ENUMERATING CYCLIC AND PANDIAGONAL LATIN SQUARES AND THEIR PROPERTIES

Vatutin E.I.

Pereslavl-Zaleskiy, 2020
What are Latin and diagonal Latin squares?

\[ A = \begin{bmatrix} a_{ij} \end{bmatrix} \]

\[ i, j = 1, N \]

\[ N = |S| \]

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

\[ N! \times (N - 1)! \]

\[ \forall i, j, k = 1, N, j \neq k: (a_{ij} \neq a_{ik}) \land (a_{ji} \neq a_{ki}) \]

\[ \forall i, j = 1, N, i \neq j: (a_{ii} \neq a_{jj}) \land (a_{N-i+1, N-i+1} \neq a_{N-j+1, N-j+1}) \]

<table>
<thead>
<tr>
<th>Normalized LS of order 10</th>
<th>Normalized DLS of order 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>\begin{pmatrix} 0 &amp; 1 &amp; 2 &amp; 3 &amp; 4 &amp; 5 &amp; 6 &amp; 7 &amp; 8 &amp; 9 \ 1 &amp; 2 &amp; 9 &amp; 4 &amp; 3 &amp; 6 &amp; 7 &amp; 5 &amp; 0 &amp; 8 \ 2 &amp; 9 &amp; 3 &amp; 1 &amp; 7 &amp; 0 &amp; 5 &amp; 8 &amp; 4 &amp; 6 \ 3 &amp; 4 &amp; 1 &amp; 2 &amp; 8 &amp; 7 &amp; 9 &amp; 6 &amp; 5 &amp; 0 \ 4 &amp; 3 &amp; 5 &amp; 9 &amp; 2 &amp; 1 &amp; 8 &amp; 0 &amp; 6 &amp; 7 \ 5 &amp; 6 &amp; 4 &amp; 8 &amp; 1 &amp; 2 &amp; 0 &amp; 9 &amp; 7 &amp; 3 \ 6 &amp; 5 &amp; 8 &amp; 7 &amp; 0 &amp; 3 &amp; 2 &amp; 1 &amp; 9 &amp; 4 \ 7 &amp; 8 &amp; 6 &amp; 0 &amp; 9 &amp; 4 &amp; 1 &amp; 2 &amp; 3 &amp; 5 \ 8 &amp; 7 &amp; 0 &amp; 5 &amp; 6 &amp; 9 &amp; 3 &amp; 4 &amp; 1 &amp; 2 \ 9 &amp; 0 &amp; 7 &amp; 6 &amp; 5 &amp; 8 &amp; 4 &amp; 3 &amp; 2 &amp; 1 \end{pmatrix}</td>
<td>\begin{pmatrix} 0 &amp; 1 &amp; 2 &amp; 3 &amp; 4 &amp; 5 &amp; 6 &amp; 7 &amp; 8 &amp; 9 \ 7 &amp; 2 &amp; 4 &amp; 9 &amp; 0 &amp; 6 &amp; 5 &amp; 1 &amp; 3 &amp; 8 \ 8 &amp; 3 &amp; 6 &amp; 7 &amp; 5 &amp; 9 &amp; 0 &amp; 2 &amp; 4 &amp; 1 \ 2 &amp; 6 &amp; 8 &amp; 5 &amp; 1 &amp; 7 &amp; 4 &amp; 0 &amp; 9 &amp; 3 \ 5 &amp; 8 &amp; 9 &amp; 1 &amp; 7 &amp; 0 &amp; 3 &amp; 4 &amp; 6 &amp; 2 \ 9 &amp; 4 &amp; 1 &amp; 2 &amp; 8 &amp; 3 &amp; 7 &amp; 6 &amp; 0 &amp; 5 \ 4 &amp; 7 &amp; 5 &amp; 6 &amp; 9 &amp; 1 &amp; 8 &amp; 3 &amp; 2 &amp; 0 \ 3 &amp; 0 &amp; 7 &amp; 8 &amp; 2 &amp; 4 &amp; 1 &amp; 9 &amp; 5 &amp; 6 \ 6 &amp; 5 &amp; 0 &amp; 4 &amp; 3 &amp; 2 &amp; 9 &amp; 8 &amp; 1 &amp; 7 \ 1 &amp; 9 &amp; 3 &amp; 0 &amp; 6 &amp; 8 &amp; 2 &amp; 5 &amp; 7 &amp; 4 \end{pmatrix}</td>
</tr>
</tbody>
</table>
Why is it 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)
Special types of LS/DLS

row[i] = cyclic_shift(row[i-1], d)

- there are known different special types of LS/DLS (plane symmetric, central symmetric, ...);
- all cyclic squares of small orders are pandiagonal.
Integer sequences (OEIS): N queens problem example

A000170  Number of ways of placing n nonattacking queens on an \( n \times n \) board.

For \( n = 3 \), \( a(n) \) is the number of maximum independent vertex sets in the \( n \times n \) queen graph. - Eric W. Weisstein, Jun 20 2017

Number of nodes on level \( n \) of the backtrack tree for the \( n \) queens problem \((a(n)) \approx A253204(n, n)\). - Peter Luschny, Sep 18 2018

For more information, see the Wikipedia page on the N queens problem.

Table of \( a(n) \) for \( n \leq 27 \):

<table>
<thead>
<tr>
<th>n</th>
<th>a(n)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>7</td>
<td>40</td>
</tr>
<tr>
<td>8</td>
<td>92</td>
</tr>
<tr>
<td>9</td>
<td>352</td>
</tr>
<tr>
<td>10</td>
<td>3752</td>
</tr>
<tr>
<td>11</td>
<td>2680</td>
</tr>
<tr>
<td>12</td>
<td>73712</td>
</tr>
<tr>
<td>13</td>
<td>57968</td>
</tr>
<tr>
<td>14</td>
<td>1787829</td>
</tr>
<tr>
<td>15</td>
<td>1707560</td>
</tr>
<tr>
<td>16</td>
<td>84812</td>
</tr>
<tr>
<td>17</td>
<td>437046</td>
</tr>
<tr>
<td>18</td>
<td>279936</td>
</tr>
<tr>
<td>19</td>
<td>1787829</td>
</tr>
<tr>
<td>20</td>
<td>9494880</td>
</tr>
<tr>
<td>21</td>
<td>3612752</td>
</tr>
<tr>
<td>22</td>
<td>126240</td>
</tr>
<tr>
<td>23</td>
<td>10394064</td>
</tr>
<tr>
<td>24</td>
<td>3612752</td>
</tr>
<tr>
<td>25</td>
<td>437046</td>
</tr>
<tr>
<td>26</td>
<td>84812</td>
</tr>
<tr>
<td>27</td>
<td>437046</td>
</tr>
</tbody>
</table>

https://oeis.org/A000170
Integer sequences connected with transversals in DLS

*A287645* — Minimum number of transversals in a diagonal Latin square of order N (N<10)
*A287644* — Maximum number of transversals in a diagonal Latin square of order N (N<10)
*A287647* — Minimum number of diagonal transversals in a diagonal Latin square of order N (N<9)
*A287648* — Maximum number of diagonal transversals in a diagonal Latin square of order N (N<9)

Transversal 1

Transversal 2

Transversal 3
Integer sequences connected with transversals in DLS: exactly known values

A287645 — 1, 0, 0, 8, 3, 32, 7, 8, 68 (N<10)
A287644 — 1, 0, 0, 8, 15, 32, 133, 384, 2241 (N<10)
A287647 — 1, 0, 0, 4, 1, 2, 0, 0, 0 (N<10)
A287648 — 1, 0, 0, 4, 5, 6, 27, 120, 333? (N<10)

a(1)-a(8) — Brute Force for all DLS
a(9) — CFs generator for main classes of DLS based on X-fillings of diagonals and ESODLS schemas (currently ongoing, ends)

What about a(10), a(11), ...? They are unknown

\[ 0 \leq X^{LS}_{\min}(N) \leq X^{DLS}_{\min}(N) \leq X^{DLS}_{\max}(N) \leq X^{LS}_{\max}(N) \]
Integer sequences connected with transversals in DLS: unknown values for high orders

A287645 — 1, 0, 0, 8, 3, 32, 7, 8, 68 (0 ≤ a(n) ≤ A287644(n) ≤ A090741(n))
A287644 — 1, 0, 0, 8, 15, 32, 133, 384, 2241, ≥5504 (a(n) ≤ A090741(n))
A287647 — 1, 0, 4, 1, 2, 0, 0, 0 (a(n) ≤ A287648(n) ≤ A007016(n))
A287648 — 1, 0, 4, 5, 6, 27, 120, ≥333, ≥866, ≥4828, ≥24901, ≥131106, ≥364596, ≥389318 (a(n) ≤ A007016(n))

Upper and lower bounds can be expanded and strengthened!
Transversals in random Latin squares

A287645 (minimum number of transversals)
\[ a(11) \leq 3266->3255->3185->3175 \]
\[ a(12) \leq 15462 \]
\[ a(13) \leq 78253 \]
\[ a(14) \leq 422312 \]
\[ a(15) \leq 2415635 \]
\[ a(16) \leq 14689972 \]
...

A287644 (maximum number of transversals)
\[ a(11) \geq 3867 \]
\[ a(12) \geq 16600 \]
\[ a(13) \geq 80999 (a(13) \geq 1030367 \text{ for cyclic squares}) \]
\[ a(14) \geq 428296 \]
\[ a(15) \geq 2429398 \]
\[ a(16) \geq 14720910 \]
...

- 16 days on Core i7 4770 CPU, special program implementation of DLX (enumeration only without covers collecting)
- [https://vk.com/wall162891802_1449](https://vk.com/wall162891802_1449)
Diagonal transversals in random Latin squares

A287647 (minimum number of diagonal transversals)
\[ a(11) \leq 324 \]
\[ a(12) \leq 1816 \]
...

A287648 (maximum number of diagonal transversals)
\[ a(11) \geq 550 \]
\[ a(12) \geq 2200 \]
...

- 16 days on Core i7 4770 CPU, special program implementation of DLX (enumeration only without covers collecting)
- [https://vk.com/wall162891802_1449](https://vk.com/wall162891802_1449)
Cyclic Latin squares: one of special types of LS

- 4 cyclic DLS, 6 cyclic LS for N=7
Number of transversals in cyclic Latin squares

1, 0, 3, 0, 15, 0, 133, 0, 2025, 0, 37851, 0, 1030367, 0, 36362925

or without zeroes:

1, 3, 15, 133, 2025, 37851, 1030367, 36362925

A006717 — Number of ways of arranging 2n+1 nonattacking semi-queens on a (2n+1) X (2n+1) toroidal board

Also the number of transversals of a cyclic Latin square of order 2n+1 and the number of orthomorphisms of the cyclic group of order 2n+1 (Ian Wanless, 2001).

• Number of transversals are same for all cyclic LS of given order N
Number of transversals in cyclic Latin squares: consequence

A090741 (maximum number of transversals in LS):

\[
\begin{align*}
a(11) & \geq 37851 \\
a(13) & \geq 1030367 \\
a(15) & \geq 36362925 \\
a(17) & \geq 1606008513 \\
a(19) & \geq 87656896891 \\
a(21) & \geq 5778121715415 \\
a(23) & \geq 452794797220965 \\
a(25) & \geq 41609568918940625 \\
\end{align*}
\]

Lower bounds can be added to sequence A090741 in OEIS...

- Number of transversals are same for all cyclic LS of given order N
Number of transversals in cyclic diagonal Latin squares: consequence

\[ a(11) \geq 37851 \]
\[ a(13) \geq 1030367 \]
cyclic DLS are not exists for N=15
\[ a(17) \geq 1606008513 \]
\[ a(19) \geq 87656896891 \]
cyclic DLS are not exists for N=21
\[ a(23) \geq 452794797220965 \]
\[ a(25) \geq 41609568918940625 \]

Lower bounds can be added to sequence A287644 in OEIS...

• exists not for all orders N
Number of diagonal transversals in cyclic diagonal Latin squares

Minimal number of diagonal transversals in cyclic DLS of order N=2n+1: 1, 0, 5, 27, 0, 4523, 128818, 0, 204330233, 11232045257 (not presented in OEIS)

Maximal number of diagonal transversals in cyclic DLS of order N=2n+1: 1, 0, 5, 27, 0, 4665, 131106, 0, 204995269, 11254190082 (not presented in OEIS)

Corresponding upper and lower bounds can be added to A287647 (weak) and A287648...
Enumerating the cyclic (diagonal) Latin squares

DLS:

1, 0, 0, 0, 2, 0, 4, 0, 0, 8, 0, 10, 0, 0, 0, 14, 0, 16, 0, 0, 0, 20, 0, 10, 0, 0, 0, 26, 0, 28, ...

Squares of this special type exists not for all orders N.

The number of positive integers k which are \( \leq n \) and where k, k-1 and k+1 are each coprime to n (well known numerical series that directly not connected with Latin squares!).

LS:

1, 1, 2, 2, 4, 2, 6, 4, 6, 4, 10, 4, 12, 6, 8, 8, 16, 6, 18, 8, ...

Euler totient function \( \phi(N) \!!!

Not connected directly with Latin squares! Can be calculated through Latin squares...
Euler totient function calculating

\[ n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_m^{\alpha_m} \]

\[ \varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_m}\right) \]

\[ 6 = 2^1 \cdot 3^1, \quad \varphi(6) = 6 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 2 \]

- calculating by definition (enumerating coprimes (k, n), k < n, Euclid algorithm)
- calculating using factoring and formula
- new method: calculating by enumerating cyclic Latin squares of order n
Euler totient function calculating by enumerating cyclic Latin squares

\[ \varphi(6) = 2 \]

- polynomial algorithm (t\(\sim O(N^2)\), m\(\sim O(N)\)) without multiplications and divisions
### Euler totient function OEIS description slightly expanded

**OEIS Description**

The **Euler totient function** is a mathematical function that counts the positive integers up to a given integer *n* that are relatively prime to *n*. It is denoted as φ(*n*). The function is defined as:

\[
\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)
\]

**Properties**

- **Prime Numbers**: \(\phi(p) = p - 1\) for prime *p*.
- **Composite Numbers**: \(\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)\), where the product is over all distinct prime factors of *n*.

**Python Example**

```python
def euler_phi(n):
    if n == 1:
        return 1
    phi = n
    for p in range(2, int(n**0.5) + 1):
        if n % p == 0:
            while n % p == 0:
                n //= p
            phi -= phi // p
            break
    if n > 1:
        phi -= phi // n
    return phi
```

**Mathematical Properties**

- **Multiplicative**: \(\phi(mn) = \phi(m) \phi(n)\) if *m* and *n* are coprime.
- **Euler's Theorem**: If *a* and *n* are coprime, then \(a^{\phi(n)} \equiv 1 \pmod{n}\).

**Further Reading**

- [OEIS A000010](https://oeis.org/A000010)
- [OEIS A000011](https://oeis.org/A000011)
- [OEIS A000012](https://oeis.org/A000012)

---

**Example**

The function is used in various areas of mathematics, including cryptography, number theory, and combinatorics. It helps in understanding the structure of integers and their divisibility properties.
Euler totient function calculating by enumerating cyclic Latin squares: practice implementation

- slower than factorization based calculating
- slower than long arithmetic implementation (estimation)
Brief conclusion

• new numerical series was calculated
• new upper and lower bounds for some series was established
• interconnections between Latin squares and different type combinatorial objects was established
• new method of Euler totient function calculating based on Latin squares was proposed
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!

E-mail: evatutin@rambler.ru
LJ: http://evatutin.livejournal.com
Skype: evatutin