, r, r]$-MDS codes over $\mathbb{F}_q$.

$$\begin{bmatrix} - & H_1 & - \\ - & H_2 & - \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{2r} \end{bmatrix} = \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_{2r} \end{bmatrix}.$$

Proposition. If the concatenated matrix $\begin{bmatrix} H_1 \\ H_2 \end{bmatrix}$ is invertible, then $\mathcal{H}_1$ and $\mathcal{H}_2$ are orthogonal.

Proposition. Suppose H_1 and H_2 are in systematic form; i.e., $H_i = [I_r | A_i]$ and that A_1, A_2 have no 0 entries, then H_1 and H_2 are orthogonal if and only if $A_1 - A_2$ is invertible.

Problems

Theorem. Let $r = 2$ and let n be either an odd prime power or $n = 2^{2k}$ for some k. Then there exists a complete set of $(n-1)^2$ mutually orthogonal $(4, n, 2, 2)$-hypercubes.

Theorem. Let n be a prime power, for any $r < n$, there exists a set of $n - 1$ mutually orthogonal $(2r, n, r, r)$-hypercubes.

Other results. by Droz and Mullen appear for $r \leq 4$.

Open Problem. Investigate Reed-Solomon codes in systematic form whose redundant portion admit no 0 entries. Determine when two such matrices have invertible difference.

Constructions in higher dimension

d-dimensional Sudoku cubes. Suppose I want to inscribe a $n^d \times \cdots \times n^d$ cube with $n \times \cdots \times n$ regularly spaced subcubes. These are just $(d, n, n^d, d-1)$ (Latin) hypercubes comprising $(d, n, d, 0)$-hypercubes. Picking the linear form

$$c_1 x_1 + \cdots + c_d x_d,$$

with $\{c_1, \ldots, c_d\}$ linearly independent is sufficient.

Punch-line.

- Analyzing linear forms comes into play,
- This leads to a coding theory
- This actually yields much more structure we can explore...

No time – some other talk: Coverage

Latin squares are orthogonal arrays

Sudokus coordinatized by AG(4,3)

Hypercubes coordinatized by AG(d-1,q)

HyperSudokus from linear forms and codes

Connections to (t, m, s)-nets and ordered orthogonal arrays

Recap

Finishing off...

This work was inspired by and joint with Gary Mullen and touched on 2 papers:

- J. Ethier, G. L. Mullen, D. Panario and D. Thomson, Orthogonal hypercubes of class r, JCTA (2012).
- M. Huggan, G. L. Mullen, B. Stevens and D. Thomson, Generalized Sudoku arrays with strong regularity conditions, DCC (2016).

Finishing off...

This work was inspired by and joint with Gary Mullen and touched on 2 papers:

- J. Ethier, G. L. Mullen, D. Panario and D. Thomson, Orthogonal hypercubes of class r, JCTA (2012).
- M. Huggan, G. L. Mullen, B. Stevens and D. Thomson, Generalized Sudoku arrays with strong regularity conditions, DCC (2016).

But I owe Gary much more than that:

- We have 6 joint papers (so far...),
- As my editor for FFA, DCC, HFF and many other acronyms,
- My first job out of PhD was at Penn State.
- He got me tickets to the Penn State vs. Ohio State game in 2012,

And many more great conversations about mathematics (or whatever!) over the years.

Thank you Gary, for 70 years of beautiful mathematical problems, with many more to come

Teeba – Photographer: Bev Mullen