Classification of Cells Mapping Schemes Related to Orthogonal Diagonal Latin Squares of Small Order

Eduard Vatutin, <u>Oleg Zaikin</u>

Southwest State University, Kursk

ISDCT SB RAS, Irkutsk

Russian Supercomputing Days
Moscow, 2023

Latin square

A *Latin square* (LS) of order N is a square table N × N filled with N symbols 0, . . . ,N −1 such that all symbols within a single row or single column are distinct.

A *diagonal Latin square* (DLS) is a Latin square in which all symbols in both main diagonal and anti-diagonal are distinct.

A *transversal* of a Latin square is a set of N entries such that no pair of them share the same row, column or symbol.

0	1	2	3
3	2	1	0
2	3	0	1
1	0	3	2

Orthogonality

Two Latin squares A = (aij),B = (bij) of order N are *orthogonal* if all ordered pairs (aij , bij), $0 \le i, j \le N - 1$ are distinct.

A set of Latin squares of the same order, all pairs of which are orthogonal, is called a *set of mutually orthogonal Latin squares* (*MOLS*). For diagonal Latin squares, *MODLS* is defined similarly.

Euler expected that no MOLS of order 10 exists.
First pair — Parker et al., 1960.

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

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

Gerasim@Home, 04.2017

MODLS are very rare combinatorial objects:
<u>~30 millions DLS</u> of order 10 has only **<u>1 pair of ODLS</u>**!

Why is it interesting?

Applications:

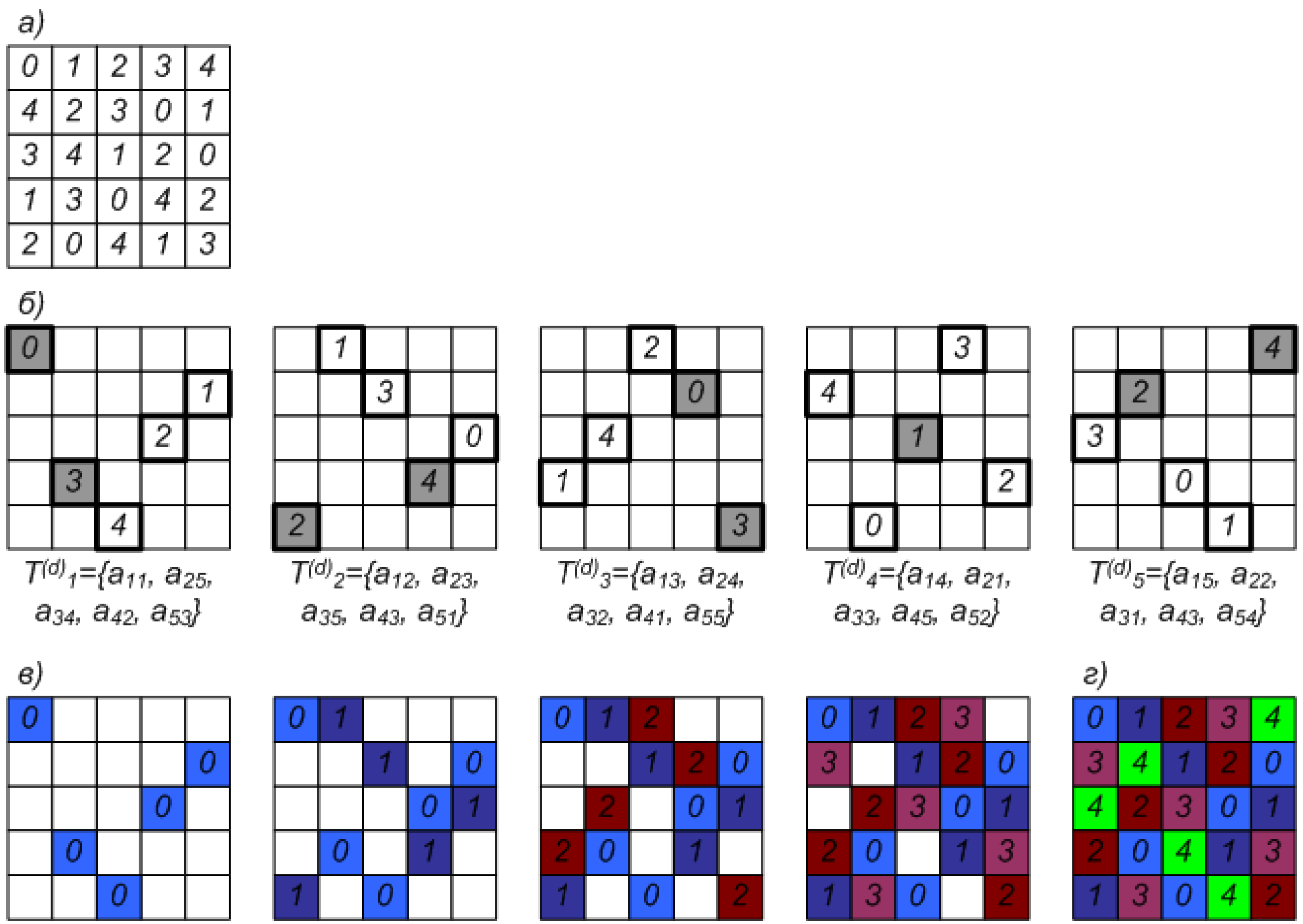
- experiment planning
- cryptography
- error correcting codes
- scheduling

Most famous open problem related to Latin squares:

- **existence of a triple of MOLS of order 10**

Searching for MOLS via Euler-Parker method

1. Find all transversals of a given LS of order N.
2. Choose a subset of N disjoint transversals.
3. Form an orthogonal mate.



Searching for MODLS: approaches

- Brute Force + backtracking + clippings + ordering + … (very long)
- SAT (very long)
- Euler-Parker (fast) – **200 – 800 DLS/s** for different algorithms!
- Euler-Parker with canonizer (searching for symmetrically placed transversals in a LS and putting them in place of the main diagonal and main anti-diagonal by rearranging rows and columns) (very fast, **~8000 DLS/s**)

DLS generators: **~6 600 000 DLS/s**

Bottleneck: transversals are to be found in Euler-Parker-based methods.

Transversals free search for MODLS: SODLS

- *Self-orthogonal Latin square* (SOLS) denotes a Latin square that is orthogonal to its transpose. SODLS is similar.
- Search without transversals is much faster.
- *Extended self-orthogonal diagonal Latin square* (ESODLS) denotes a diagonal Latin square that is orthogonal to some diagonal Latin square from the same main class (equivalence class obtained via M-transformations).
- ESODLS is a generalization of SODLS and can be also used to find MODLS.

SODLS: $B = A^T$

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

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

SODLS and ESODLS in OEIS

OEIS sequences (SODLS, H. White):

- A287761 — **1, 0, 0, 2, 4, 0, 64, 1152, 224832;**
- A287762 — **1, 0, 0, 48, 480, 0, 322560, 46448640, 81587036160.**

OEIS sequences (ESODLS, new):

- A309210 — **1, 0, 0, 1, 1, 0, 5, 23;**
- A309598 — **1, 0, 0, 2, 4, 0, 256, 4608;**
- A309599 — **1, 0, 0, 48, 480, 0, 1290240, 185794560.**

This site is supported by donations to The OEIS Foundation.

THE ON-LINE ENCYCLOPEDIA OF INTEGER SEQUENCES ®

founded in 1964 by N. J. A. Sloane

Search Hints

(Greetings from The On-Line Encyclopedia of Integer Sequences!)

A309598 Number of extended self-orthogonal diagonal Latin squares of order n with ordered first string. 0

1, 0, 0, 2, 4, 0, 256, 4608 (list; graph; refs; listen; history; text; internal format)

OFFSET 1,4

COMMENTS A self-orthogonal diagonal Latin square (SODLS) is a diagonal Latin square orthogonal to its transpose. An extended self-orthogonal diagonal Latin square (ESODLS) is a diagonal Latin square that has an orthogonal diagonal Latin square from the same main class. SODLS is a special case of ESODLS.

LINKS Table of n, a(n) for n=1..8.
E. I. Vatutin, Discussion about properties of diagonal Latin squares (in Russian)
Index entries for sequences related to Latin squares and rectangles

EXAMPLE

```
The diagonal Latin square
  0 1 2 3 4 5 6 7 8 9
  1 2 0 4 5 7 9 8 6 3
  5 0 1 6 3 9 8 2 4 7
  9 3 5 8 2 1 7 4 0 6
  4 6 3 5 7 8 0 9 2 1
  8 4 6 9 1 3 2 5 7 0
  7 8 9 0 6 4 5 1 3 2
  2 9 4 7 8 0 3 6 1 5
  6 5 7 1 0 2 4 3 9 8
  3 7 8 2 9 6 1 0 5 4
has orthogonal diagonal Latin square
  0 1 2 3 4 5 6 7 8 9
  3 5 9 8 6 2 0 1 4 7
  4 3 8 7 2 1 9 0 5 6
  6 9 3 4 8 0 1 2 7 5
  7 2 0 1 9 3 5 8 6 4
  2 0 1 5 7 6 4 9 3 8
  8 6 4 2 0 9 7 5 1 3
  1 7 6 0 5 4 8 3 9 2
  9 8 5 6 1 7 3 4 2 0
  5 4 7 9 3 8 2 6 0 1
from the same main class.
```

CROSSREFS Cf. A287761.
Sequence in context: A287761 A009512 A317411 * A305570 A287651 A163259
Adjacent sequences: A309595 A309596 A309597 * A309599 A309600 A309601

KEYWORD nonn,more

AUTHOR Eduard I. Vatutin, Aug 09 2019

STATUS approved

How can one find ESODLS? CMS-based search.

Cells Mapping Scheme (CMS) — a mapping of a Latin square to another Latin square.

CMS of order N – a square table comprised of elements 0, …, N^2 – 1.
CMS of order N – a permutation of size N.

DLS A

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

→

CMS

77	17	97	67	57	47	37	7	87	27
71	11	91	61	51	41	31	1	81	21
79	19	99	69	59	49	39	9	89	29
76	16	96	66	56	46	36	6	86	26
75	15	95	65	55	45	35	5	85	25
74	14	94	64	54	44	34	4	84	24
73	13	93	63	53	43	33	3	83	23
70	10	90	60	50	40	30	0	80	20
78	18	98	68	58	48	38	8	88	28
72	12	92	62	52	42	32	2	82	22

→

DLS B

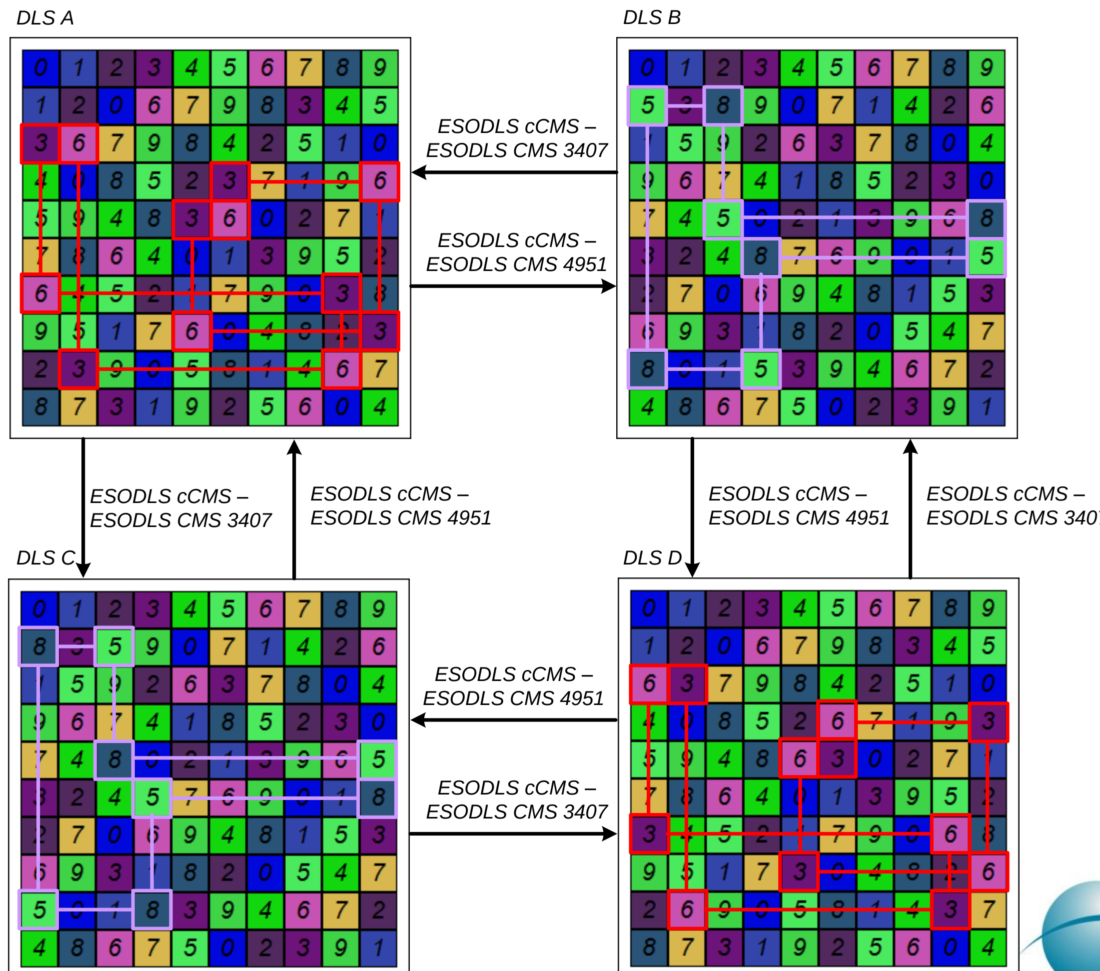
6	8	1	9	0	4	3	7	5	2
5	2	3	8	4	9	0	1	7	6
0	5	4	3	6	7	1	9	2	8
2	9	7	5	8	3	4	6	1	0
4	7	0	6	9	1	2	5	8	3
1	3	2	7	5	8	6	4	0	9
8	4	9	0	1	2	7	3	6	5
9	1	8	2	3	6	5	0	4	7
7	6	5	1	2	0	9	8	3	4
3	0	6	4	7	5	8	2	9	1

Loops structure for CMS

- CMS cells CMS[i1] -> CMS[i2] -> … -> CMS[iM] -> CMS[i1] form a loop of length **M**.
- Lengths of all CMS loops form a multiset **L = {M, …}**.

Examples for order 10:

- L = {1:100} — trivial;
- L = {1:10, 2:45} — canonical, all known ODLS;
- L = {4:25} — rare 1-CF loop-4 combinatorial structures;
- L = {1:10, 3:30} — ???



First new result: classification of ESODLS CMS of small order

- For orders 1-9, full classification was built via depth-first search.
- The classification is based on multisets of cycle lengths, which correspond to the obtained set of MODLS.

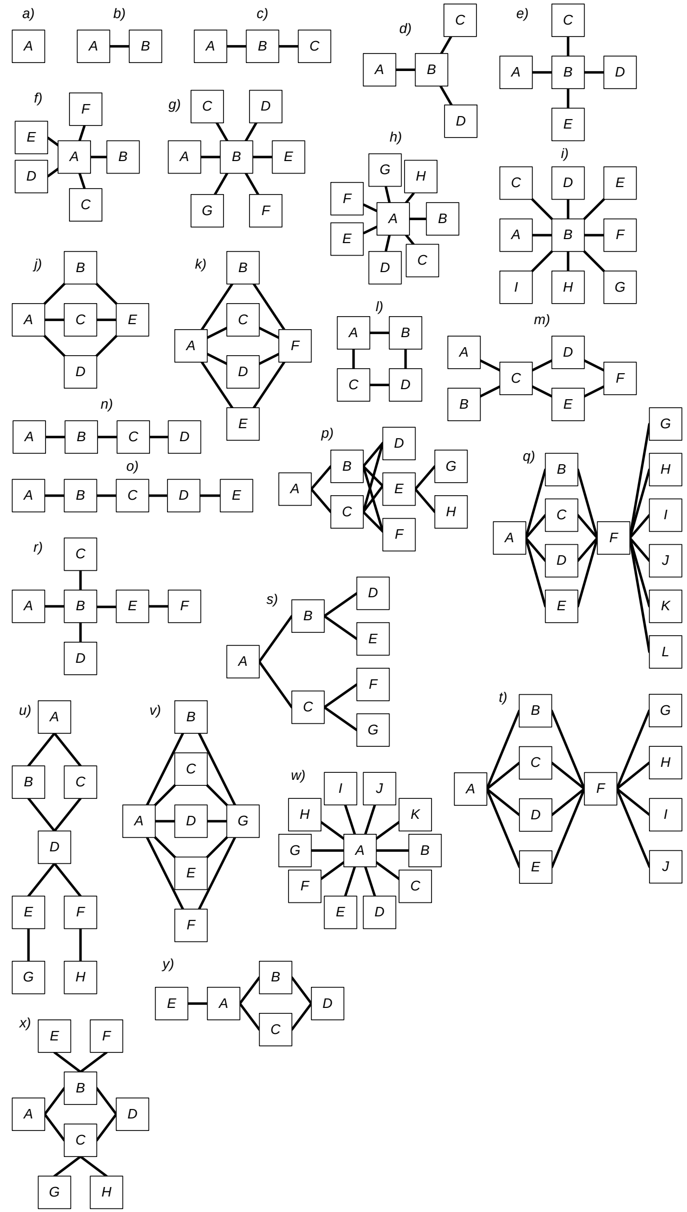
List of multisets of cycle lengths for ESODLS CMS of order 4

No.	Multiset	MODLS	CMS
1	{1:16}	-	trivial CMS 0
2	{1:4, 2:6}	bachelor, 1-CF	canonical CMS 1
3	{2:8}	-	-
4	{4:4}	bachelor, 1-CF	CMS 3

List of multisets of cycle lengths for ESODLS CMS of order 5

No.	Multiset	MODLS	CMS
1	{1:25}	-	trivial CMS 0
2	{1:5, 2:10}	bachelor, 1-CF	canonical CMS 1
3	{1:1, 4:6}	bachelor, 1-CF	CMS 13
4	{1:1, 2:12}	-	-
4	{1:9, 2:8}	-	-

Structures of MODLS (Eduard Vatutin et al)



Order 10: experiment in Gerasim@home

- There are 15360 ESODLS CMS of order 10 (easy to find).
- However, it is hard to find matching MODLS for all of them to complete the classification.
- For order 10, a series of short experiments was carried out in a volunteer computing project Gerasim@home.
- As a result, cycles of MODLS of order 10, which match ESODLS CMS, were found. In turned out, that all of them have either length 2 or 4.
- For some ESODLS CMS, it is time-consuming to find all matching MODLS via depth-first search.

SAT

Boolean satisfiability problem (*SAT*) - for an arbitrary propositional Boolean formula to determine if there exists such assignment of Boolean variables from this formula that makes it true.

Usually, a formula in considered in the Conjunctive Normal Form (CNF) that is a conjunction of disjunctions.

An example of CNF with 3 disjunctions over 5 variables:

$$C = (x_1 \vee \overline{x_2}) \cdot (x_2 \vee x_3 \vee \overline{x_4}) \cdot (\overline{x_3} \vee x_4 \vee \overline{x_5})$$

This CNF is satisfiable, e.g., on (11001).

X-based diagonal fillings and ESODLS CMS

- In [1], X-like partial Latin squares of order 10 for ESODLS CMS were proposed.
- First, all distinct partial Latin squares with known main diagonal are formed.
- Then all possible M-transformations are applied to them, and the obtained partial Latin squares are normalized by the main diagonal.
- As a result, in these X-like partial Latin squares, the main diagonal has values 0, . . . , 9, while the main anti-diagonal is also known, but it may have any values.
- Finally, lexicographically minimal representatives are chosen, and each of them corresponds to an equivalence class. Such representatives are called *highly normalized DLSs*.
- **There are 67 highly normalized DLSs of order 10.**

[1] Vatutin, E.I., Belyshev, A.D., Nikitina, N.N., O.Manzuk, M.: Use of x-based diagonal fillings and esodls cms schemes for enumeration of main classes of diagonal latin squares (in russian). Telecommunications 1(1), 2–16 (2023)

Second new result: searching for MODLS via SAT and ESODLS CMS

- For order 10, CMS 1234, 3407, 4951, and 5999 were considered (out of 15360).
- For each of them a CNF was constructed that encodes searching for a pair of MODLS of order 10 that matches the CMS.
- Each of four CNF was divided into 67 CNFs by assigning X-like fillings in the first DLS.
- A sequential SAT solver Kissat was run on each of 268 CNFs on a computer.
- All were solved – maximal runtime is 2 hours.
- For CMS 1234, 3407, 4951, all CNFs were unsatisfiable, so it was proven that there is no corresponding pair of MODLS.
- For CMS 5999, 1 CNF was satisfiable, and all 8 pairs of MODLS were found.
- Thus, for 4 CMS our of 15360 all matching MODLS were found on a computer.
- It is planned to process the remaining CMSs in a volunteer computing project.

One found pair of MODLS

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

Corresponding X-like filling:

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

Conclusions

- The present paper proposes a classification of cells mapping schemes based on extended self-orthogonal diagonal Latin squares.
- For order 1-9, the classification is fully presented, while for order 10 it is partial.
- Some experiments for order 10 were held in a volunteer computing project.
- Preliminary results on finding MODLS of order 10 via SAT and ESODLS CMS are given.
- Based on SAT results, it is planned to start a large-scale experiment in a volunteer computing project to complete the classification for order 10.

Thank you for your attention!

Thanks to all the volunteers who took part in the Gerasim@home and RakeSearch projects!

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