Southwest State University

# ENUMERATION OF ISOTOPY CLASSES OF DIAGONAL LATIN SQUARES OF SMALL ORDER USING VOLUNTEER COMPUTING

**Eduard Vatutin, Alexey Belyshev, Stepan Kochemazov, Oleg Zaikin and Natalia Nikitina**

Moscow, 2018

# What is Latin square?

$$A = \|a_{ij}\|$$

$$i, j = \overline{1, N}$$

$$N = |S|$$

$$S = \{0, 1, 2, ..., N-1\}$$

$$\forall i, j, k = \overline{1, N}, j \neq k : (a_{ij} \neq a_{ik}) \wedge (a_{ji} \neq a_{ki})$$

$$\forall i, j = \overline{1, N}, i \neq j : (a_{ii} \neq a_{jj}) \wedge (a_{N-i+1,\, N-i+1} \neq a_{N-j+1,\, N-j+1})$$

$$\begin{pmatrix}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
1 & 2 & 9 & 4 & 3 & 6 & 7 & 5 & 0 & 8 \\
2 & 9 & 3 & 1 & 7 & 0 & 5 & 8 & 4 & 6 \\
3 & 4 & 1 & 2 & 8 & 7 & 9 & 6 & 5 & 0 \\
4 & 3 & 5 & 9 & 2 & 1 & 8 & 0 & 6 & 7 \\
5 & 6 & 4 & 8 & 1 & 2 & 0 & 9 & 7 & 3 \\
6 & 5 & 8 & 7 & 0 & 3 & 2 & 1 & 9 & 4 \\
7 & 8 & 6 & 0 & 9 & 4 & 1 & 2 & 3 & 5 \\
8 & 7 & 0 & 5 & 6 & 9 & 3 & 4 & 1 & 2 \\
9 & 0 & 7 & 6 & 5 & 8 & 4 & 3 & 2 & 1
\end{pmatrix}$$

Normalized LS of order 10

$$N! \times (N-1)!$$

$$\begin{pmatrix}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
7 & 2 & 4 & 9 & 0 & 6 & 5 & 1 & 3 & 8 \\
8 & 3 & 6 & 7 & 5 & 9 & 0 & 2 & 4 & 1 \\
2 & 6 & 8 & 5 & 1 & 7 & 4 & 0 & 9 & 3 \\
5 & 8 & 9 & 1 & 7 & 0 & 3 & 4 & 6 & 2 \\
9 & 4 & 1 & 2 & 8 & 3 & 7 & 6 & 0 & 5 \\
4 & 7 & 5 & 6 & 9 & 1 & 8 & 3 & 2 & 0 \\
3 & 0 & 7 & 8 & 2 & 4 & 1 & 9 & 5 & 6 \\
6 & 5 & 0 & 4 & 3 & 2 & 9 & 8 & 1 & 7 \\
1 & 9 & 3 & 0 & 6 & 8 & 2 & 5 & 7 & 4
\end{pmatrix}$$

Normalized DLS of order 10

$$(N-1)!$$

# Why is this interesting?

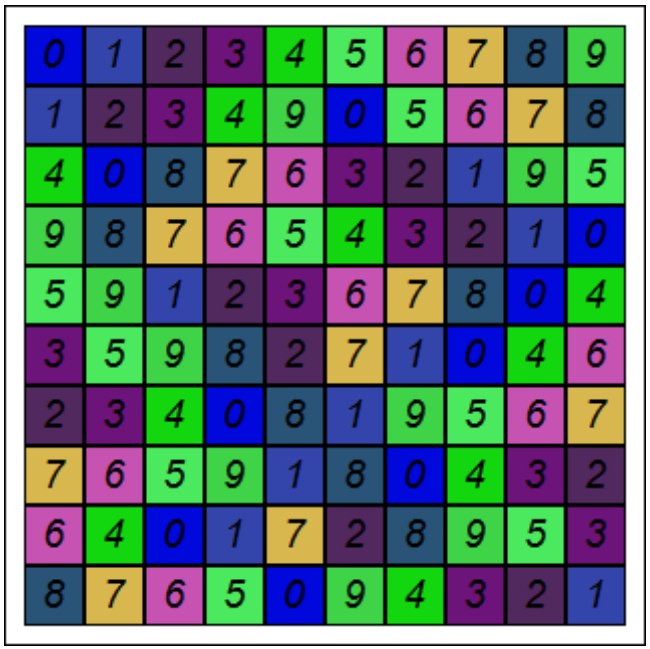
Applied problems:

- experiment planning
- cryptography
- error correcting codes
- scheduling
- algebra, combinatorics, statistics, ...

Mathematical problems:

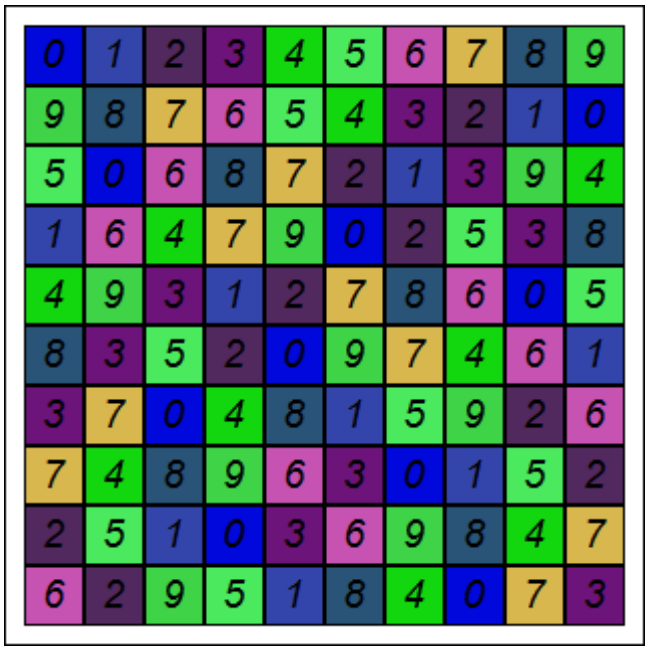
- **existence of a triple of MOLS / MODLS (combinatorial structures collecting)**
- **generating functions**
- **asymptotic behavior of combinatorial characteristics based on DLSs (OEIS)**
- number theory (relations between different fields of knowledge)
- magic squares
- Sudoku (LS of order 9 with additional constraints)

# Isomorphic decisions and canonical forms (CFs)



| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 1 | 2 | 3 | 4 | 9 | 0 | 5 | 6 | 7 | 8 |
| 4 | 0 | 8 | 7 | 6 | 3 | 2 | 1 | 9 | 5 |
| 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| 5 | 9 | 1 | 2 | 3 | 6 | 7 | 8 | 0 | 4 |
| 3 | 5 | 9 | 8 | 2 | 7 | 1 | 0 | 4 | 6 |
| 2 | 3 | 4 | 0 | 8 | 1 | 9 | 5 | 6 | 7 |
| 7 | 6 | 5 | 9 | 1 | 8 | 0 | 4 | 3 | 2 |
| 6 | 4 | 0 | 1 | 7 | 2 | 8 | 9 | 5 | 3 |
| 8 | 7 | 6 | 5 | 0 | 9 | 4 | 3 | 2 | 1 |

Orthogonality characteristic 74,
citerra
(**world record, 2016**)



| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| 5 | 0 | 6 | 8 | 7 | 2 | 1 | 3 | 9 | 4 |
| 1 | 6 | 4 | 7 | 9 | 0 | 2 | 5 | 3 | 8 |
| 4 | 9 | 3 | 1 | 2 | 7 | 8 | 6 | 0 | 5 |
| 8 | 3 | 5 | 2 | 0 | 9 | 7 | 4 | 6 | 1 |
| 3 | 7 | 0 | 4 | 8 | 1 | 5 | 9 | 2 | 6 |
| 7 | 4 | 8 | 9 | 6 | 3 | 0 | 1 | 5 | 2 |
| 2 | 5 | 1 | 0 | 3 | 6 | 9 | 8 | 4 | 7 |
| 6 | 2 | 9 | 5 | 1 | 8 | 4 | 0 | 7 | 3 |

Orthogonality characteristic 74,
evatutin (2017)

- Can characteristic value be increased? It is open question, we are trying...
- Are decisions differ?
- Are decisions have special properties?

# Latin squares equivalent transformations

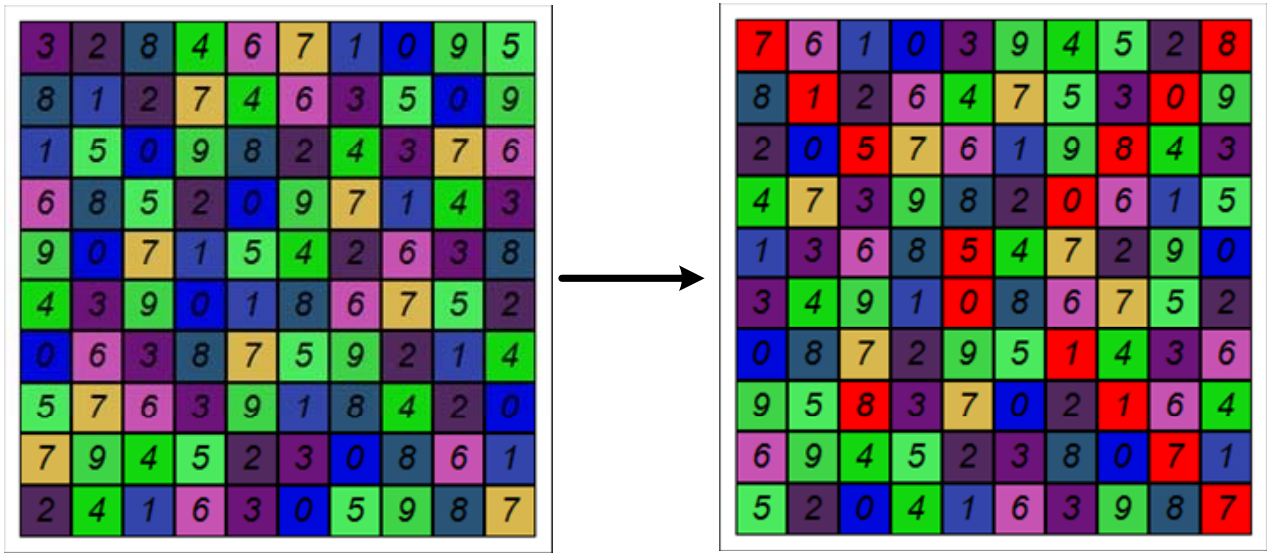
Latin squares:

- substitution of values (any of N!)
- permutation of rows (any of N!)
- permutation of columns (any of N!)
- rotations
- transposes
- reflections
- parastrofic transformations (isotopy classes vs. main classes)

Diagonal Latin squares:

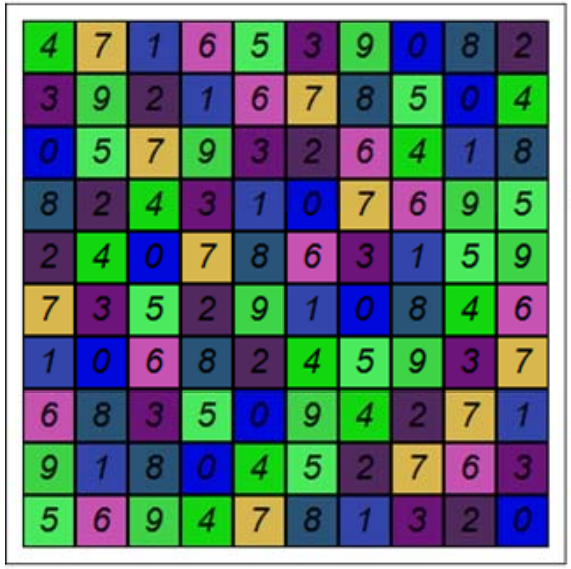
- not of all listed above transformations are allowed due to requirement for unique diagonal elements

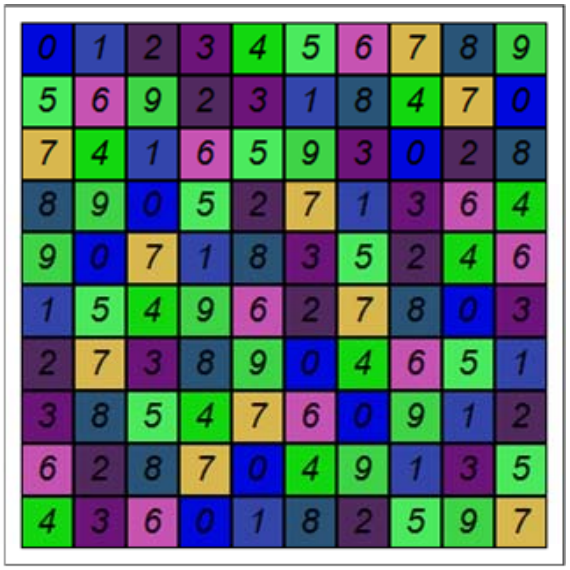
$$(x, y, v) \rightarrow (x, v, y)$$

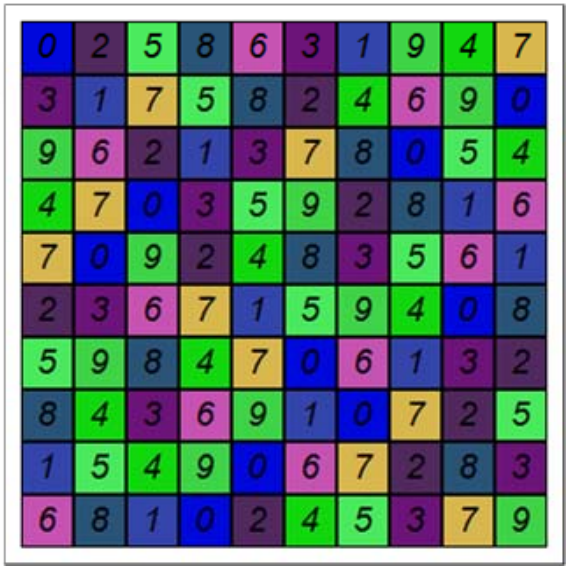


# Normalization example

$$P_1 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 2 & 9 & 5 & 0 & 4 & 3 & 1 & 8 & 6 \end{pmatrix}$$





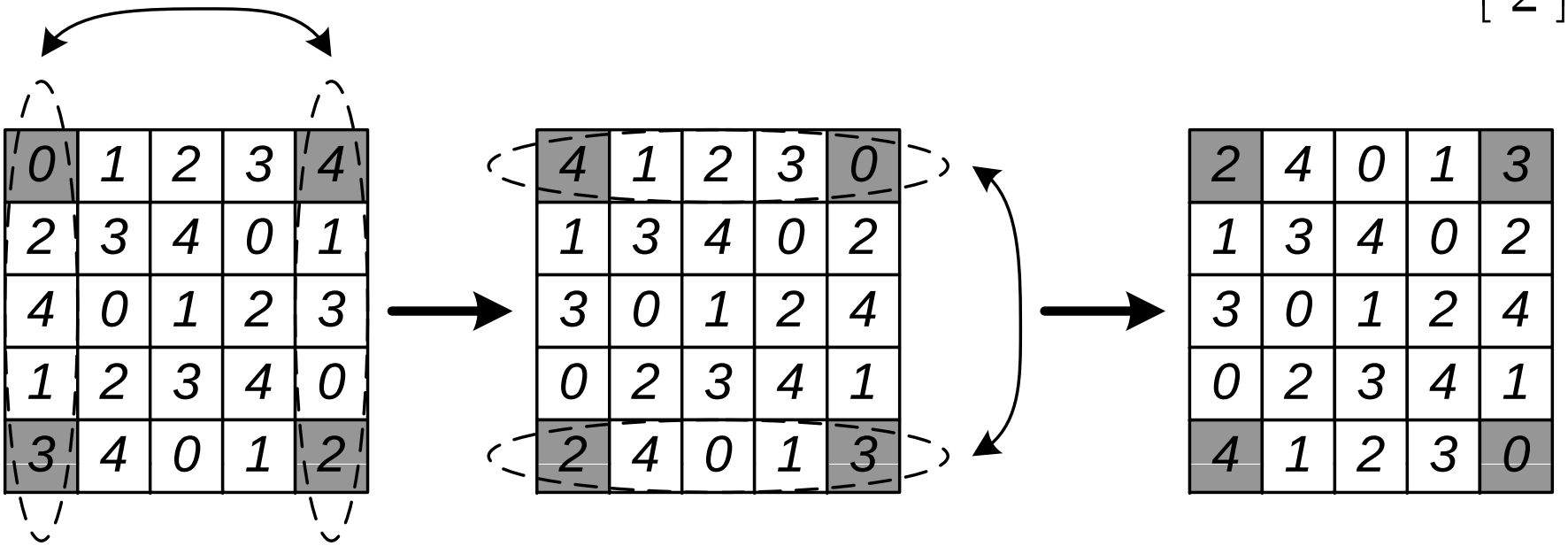


$$P_2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 5 & 7 & 3 & 0 & 6 & 8 & 2 & 4 & 1 \end{pmatrix}$$

## M1 transformation example

$$C_1 = 2^m$$

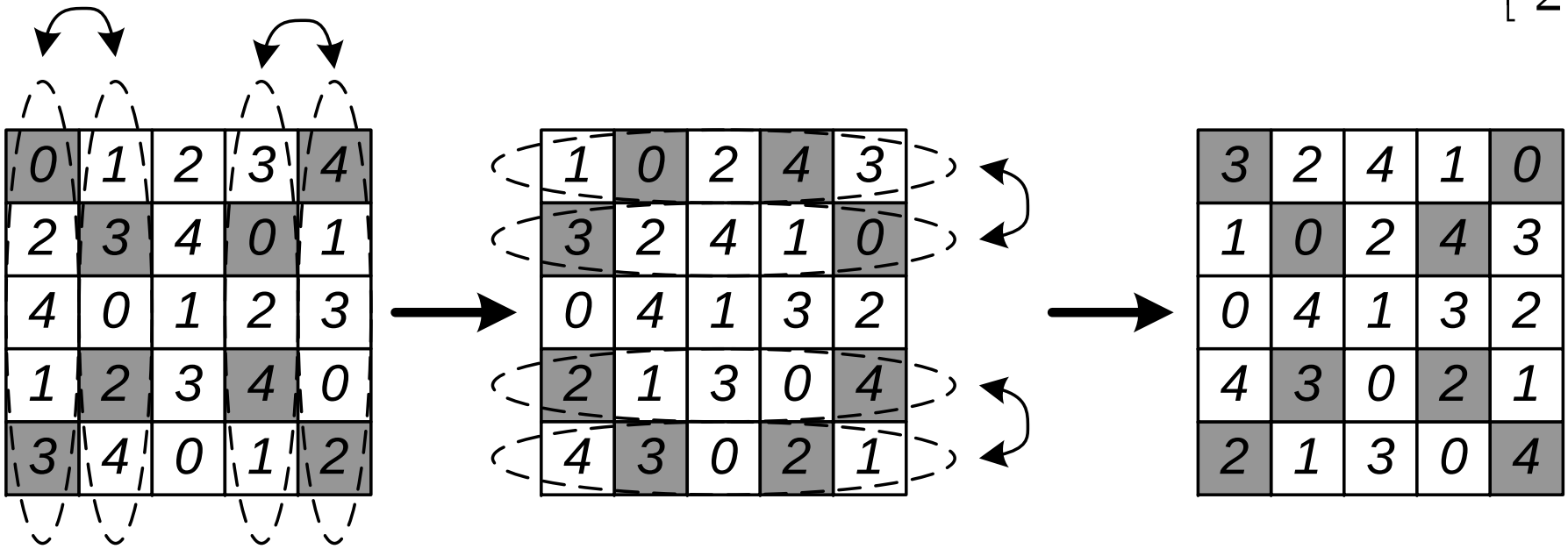
$$m = \left\lfloor \frac{N}{2} \right\rfloor$$



## M2 transformation example

$$C_2 = m!$$

$$m = \left\lfloor \frac{N}{2} \right\rfloor$$



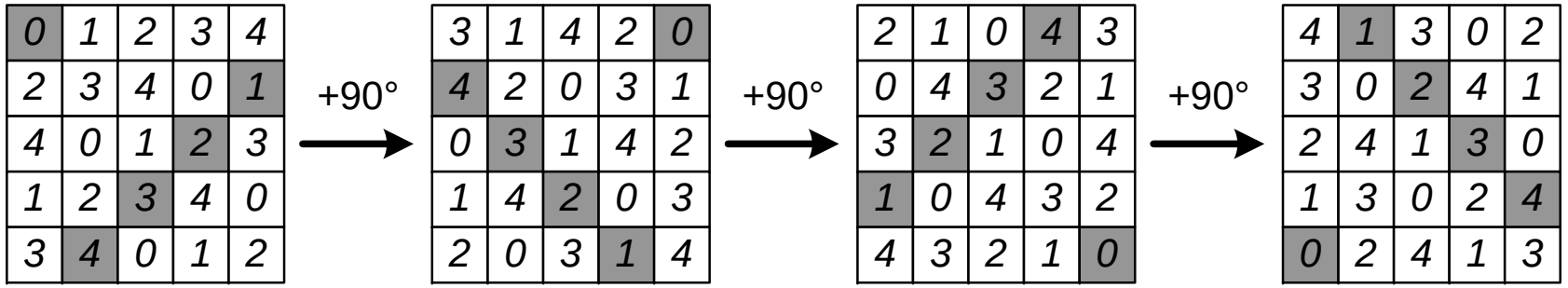

- M-transformations are equivalent to the special permutations (M-permutations) of rows and corresponding columns:

$$a_i + a_{N-1-i} = N-1, \; i = \overline{0, \left\lfloor \frac{N}{2} \right\rfloor}$$

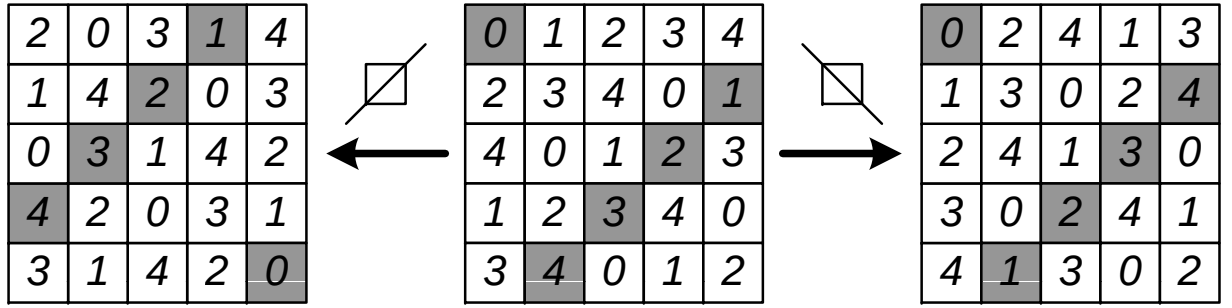
# Rotations, transposes, reflections



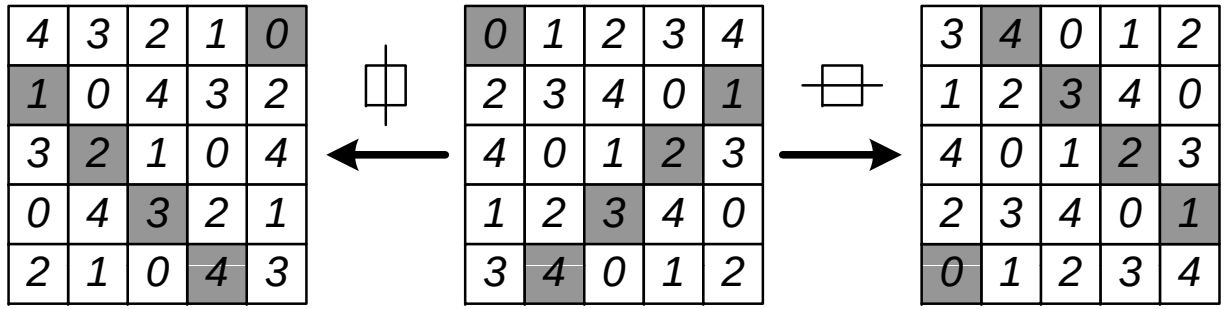
a)




b)



c)



$$C = C_M \cdot C_3 = 2^m \cdot m! \cdot 4 \quad (C = 15\,360 \quad for \quad N = 10)$$

# Canonical form definition

DLS enumeration problem:

$$X = \sum_{i=1}^{Q} \left| \Theta\left( \tilde{A}_i \right) \right|$$

| | | | | |
|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 |
| 2 | 3 | 4 | 0 | 1 |
| 4 | 0 | 1 | 2 | 3 |
| 1 | 2 | 3 | 4 | 0 |
| 3 | 4 | 0 | 1 | 2 |

01234 23401 40123 12340 34012
**– lexicographical minimum!**

| | | | | |
|---|---|---|---|---|
| 2 | 4 | 0 | 1 | 3 |
| 0 | 1 | 3 | 2 | 4 |
| 3 | 2 | 4 | 0 | 1 |
| 4 | 0 | 1 | 3 | 2 |
| 1 | 3 | 2 | 4 | 0 |

24013 01324 32401 40132 13240

| | | | | |
|---|---|---|---|---|
| 0 | 2 | 4 | 1 | 3 |
| 4 | 1 | 3 | 0 | 2 |
| 3 | 0 | 2 | 4 | 1 |
| 2 | 4 | 1 | 3 | 0 |
| 1 | 3 | 0 | 2 | 4 |

02413 41302 30241 24130 13024

- one of N! orders

# Program implementation

- source version — **1-2 DLS/s** (very slow, for example, DLS enumeration pace — 6.6M DLS/s for N=10);

Algorithmic optimizations:

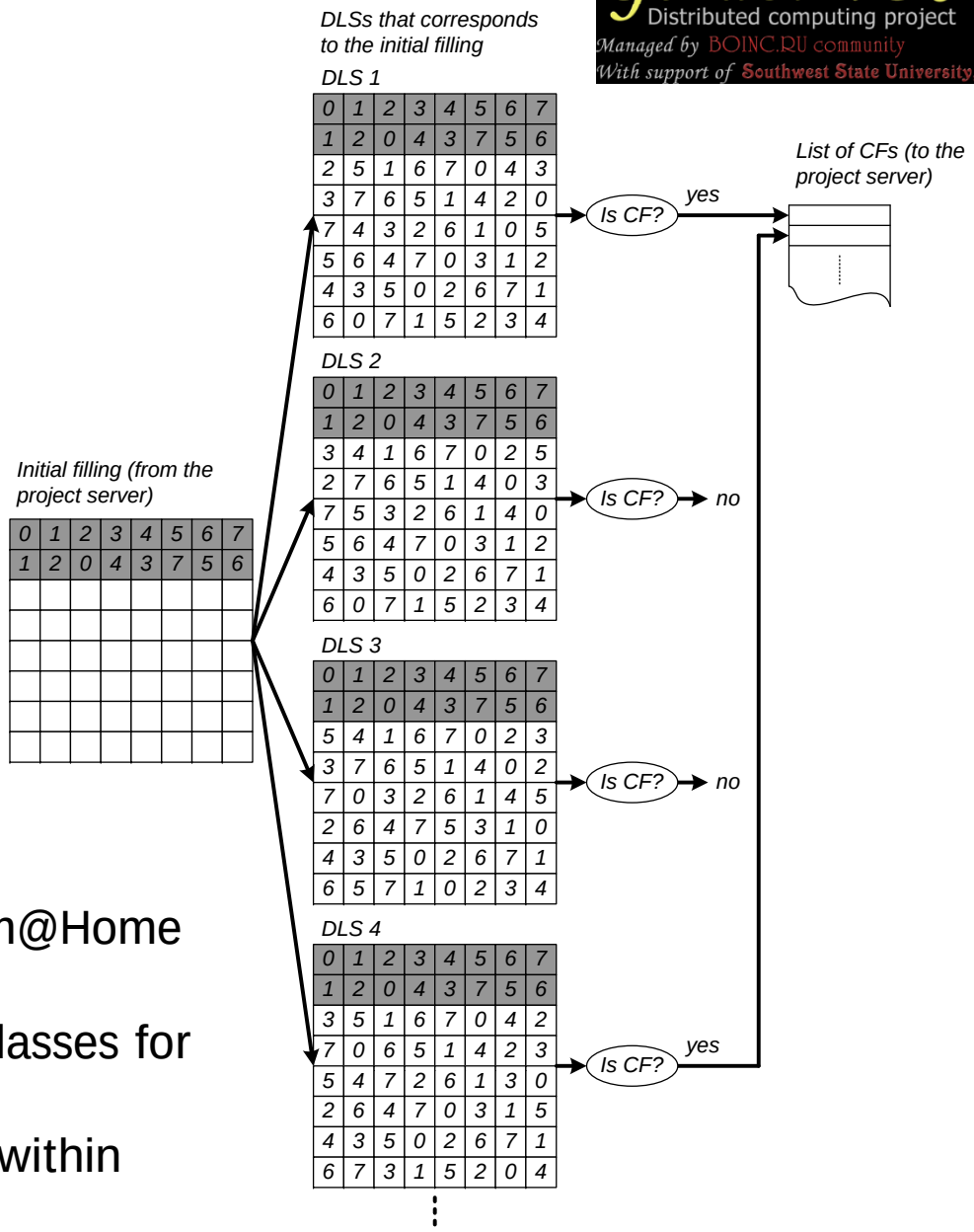
- avoid dynamic memory and dynamic strings usage — **31 DLS/s**;
- using Johnson–Trotter algorithm (Gray code like, but for permutations) — **56 DLS/s**;
- compiler checks off (range checkings, assertions, etc.) — **118 DLS/s**;
- fused normalization and reflection — **277 DLS/s**;
- horizontal reflection instead of vertical reflection — **305 DLS/s**;
- early break when current square less then source square ( IsCF() ) — **642 DLS/s**.

# Computing experiment: isotopy classes enumeration

| Square order $N$ | Isotopy classes count |
|---|---|
| 1 | 1 |
| 2 | – |
| 3 | – |
| 4 | 1 |
| 5 | 2 |
| 6 | 2 |
| 7 | 972 |

- Different sequences calculated by authors: A123565, A274171, A274806, A287645, A287644, A287647, A287648, A287649, A287650, A292516, A292517, A296060, A296061, A287651, A287695, A293777, A293778, A287761 and A287762.

# Isotopy classes enumeration for N=8




- 2 days within Gerasim@Home project
- **4 873 096** isotopy classes for N=8
- sequence **A287764** within OEIS

# Isotopy classes enumeration for N=9?

- **505 699 465 350 758** DLSs for N=9
- IsCF() pace **~60k DLS/s** (average, approximately)
- **~267 years** for single threaded program
- **~1-2 year** for 1 TFLOP/s computing system (Gerasim@Home — 1-2 TFLOP/s)

## Isotopy classes cardinalities and symmetries

$$C = C_M \cdot C_3 = 2^m \cdot m! \cdot 4$$

| $N$ | Minimal cardinality of isomorphism class | Maximal cardinality of isomorphism class |
|---|---|---|
| 1 | 1 | 1 |
| 2 | – | – |
| 3 | – | – |
| 4 | 2 | 2 |
| 5 | 4 | 4 |
| 6 | 32 | 96 |
| 7 | 32 | 192 |
| 8 | 96 | 1 536 |

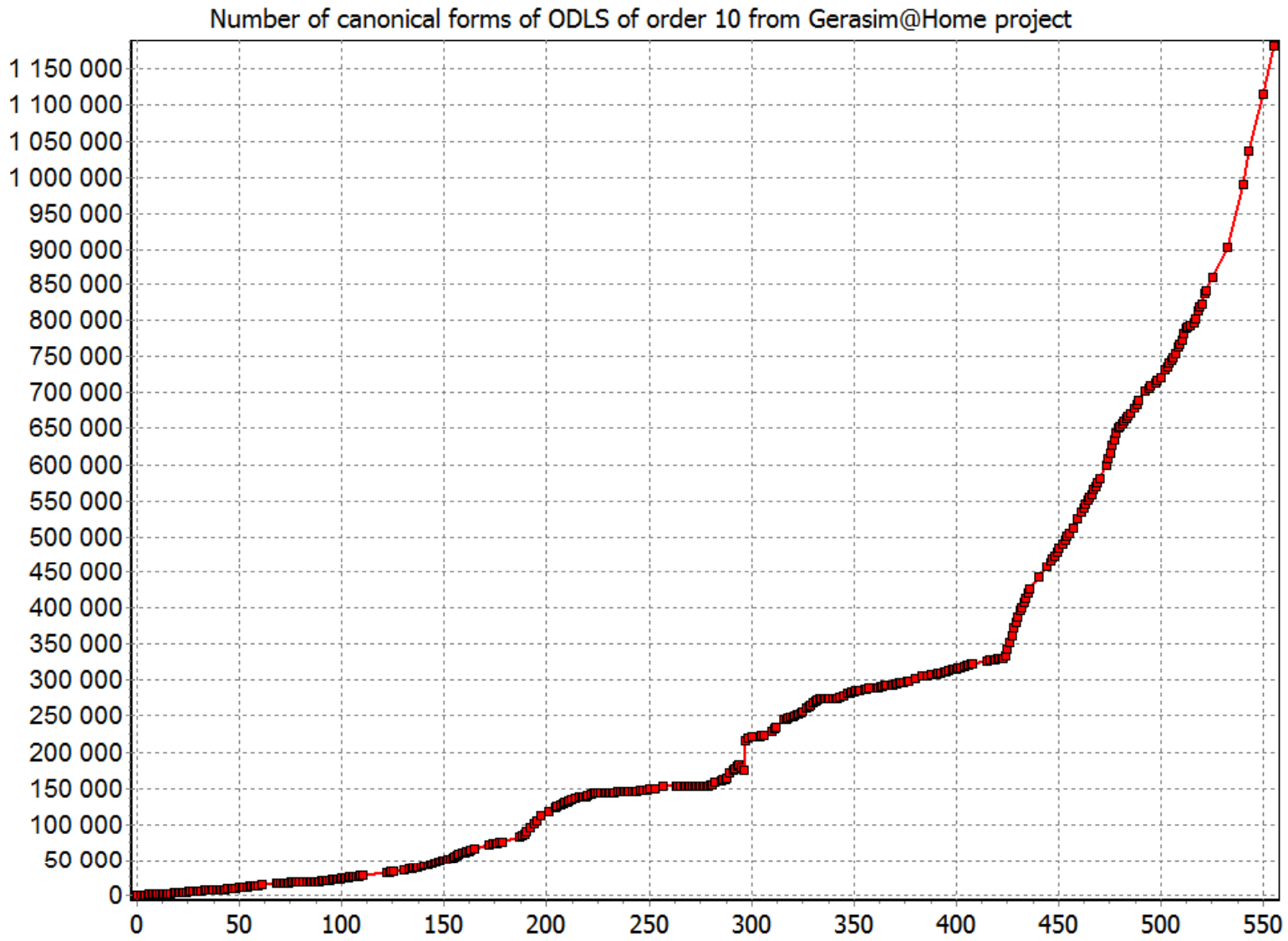
New sequences, not represented in OEIS:

- **1, 0, 0, 2, 4, 32, 32, 96**
- **1, 0, 0, 2, 4, 96, 192, 1536**

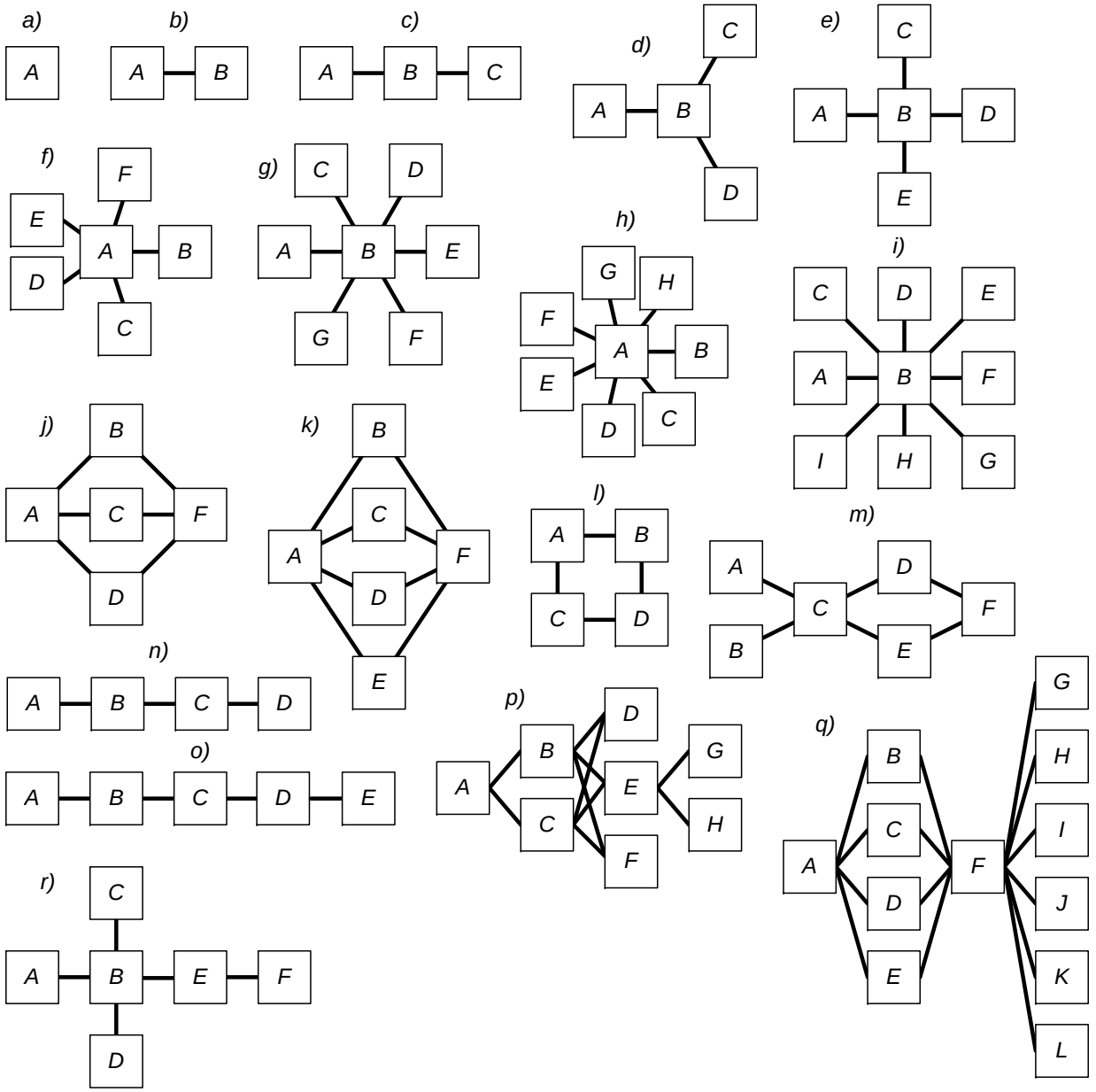
## I have some additional minutes? :)

Related works...

# ODLS canonical forms for N=10



# Combinatorial structures collection



# Future plans

Collecting CFs and new combinatorial structures search:

- triple of MODLS (is it exist?)
- different structures?

GPU implementation of transversal and cover algorithms?

Enumeration problems (OEIS):

- expanding current sequences
- enumerating DLS and ODLS of special kind (string-inverse, symmetric, ...) and its CFs

Pseudo triples:

- 3 kinds of pseudo triples, only 1 was investigated in details


# Thank you for your attention!

Thanks to all the volunteers who took part in the Gerasim@home project!

WWW: http://evatutin.narod.ru, http://gerasim.boinc.ru
E-mail: evatutin@rambler.ru
LJ: http://evatutin.livejournal.com
Skype: evatutin