Latin squares and beyond, What's wrong with six?

How an incorrect proof of a century old conjecture was fixed after several decades.

Grad Student Seminar,
Brian Mintz,
Dartmouth 2024

Website with slides
(and more)

Latin Squares

- **Definition**: A "Latin square" is a $n \times n$ array of numbers from the set $S = \{1, 2, 3, \ldots, n\}$ where each element appears exactly once in each row and column.

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix} \qquad \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \\ 3 & 5 & 4 & 2 & 1 \\ 4 & 1 & 5 & 3 & 2 \\ 5 & 3 & 2 & 1 & 4 \end{bmatrix} \qquad \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}$$

- Note rearranging the rows or columns by any permutation will result in another Latin square. Thus one can permute any Latin square into its **reduced** form, where the first row and column are in increasing order.

- This can be generalized to cubes, hypercubes, in a similar fashion.

- Sudoku are 9x9 Latin squares with an added constraint.

Basic Results:

- Any group's multiplication table forms a Latin square (inverses guarantee this). However, arbitrary Latin squares give the multiplication table of a **quasigroup** (not a group, as they may not have an identity or be associative). For example, the middle table has 3*(4*5)=3*2=5 which is not (3*4)*5=2*5=3.

- Consequently, there is at least one for all n, e.g. the table of $\mathbb{Z}/n\mathbb{Z}$.

Basic Results:

- Any group's multiplication table forms a Latin square (inverses guarantee this). However, arbitrary Latin squares give the multiplication table of a **quasigroup** (not a group, as they may not have an identity or be associative). For example, the middle table has 3*(4*5)=3*2=5 which is not (3*4)*5=2*5=3.

- Consequently, there is at least one for all n, e.g. the table of $\mathbb{Z}/n\mathbb{Z}$.

- The number of reduced Latin squares does not have a (simple) known closed formula, but some bounds are known. Up to symmetry, the number of squares is given by A000315: 1, 1, 1, 4, 56, 9408, 16942080, …

$$\prod_{k=1}^{n} (k!)^{n/k} \geq L_n \geq \frac{(n!)^{2n}}{n^{n^2}}.$$

- Completing partial Latin squares is known to be NP-complete

Euler Squares

- **Definition**: An "Euler," or "Graeco-Latin" square, is an $n \times n$ array of pairs from the set $S^2 = \{1, 2, 3, \ldots, n\}^2$ where the array formed by taking the first component of each cell is a Latin square, as well as the second component, and every pair in S^2 is used. This property of a pair of Latin squares is called **orthogonality**.

Aα	Bγ	Cβ
Bβ	Cα	Aγ
Cγ	Aβ	Bα

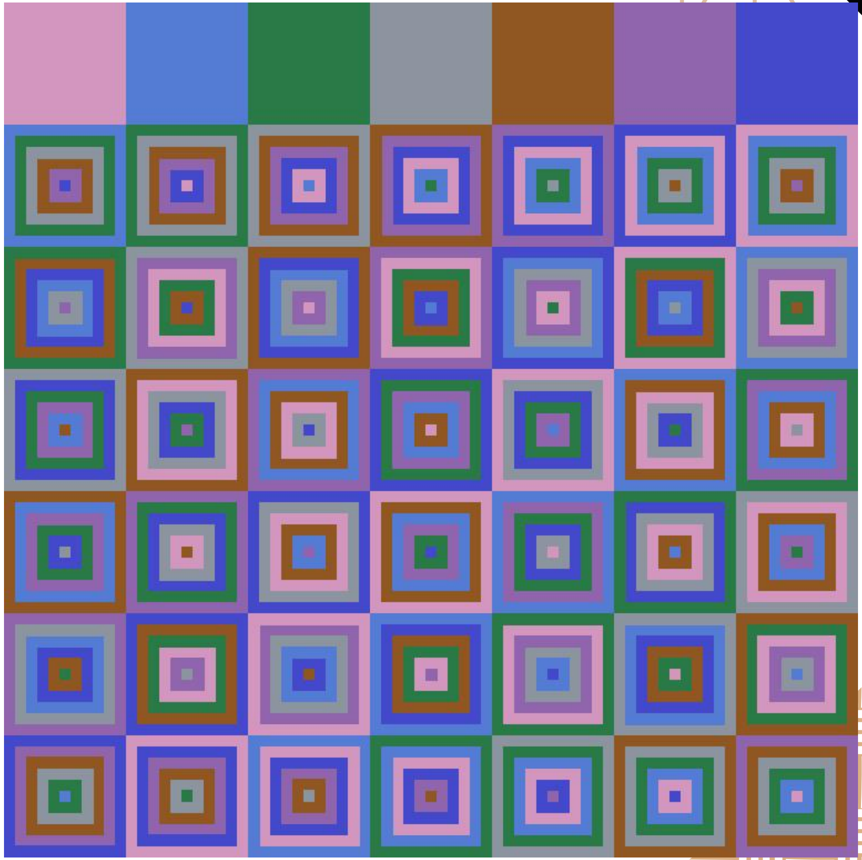
Aα	Bγ	Cδ	Dβ
Bβ	Aδ	Dγ	Cα
Cγ	Dα	Aβ	Bδ
Dδ	Cβ	Bα	Aγ

Stained glass art display in Kemeny Hall, Dartmouth Math department

Example: Arrange the sixteen face cards (ace, jack, queen, and king for each of the four suits: spades, hearts, diamonds, and clubs) such that every row/column has all the face values and suits (Jaques Ozanam, 1725).

Higher orders

- This can be extended to larger sets of Latin squares, where each pair is mutually orthogonal. The maximum size of such a set is given by A001438: 1, 2, 3, 4, 1, 6, 7, 8, then it’s unknown!



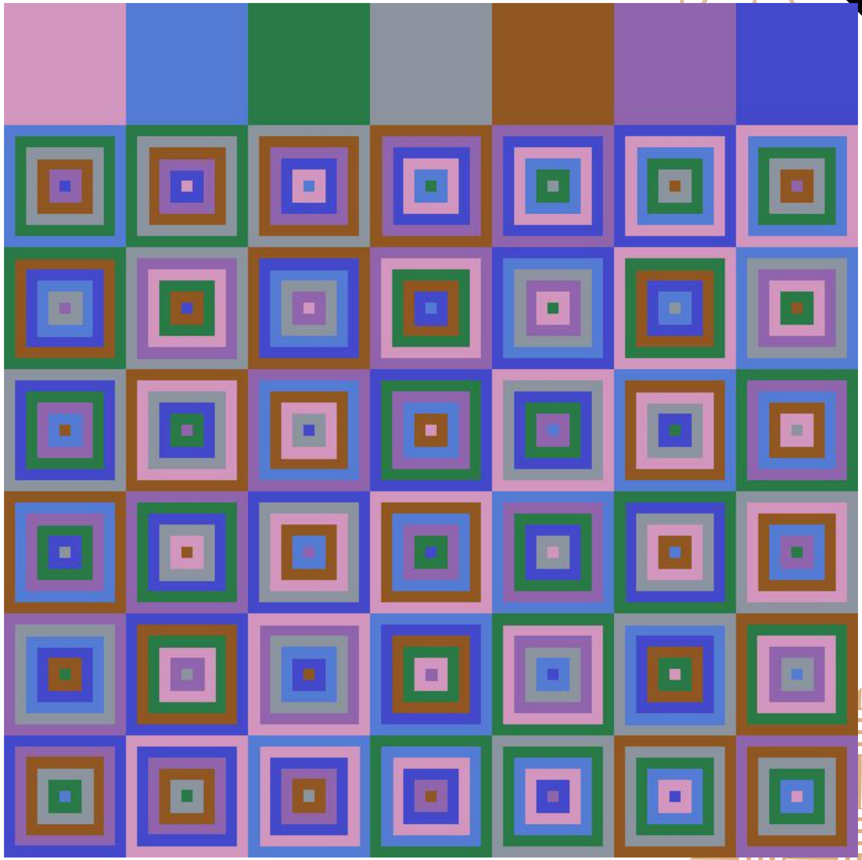
https://puzzlewocky.com/math-fun/graeco-latin-squares/

Higher orders

- This can be extended to larger sets of Latin squares, where each pair is mutually orthogonal. The maximum size of such a set is given by A001438: 1, 2, 3, 4, 1, 6, 7, 8, then it's unknown!

- An upper bound on this maximum is n-1.

Proof: Permute so the first row of each is 1, 2, … n. Then the first cells of the second rows are all distinct. If there was a duplicate r, then the pair (r,r) would appear in this cell of the combined square, as well as in the rth entry of the first row, contradicting orthogonality. Further, 1 can't be in the first cell of any of the second rows, or else it would occur twice in the first column of that square contradicting the Latin property.



https://puzzlewocky.com/math-fun/graeco-latin-squares/

Basic Results:

- Impossible for n=2. There are only two Latin squares with n=2, and they don't work.

- Existence for all odd values of n:

$$E_{i,j} = (i + j, i + 2j) \bmod n$$

Each component forms a Latin square, as subsequent columns are shifted by 1 in the first, and 2 in the second (and n is odd). They are orthogonal, as we can solve $\mathrm{E}_{i,\mathrm{j}} = (a, b) \bmod n$ with $\mathrm{j} = b - a,\ i = 2a - b$.

i \ j	0	1	2	3	4	5	6
0	0,0	1,2	2,4	3,6	4,1	5,3	6,5
1	1,1	2,3	3,5	4,0	5,2	6,4	0,6
2	2,2	3,4	4,6	5,1	6,3	0,5	1,0
3	3,3	4,5	5,0	6,2	0,4	1,6	2,1
4	4,4	5,6	6,1	0,3	1,5	2,0	3,2
5	5,5	6,0	0,2	1,4	2,6	3,1	4,3
6	6,6	0,1	1,3	2,5	3,0	4,2	5,4

Basic Results:

- Impossible for n=2. There are only two Latin squares with n=2, and they don't work.

- Existence for all odd values of n:

$$E_{i,j} = (i + j, i + 2j) \bmod n$$

Each component forms a Latin square, as subsequent columns are shifted by 1 in the first, and 2 in the second (and n is odd). They are orthogonal, as we can solve $\mathrm{E}_{i,\mathrm{j}} = (a, b) \bmod n$ with $\mathrm{j} = b - a,\ i = 2a - b$.

i \ j	0	1	2	3	4	5	6
0	0,0	1,2	2,4	3,6	4,1	5,3	6,5
1	1,1	2,3	3,5	4,0	5,2	6,4	0,6
2	2,2	3,4	4,6	5,1	6,3	0,5	1,0
3	3,3	4,5	5,0	6,2	0,4	1,6	2,1
4	4,4	5,6	6,1	0,3	1,5	2,0	3,2
5	5,5	6,0	0,2	1,4	2,6	3,1	4,3
6	6,6	0,1	1,3	2,5	3,0	4,2	5,4

- Euler had a construction for $n = 4k$, but couldn't crack $n = 6$. And if Euler can't do it, there's a good chance it's impossible. This led to the 1779 conjecture that there are no Euler squares when $n = 4k + 2$ for some natural number k.

History Time!

- In 1901, Gaston Tarry manually checked all Latin squares with n=6 and confirmed there were no solutions. They even published a proof of the conjecture…

Tarry

History Time!

- In 1901, Gaston Tarry manually checked all Latin squares with n=6 and confirmed there were no solutions. They even published a proof of the conjecture…

- But decades later, in 1959, Raj Bose found a 22x22 counterexample, dubbed an "Euler Spoiler." Soon soon after they found a 10x10 example, with the help of some other mathematicians and early computers, ultimately finding a construction for every single n=4k+2!

Tarry

The Conjecture couldn't have been more wrong! 6 is the **ONLY** number, other than 2, that doesn't have an Euler square.

Bose

Applications

- Tournament design: each day (row), players are matched to compete in locations (column) according to an Euler square. All pairs are tested against each other.

- Design of experiments – blocking to control for confounding variables. For example, each day (row) you might test some of each batch (column) according to a Latin square to account for the two effects. Additional variables are taken into account with higher order squares.

Applications

- Tournament design: each day (row), players are matched to compete in locations (column) according to an Euler square. All pairs are tested against each other.

- Design of experiments – blocking to control for confounding variables. For example, each day (row) you might test some of each batch (column) according to a Latin square to account for the two effects. Additional variables are taken into account with higher order squares.

- Some things I didn’t dive into the details on:
  - Euler squares are in bijection with finite projective planes.
  - One can efficiently sample multidimensional distributions, for example in Monte Carlo simulations, according to a Latin Hypercube.

- And the fun ones…

Magic Squares!

- **Definition**: A “magic square” is an $n \times n$ array of the numbers $1, 2, 3, \ldots, n^2$ where every row and every column sums to the same number.

- One can use an Euler square to construct a magic square as follows: Take the two alphabets 0, 1, 2, $\ldots n-1$, then replace the cell label (a, b) with $a + bn$.

i \ j	0	1	2	3	4	5	6
0	0,0	1,2	2,4	3,6	4,1	5,3	6,5
1	1,1	2,3	3,5	4,0	5,2	6,4	0,6
2	2,2	3,4	4,6	5,1	6,3	0,5	1,0
3	3,3	4,5	5,0	6,2	0,4	1,6	2,1
4	4,4	5,6	6,1	0,3	1,5	2,0	3,2
5	5,5	6,0	0,2	1,4	2,6	3,1	4,3
6	6,6	0,1	1,3	2,5	3,0	4,2	5,4

$\rightarrow$

0	15	30	45	11	26	41
8	23	38	4	19	34	42
16	31	46	12	27	35	1
24	39	5	20	28	43	9
32	47	13	21	36	2	17
40	6	14	29	44	10	25
48	7	22	37	3	18	33

Magic Squares!

- **Definition**: A "magic square" is an $n \times n$ array of the numbers $1, 2, 3, \dots, n^2$ where every row and every column sums to the same number.

- One can use an Euler square to construct a magic square as follows: Take the two alphabets 0, 1, 2, $\dots n - 1$, then replace the cell label (a, b) with $a + bn$.

- This is the base-n representation of the numbers from 0 to $n^2 - 1$, so includes all of them uniquely. Since this is a Latin square in a and also in b, each row or column has the same set of values, so summing them gives the same result!

0	15	30	45	11	26	41
8	23	38	4	19	34	42
16	31	46	12	27	35	1
24	39	5	20	28	43	9
32	47	13	21	36	2	17
40	6	14	29	44	10	25
48	7	22	37	3	18	33

Error Correcting Codes

With n-2 MOLS of size $q \times q$, we can use n letters from the set {0,1, 2, …, q} to encode q^2 symbols and correct up to $\frac{n-1}{2}$ errors!

First make a $q \times q$ table symbols. To encode the symbol in location (i, j), use the codeword

$$\left(i, j,\ L_{i,j}^{1},\ L_{i,j}^{1}, \dots ,\ L_{i,j}^{n-3},\ L_{i,j}^{n-2}\right)$$

Error Correcting Codes

With n-2 MOLS of size $q \times q$, we can use n letters from the set {0,1, 2, …, q} to encode q^2 symbols and correct up to $\frac{n-1}{2}$ errors!

First make a $q \times q$ table symbols. To encode the symbol in location (i, j), use the codeword

$$\left(i, j,\ L^1_{i,j},\ L^1_{i,j}, \ldots,\ L^{n-3}_{i,j},\ L^{n-2}_{i,j}\right)$$

A	F	K	P	U
B	G	L	Q	V
C	H	M	R	W
D	I	N	S	X
E	J	O	T	Y

1	2	3	4	5
2	3	4	5	1
3	4	5	1	2
4	5	1	2	3
5	1	2	3	4

L^1

1	2	3	4	5
3	4	5	1	2
5	1	2	3	4
2	3	4	5	1
4	5	1	2	3

L^2

1	2	3	4	5
5	1	2	3	4
4	5	1	2	3
3	4	5	1	2
2	3	4	5	1

L^3

1	2	3	4	5
4	5	1	2	3
2	3	4	5	1
5	1	2	3	4
3	4	5	1	2

L^4

For example, L is in position (0,2), so the codeword is (0,2,4,5,2,1).

Error Correcting Codes

With n-2 MOLS of size $q \times q$, we can use n letters from the set {0,1, 2, …, q} to encode q^2 symbols and correct up to $\frac{n-1}{2}$ errors!

First make a $q \times q$ table symbols. To encode the symbol in location (i, j), use the codeword

$$\left(i, j,\ L^1_{i,j},\ L^1_{i,j}, \dots,\ L^{n-3}_{i,j},\ L^{n-2}_{i,j}\right)$$

A	F	K	P	U
B	G	L	Q	V
C	H	M	R	W
D	I	N	S	X
E	J	O	T	Y

L^1

1	2	3	4	5
2	3	4	5	1
3	4	5	1	2
4	5	1	2	3
5	1	2	3	4

L^2

1	2	3	4	5
3	4	5	1	2
5	1	2	3	4
2	3	4	5	1
4	5	1	2	3

L^3

1	2	3	4	5
5	1	2	3	4
4	5	1	2	3
3	4	5	1	2
2	3	4	5	1

L^4

1	2	3	4	5
4	5	1	2	3
2	3	4	5	1
5	1	2	3	4
3	4	5	1	2

For example, L is in position (0,2), so the codeword is (0,2,4,5,2,1).

Suppose we only got the information (-,-,4,-,-,1). This means the encoded value corresponds to a 4 in L^1 and a 1 in L^4. Because the pair are orthogonal, (4,1) occurs exactly once, in position (0,2), so that must be the location of the secret!

Error Correcting Codes

With n-2 MOLS of size $q \times q$, we can use n letters from the set {0,1, 2, …, q} to encode q^2 symbols and correct up to $\frac{n-1}{2}$ errors!

First make a $q \times q$ table symbols. To encode the symbol in location (i, j), use the codeword

$$\left(i, j,\ L_{i,j}^{1},\ L_{i,j}^{1}, \dots ,\ L_{i,j}^{n-3},\ L_{i,j}^{n-2}\right)$$

Note that just two pieces of information are sufficient to determine (i, j). This is clear if those correct values are i and j themselves. If you know i, or j, and any $L_{i,j}^{k}$, then the fact that L^k is a Latin square allows you to determine the the other value. If you know $L_{i,j}^{k}$ and $L_{i,j}^{\ell}$, then orthogonality guarantees that the pair $(L_{i,j}^{k}, L_{i,j}^{\ell})$ appears in the combined square, and it only appears in position (i, j).

Because of this, any two codewords overlap in no more than two positions, or else they would share two pieces of information and therefore encode the same (i, j) and thus be identical.

Therefore the hamming distance between any two codewords is n-1, so if the received word has less than $\frac{n-1}{2}$ errors, it must be a corrupted version of the closer of the two code words! When q is a power of a prime, this achieves a theoretical upper bound!

Thanks!

References

1. "Euler Squares." Numberphile, YouTube - https://www.youtube.com/watch?v=qu04xLNrk94
2. "The Korean king's magic square: a brilliant algorithm in a k-drama (plus geomagic squares)." Mathologer, YouTube - https://www.youtube.com/watch?v=FANbncTMCGc
3. Dénes, J.; Keedwell, A. D. (1974), Latin squares and their applications, New York-London: Academic Press
4. https://www.whitman.edu/mathematics/cgt_online/book/section04.03.html
5. Padraic Bartlett, Lecture 8: Error-Correcting Codes and Latin Squares, Part 2/2, Week 3 Mathcamp 2012. https://web.math.ucsb.edu/~padraic/mathcamp_2012/latin_squares/MC2012_LatinSquares_lecture8.pdf