# CLIQUES PROPERTIES FROM DIAGONAL LATIN SQUARES OF SMALL ORDER 

## Vatutin E.I., Nikitina N.N., Manzuk M.O., Zaikin O.S., Belyshev A.D.

## What is Latin squares?

$$
\begin{array}{lr}
A=\left\|a_{i j}\right\| \\
i, j=\overline{1, N} & \forall i, j, k=\overline{1, N}, j \neq k:\left(a_{i j} \neq a_{i k}\right) \wedge\left(a_{j i} \neq a_{k i}\right) \\
& \forall i, j=\overline{1, N}, i \neq j:\left(a_{i i} \neq a_{j j}\right) \wedge\left(a_{N-i+1, N-i+1} \neq a_{N-j+1, N-j+1}\right)
\end{array}
$$

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

$$
\left(\begin{array}{llllllllll}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
1 & 2 & 9 & 4 & 3 & 6 & 7 & 5 & 0 & 8 \\
2 & 9 & 3 & 1 & 7 & 0 & 5 & 8 & 4 & 6 \\
3 & 4 & 1 & 2 & 8 & 7 & 9 & 6 & 5 & 0 \\
4 & 3 & 5 & 9 & 2 & 1 & 8 & 0 & 6 & 7 \\
5 & 6 & 4 & 8 & 1 & 2 & 0 & 9 & 7 & 3 \\
6 & 5 & 8 & 7 & 0 & 3 & 2 & 1 & 9 & 4 \\
7 & 8 & 6 & 0 & 9 & 4 & 1 & 2 & 3 & 5 \\
8 & 7 & 0 & 5 & 6 & 9 & 3 & 4 & 1 & 2 \\
9 & 0 & 7 & 6 & 5 & 8 & 4 & 3 & 2 & 1
\end{array}\right) \quad\left(\begin{array}{llllllllll}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
7 & 2 & 4 & 9 & 0 & 6 & 5 & 1 & 3 & 8 \\
8 & 3 & 6 & 7 & 5 & 9 & 0 & 2 & 4 & 1 \\
2 & 6 & 8 & 5 & 1 & 7 & 4 & 0 & 9 & 3 \\
5 & 8 & 9 & 1 & 7 & 0 & 3 & 4 & 6 & 2 \\
9 & 4 & 1 & 2 & 8 & 3 & 7 & 6 & 0 & 5 \\
4 & 7 & 5 & 6 & 9 & 1 & 8 & 3 & 2 & 0 \\
3 & 0 & 7 & 8 & 2 & 4 & 1 & 9 & 5 & 6 \\
6 & 5 & 0 & 4 & 3 & 2 & 9 & 8 & 1 & 7 \\
1 & 9 & 3 & 0 & 6 & 8 & 2 & 5 & 7 & 4
\end{array}\right)
$$

Normalized DLS of order 10

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

$$
(N-1)!
$$



## 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 of order 10 (or larger clique)

■ increasing world record of orthogonality characteristic for pseudo triple of MOLS (291/300) or MODLS (274/300)

- 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)


## Brief history and approaches

■ Euler - triple of MOLS of order 10 does not exist (disproved);
■ Parker et al. (1960) - first pair of MOLS of order 10 using transversals;
■ Brown et al. (1995) - horyzontally symmetric DLS, 1:4;
■ Zaikin et al. (2015-2016) — SAT approach (system of Boolean equations), ~100 CFs of ODLS, onces;

- Vatutin et al. (from 2017) - RS+LBF generator $->$ transversals + DLX, $\sim 1 M$ CFs of ODLS, twices, 1:3;
- Vatutin et al. (2017) - plane symmetry generator -> transversals + DLX, ~200k CFs of ODLS, 1:6, 1:8, rhombus-4, line-4, line-5, loop-4, fish;
- Vatutin et al. (from 2017) - central symmetry, partial central and plane symmetries, generalized symmetries, neighborhoods of generalized symmetris generator $->$ canonizer $->$ postprocessor, $\sim 7 \mathrm{M}$ CFs of ODLS, 1:5, 1:7, 1:10, rhombus-3, cross, flyer, tree-1, Venus, Daedalus-8, Daedalus-10, robot, stingray;
- Vatutin et al. (from 2019) - none transversal search for ODLS.


## Classical search for pairs of ODLS of order 10

L. Euler expected that for $\mathrm{N}=10$ ODLS doesn't exist First pair — Parker et al., 1960


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

SAT@Home, 04.2015


Gerasim@Home, 04.2017
Very rare combinatorial objects: ~ $\mathbf{3 0}$ millions DLS of order 10 has only 1 pair of ODLS!

## Searching for ODLS: approaches

- Brute Force + backtracking + clippings + ordering $+\ldots$ (very long)
- SAT (some tens of hours, long)
- filling by pairs of elements [ $\mathrm{a}_{\mathrm{ij}}, \mathrm{b}_{\mathrm{ij}}$ ] (long)
- using transversals (fast) - 200 - 800 DLS/ s for different algorithms!
- using transversals with canonizer ( $\mathbf{8 0 0 0}$ DLS/ s effective pace)

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



## Neighborhoods of generalized symmetries (01.11.2019)



- 268 from 903 neighborhoods processed (29,7\%)

Properties of cliques within combinatorial structures of small order ( $\mathrm{N}=4$ )


- clique-2, 1 CF

Properties of cliques within combinatorial structures of small order ( $\mathrm{N}=5$ )
a)


- clique-2, 1 CF

Properties of cliques within combinatorial structures of small order ( $\mathrm{N}=7$ )
a)

a)

b)


- clique-2, 1 CF
- clique-4, 1 CF

Properties of cliques within combinatorial structures of small order ( $\mathrm{N}=8$ )

- N824HUGE structure (348000 DLSs, 657 CFs), includes clique-6, $\mathbf{1 ~ C F}$


## Properties of cliques within combinatorial structures of small order ( $\mathrm{N}=9$ )

197 different combinatorial structures (some of them with cliques):

- 24N54M4C - clique-3, 1 CF;
- 120N480M5C - clique-4, 1 CF;
- 24N60M4C - clique-4, 1 CF;
- 32N86M13C - clique-3, 3 CFs;
- 48N126M6C - clique-6, 2 CFs.


Figure 148. Graph of ODLS from workunit R9_000463421/02.
2017.12.15. Rake Search project. [B@P] Daniel (BOINC@Poland) and LCB001 (Hardware Canucks)

```
http://evatutin.narod.ru/evatutin Is all_structs_n1to8_eng.pdf
http://evatutin.narod.ru/evatutin Is all structs n9 eng.pdf
http://evatutin.narod.ru/evatutin_Is_all_structs_eng.pdf
```

- based on RakeSearch project results (https://rake.boincfast.ru/rakesearch/)


## Properties of cliques within combinatorial structures of order $\mathrm{N}=10$

More then clique-2 subgraphs don't known...

Searching for ODLS from same main class?


- Bennett F.E., Beiliang Du, Hantao Zhang. Existence of self-orthogonal diagonal Latin squares with a missing subsquare // Discrete Mathematics. Vol. 261. 2003. pp. 69-86.


## SODLS can be extended for ESODLS

ESODLS (Ed's SODLS) — MODLS from DLSs within same main class

This site is supported by donations to The OEIS Foundation.
0136
$\vdots$ OE
THE ON-LINE ENCYCLOPEDIA
OF INTEGER SEQUENCES ${ }^{\circledR}$
founded in 1964 by N. J. A. Sloane

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.
(Greetings from The On-Line Encyclopedia of Integer Sequences!) Search Hints
A309598 Number of extended self-orthogonal diagonal Latin squares of order n with ordered first string.
$1,0,0,2,4,0,256,4608$ (list; graph; refs; listen; history, text; internal format)
OFFSET
comamnts 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 able of $n, \bar{a}(n)$ 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 The diagonal Latin square

from the same main class.
Cf. A287761.
Sequence in context: A287761 A009512 A317411 * A305570 A287651 A163259
Adjacent sequences: A309595 A309596 $\frac{A 309597}{*}$ A309599 A309600 A309601
nonn, more
author Eduard I. Vatutin, Aug 092019
status approved


## How we can find ESODLS? CMS-based search...

Bijective mapping for $\mathrm{N}^{\wedge} 2$ cells of square with some special properties

## SODLS - one of them...

M-transformations


## Different properties of CMS: example 1

CMS[ 0] $=0$ CMS[ 1] $=1$ CMS[ 2] $=2$ CMS[ 3] $=3$ CMS[ 4] $=4$ CMS[ 5] $=5$ CMS[ 6] $=6$ CMS[ 7] $=7$ CMS[ 8] $=8$ CMS[ 9] $=9$ CMS[10] $=30$ CMS[11] $=95$ $\mathrm{CMS}[12]=32$ CMS[13] $=35$ CMS[14] $=48$ CMS[15] $=92$ CMS[16] $=93$ CMS[17] $=78$ CMS[18] $=65$ CMS[19] $=45$ CMS[20] $=31$ CMS[21] $=51$ CMS[22] $=83$ CMS[23] $=80$ CMS[24] $=47$ CMS[25] $=39$ CMS[26] $=72$ CMS[27] $=89$ CMS[28] $=40$ CMS[29] $=82$ CMS[30] $=10$ CMS[31] $=20$ CMS[32] $=12$ $\mathrm{CMS}[33]=34$
$\mathrm{CMS}[34]=33$
CMS[35] $=13$
CMS[36] $=59$
$C M S[37]=60$
CMS[38] $=50$
CMS[39] $=25$
CMS[40] $=28$
$C M S[41]=90$
CMS[42] $=53$
CMS[43] $=67$
CMS[44] $=94$
CMS[45] $=19$
$C M S[46]=64$
$C M S[47]=24$
$C M S[48]=14$
CMS[49] $=62$
CMS[50] $=38$
$\mathrm{CMS}[51]=21$
$\mathrm{CMS}[52]=70$
$\mathrm{CMS}[53]=42$
$C M S[54]=88$
CMS[55] $=99$
$C M S[56]=76$
$\mathrm{CMS}[57]=77$
$C M S[58]=74$
CMS[59] $=36$
CMS[60] $=37$
CMS[61] $=91$
CMS[62] $=49$
CMS[63] $=73$
$C M S[64]=46$
CMS[65] $=18$
$C M S[66]=84$
CMS[67] $=43$

CMS[68] $=69$
CMS[69] $=68$
CMS[70] $=52$
$\mathrm{CMS}[71]=81$
$\mathrm{CMS}[72]=26$
CMS[73] $=63$
CMS[74] $=58$
CMS[75] $=79$
$\mathrm{CMS}[76]=56$
CMS[77] $=57$
CMS[78] $=17$
CMS[79] $=75$
CMS[80] $=23$
CMS[81] $=71$
$\mathrm{CMS}[82]=29$
CMS[83] $=22$
$C M S[84]=66$
CMS[85] $=96$
CMS[86] $=87$
CMS[87] $=86$
CMS[88] $=54$
CMS[89] $=27$
CMS[90] $=41$
CMS[91] $=61$
CMS[92] $=15$
CMS[93] $=16$
CMS[94] $=44$
CMS[95] $=11$
CMS[96] $=85$
CMS[97] $=98$
CMS[98] $=97$
CMS[99] $=55$

82 hours per ODLS pair ( $\sim 10$ times slower)


## Different properties of CMS: example 2

CMS[ 0] $=0$
CMS[ 1] $=44$ CMS[ 2] $=77$ CMS[ 3] $=38$ CMS[ 4] $=97$ CMS[ 5] $=47$ CMS[ 6] $=16$ CMS[ 7] $=43$ CMS[ 8] $=84$ CMS[ 9] $=9$ CMS[10] $=10$ CMS[11] $=23$ CMS[12] $=36$ CMS[13] $=26$ CMS[14] $=31$ CMS[15] $=83$ $C M S[16]=6$ CMS[17] $=98$ CMS[18] $=79$ CMS[19] $=80$ CMS[20] $=41$ CMS[21] $=21$ CMS[22] $=39$ CMS[23] $=11$ $\mathrm{CMS}[24]=51$ CMS[25] $=74$ CMS[26] $=13$ CMS[27] $=75$ CMS[28] $=49$ CMS[29] $=95$ $\mathrm{CMS}[30]=94$ CMS[31] $=14$

$$
\mathrm{CMS}[32]=76
$$

CMS[33] $=33$
$\mathrm{CMS}[34]=42$
$\mathrm{CMS}[35]=45$
CMS[36] $=12$
CMS[37] $=91$
CMS[38] $=3$
CMS[39] $=22$
CMS[40] $=60$
CMS[41] $=20$
CMS[42] $=34$
CMS[43] $=7$
CMS[44] $=1$
CMS[45] $=35$
CMS[46] $=58$
CMS[47] $=5$
CMS[48] $=52$
CMS[49] $=28$
CMS[50] $=50$
$C M S[51]=24$
CMS[52] $=48$
CMS[53] $=54$
CMS[54] $=53$
CMS[55] $=87$
CMS[56] $=93$
$C M S[57]=64$
$C M S[58]=46$
$C M S[59]=73$
$C M S[60]=40$
$C M S[61]=67$
CMS[62] $=70$
CMS[63] $=86$
$C M S[64]=57$
CMS[65] $=96$
CMS[66] $=99$
CMS[67] $=61$
$\mathrm{CMS}[68]=78$
CMS[69] $=71$
$\mathrm{CMS}[70]=62$
CMS[71] $=69$
CMS[72] $=72$
CMS[73] $=59$
$\mathrm{CMS}[74]=25$
$\mathrm{CMS}[75]=27$
$\mathrm{CMS}[76]=32$
CMS[77] $=2$
$\mathrm{CMS}[78]=68$
CMS[79] $=18$
CMS[80] $=19$
$\mathrm{CMS}[81]=85$
$\mathrm{CMS}[82]=82$
$\mathrm{CMS}[83]=15$
CMS[84] $=8$
$\mathrm{CMS}[85]=81$
$\mathrm{CMS}[86]=63$
CMS[87] $=55$
CMS[88] $=92$
CMS[89] $=89$
CMS[90] $=90$
CMS[91] $=37$
CMS[92] $=88$
CMS[93] $=56$
$\mathrm{CMS}[94]=30$
CMS[95] $=29$
CMS[96] $=65$
$\mathrm{CMS}[97]=4$
$\mathrm{CMS}[98]=17$
$\mathrm{CMS}[99]=66$


## 28 seconds per ODLS pair (~1000 times faster)

- Nested loops implementation?
- GPU/Phi implementation?


## What we know about ESODLS of order 10?

- 32010 ESODLS CFs - Gerasim@Home results:
- 30429 SODLS CFs - SOLS to SODLS (whitefox);
- 1581 CFs — Gerasim@Home generalized symmetries neighborhoods.

Combinatorial structures:
ONCE (A): 1 - 32010, where:
1 CFs-32010
LINE4 (C):1-3, where:
2 CFs - 3
LINE4 (C):2-3, where:
2 CFs - 3
LOOP4 (E):2-76, where:
1 CFs - 2
2 CFs - 74

## Computing experiment (from 07.2019)

Very rare objects!

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

06.08. 2019

1CF Loop-4 (re-find in different WU's)

| 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 |

09.08.2019

1CF Once (new!)

- +4 additional 1 CF Onces (new!) and 13 re-find 1 CF Onces


## Getting ODLS CFs within Gerasim@Home project

Strategy of search: getting source square (random generator, symmetric random generator), try to get orthogonal square, add the unique CF to collection


- Brute Force with bits arithmetic (03.2017)
- DLX v1, array (04.2017)
- DLX v2, pointers (05.2017)
- SN DLS (SCFs) (08.2017)
- horizontal symmetry (10.2017)
- different canonization strategy (04.2018)


## Related work

Collecting CFs and new combinatorial structures search:

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

GPU implementation of transversal, cover and ESODLS 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!

