

## Algorithm for the fast generation of Latin squares

Carolin Hannusch \*

Roland Major †

*Faculty of Informatics*

*University of Debrecen*

*Kassai út 26*

*Debrecen 4028*

*Hungary*

Marco Pavone §

*Dipartimento di Ingegneria*

*Università degli Studi di Palermo*

*Palermo 90128*

*Italy*

---

### Abstract

We introduce an algorithm for the fast generation of Latin squares. Considering Latin squares with  $n$  rows and columns, we introduce a map which maps one square to another one of opposite parity. This map is not unique and it is determined by two indices, i.e. two single numbers. These numbers can be used as secret key in cryptographic schemes which are build up on Latin squares. Thus the introduced algorithm can be applied in cryptography. Additionally, we give a theoretical upper bound for the number of Latin squares of order  $n$ .

---

**Subject Classification:** 05B15, 94A60, 65Y20.

**Keywords:** *Generating discrete structures, Number of Latin squares, Cryptographic scheme, Alon-Tarsi conjecture.*

---

\* ORCID-ID: 0000-0002-0098-7293

† ORCID-ID: 0009-0000-3323-3327

§ ORCID-ID: 0000-0002-8674-5841

---

\* E-mail: [hannusch.carolin@inf.unideb.hu](mailto:hannusch.carolin@inf.unideb.hu) (Corresponding Author)

† E-mail: [major.sandor@inf.unideb.hu](mailto:major.sandor@inf.unideb.hu)

§ E-mail: [marco.pavone@unipa.it](mailto:marco.pavone@unipa.it)

## 1. Introduction

Latin squares are  $n \times n$  arrays containing  $n$  distinct symbols in each row and each column. They have a long history - see for example the Problem of 36 officers [1] and they are still objects of active research. For some general basics on Latin squares we direct the reader to [2].

Latin squares have many applications. One important area of applications is cryptography. The reader can find more details on cryptographic schemes using Latin squares for example in [3], [4], [5] and [6]. Furthermore, Latin squares can be also considered as matrices for cryptographic schemes, which are widely investigated, see for example [7], as the fast development of cryptography requires new ideas constantly.

The purpose of the present paper is to introduce a map on Latin squares which defines orbits. We use these orbits for a fast generation of Latin squares. Furthermore, this construction can be used to create public and private keys for asymmetric cryptographic schemes.

## 2. Definitions and Notations

Throughout this paper,  $n$  denotes a natural number.

**Definition 1:** Let  $H$  be a set of  $n$  different symbols. A Latin square with  $n$  rows and columns is an  $n \times n$  array such that all rows and columns contain all elements of  $H$ .

**Definition 2:** A permutation on a set of  $n$  elements is an arrangement of these elements.

Usually, the  $n$  different symbols in a Latin squares are the natural numbers from 1 to  $n$ . Then every row and every column can be regarded as a permutation on the set  $\{1, \dots, n\}$ .

We denote the row permutations of a Latin square by  $\sigma_1, \dots, \sigma_n$  and the column permutations by  $\tau_1, \dots, \tau_n$ .

**Definition 3:** Let  $\lambda$  be a Latin square of order  $n$ . We say that  $\lambda$  is a reduced Latin square if  $\sigma_1 = 1_{\text{id}}$  and  $\tau_1 = 1_{\text{id}}$ , where  $1_{\text{id}}$  denotes the identity permutation, i.e. its first row and first column are in natural order  $1 < \dots < n$ .

Let us denote the set of Latin squares with  $n$  rows by  $L_n$  and the set of reduced Latin squares with  $n$  rows by  $R_n$ . It is well known that  $\#L_n = n!(n-1)!\#R_n$ , where  $\#L_n$  denotes the size of the set containing all Latin squares of order  $n$  and  $\#R_n$  denotes the size of the set containing all reduced Latin squares of order  $n$ .

**Definition 4:** A pair of numbers  $x$  and  $y$  in a permutation with  $x > y$  and  $x$  preceding  $y$  in the permutation is called *inversion*. The *inversion number* of a permutation is the sum of all inversions. A permutation is called *odd* (*even*), if its number of inversions is odd (even respectively).

It is also common to denote the parity of a permutation  $\sigma$  by its signum:

$$\text{sgn}(\sigma) = 1 \text{ if } \sigma \text{ is even and } \text{sgn}(\sigma) = -1 \text{ otherwise.}$$

We know that the product of two odd permutations is an even permutation, and multiplying two even permutations gives an even permutation as well. Whereas, the product of an even and an odd permutation (or the other way round) results in an odd permutation [8].

**Definition 5:** Let  $\lambda$  be a Latin square with its row permutations  $\sigma_1, \dots, \sigma_n$  and its column permutations  $\tau_1, \dots, \tau_n$ . If

$$\text{sgn}\left(\prod_{i=1}^n \sigma_i \tau_i\right) = 1,$$

then  $\lambda$  is called even Latin square. Otherwise  $\lambda$  is called odd Latin square.

### 3. A map switching between even and odd Latin squares

In this section, we introduce a map that can be defined on a big class of Latin squares. With the help of this definition, we can map an even Latin square to an odd one and vice versa. Furthermore, this map defines orbits on the set of Latin squares of a given order  $n$ .

#### 3.1 Definition of the map

**Definition 6:** Let  $\lambda$  be a Latin square. We define the map  $m_{i,j}$  on  $\lambda$  for a pair of rows (columns) in the following way: If the product of the row permutations  $\sigma_i^{-1}\sigma_j$  (column permutations  $\tau_i^{-1}\tau_j$  respectively), where  $i \neq 1, j \neq 1$ , is such that the cycle containing  $i$  and  $j$  has odd length, then  $m_{i,j}(\lambda)$  is defined as follows: Now, we don't move the elements  $i,j$  and all other elements of the cycle containing  $i,j$  in  $\sigma_i^{-1}\sigma_j$  (in  $\tau_i^{-1}\tau_j$  respectively). Interchange all other elements of the  $i^{\text{th}}$  and the  $j^{\text{th}}$  row (column). All other rows (columns) are the same as in  $\lambda$ .

**Proposition 1:** Let  $n$  be an even natural number and  $\lambda$  be a Latin square of order  $n$ . Further,  $m_{i,j}$  is defined on  $\lambda$  by Definition 6.

$$\text{Then } \text{sgn}(m_{i,j}(\lambda)) = -\text{sgn}(\lambda).$$

**Proof:** Multiplying all row and column permutations of  $m_{i,j}(\lambda)$  has the same result as multiplying all row and column permutations of  $\lambda$  multiplied by an odd number of transpositions.

**Example 1:** First we introduce the Latin square  $\lambda$ :

|   |   |   |   |   |   |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 1 | 5 | 6 | 3 | 4 |
| 3 | 6 | 1 | 5 | 4 | 2 |
| 4 | 3 | 2 | 1 | 6 | 5 |
| 5 | 4 | 6 | 2 | 1 | 3 |
| 6 | 5 | 4 | 3 | 2 | 1 |

Multiplying all row and column permutations, we get an odd permutation, thus  $\lambda$  is a Latin square which is odd and reduced. We have  $\sigma_2^{-1} \sigma_3 = (1, 6, 5)(2, 3, 4)$ .

Thus  $m_{2,3}(\lambda)$  is the following Latin square:

|   |   |   |   |   |   |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 6 | 1 | 5 | 3 | 4 |
| 3 | 1 | 5 | 6 | 4 | 2 |
| 4 | 3 | 2 | 1 | 6 | 5 |
| 5 | 4 | 6 | 2 | 1 | 3 |
| 6 | 5 | 4 | 3 | 2 | 1 |

Multiplying all row and column permutations, we get an even permutation, therefore  $m_{2,3}(\lambda)$  is an even reduced Latin square.

**Proposition 2:** Let  $\lambda$  be a reduced Latin square of order  $n$  and  $m_{i,j}$  is defined on  $\lambda$  by Definition 6. Then  $m_{i,j}(\lambda)$  is also a reduced Latin square.

**Proof:** By Definition 6, the map  $m_{i,j}$  always fixes the first row and first column.

We denote the map  $m: A \rightarrow B$ , if there exists a pair  $(i,j)$  such that for some  $\lambda \in A$  we have  $m_{i,j}(\lambda) \in B$ . The map  $m: R_{\text{odd}} \rightarrow R_{\text{even}}$  is not injective. For example, the even reduced Latin square

|   |   |   |   |   |   |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 1 | 4 | 3 | 6 | 5 |
| 3 | 4 | 5 | 6 | 2 | 1 |
| 4 | 3 | 6 | 5 | 1 | 2 |
| 5 | 6 | 1 | 2 | 3 | 4 |
| 6 | 5 | 2 | 1 | 4 | 3 |

has three preimages:

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 1 | 2 | 3 | 4 | 5 | 6 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 1 | 4 | 3 | 6 | 5 | 2 | 4 | 5 | 3 | 6 | 1 | 2 | 5 | 4 | 1 | 6 | 3 |
| 3 | 5 | 2 | 6 | 4 | 1 | 3 | 1 | 4 | 6 | 2 | 5 | 3 | 4 | 5 | 6 | 2 | 1 |
| 4 | 3 | 6 | 5 | 1 | 2 | 4 | 3 | 6 | 5 | 1 | 2 | 4 | 3 | 6 | 5 | 1 | 2 |
| 5 | 6 | 1 | 2 | 3 | 4 | 5 | 6 | 1 | 2 | 3 | 4 | 5 | 6 | 1 | 2 | 3 | 4 |
| 6 | 4 | 5 | 1 | 2 | 3 | 6 | 5 | 2 | 1 | 4 | 3 | 6 | 1 | 2 | 3 | 4 | 5 |

### 3.2 Orbits

It is clear that if  $m_{i,j}(\lambda)$  is defined for a Latin square  $\lambda$ , then  $m_{i,j}(m_{i,j}(\lambda)) = \lambda$ , i.e. the map  $m$  is an involution. In this section we will also consider the composition of maps  $m_{i,j}$  and  $m_{k,l}$ , which means  $m_{i,j} \circ m_{k,l}(\lambda) = m_{i,j}(m_{k,l}(\lambda))$ .

Now, we consider the set  $H_\lambda$  for a given Latin square  $\lambda$ , which contains all Latin squares which can be obtained from  $\lambda$  by applying any composition of maps  $m$ . Let  $\lambda \in R_n$  and  $m_{i_1,j_1}, \dots, m_{i_t,j_t}$  be all maps which can be defined on  $\lambda$  and its images. Thus

$$H_\lambda = \{\Lambda \mid \Lambda = m_{i_1,j_1} \circ \dots \circ m_{i_t,j_t}(\lambda)\},$$

where  $\{i_1, \dots, i_t\} \subseteq \{1, \dots, t\}$ .

Then  $H_\lambda \subseteq R_n$ .

**Definition 7:** We say that the set  $H_\lambda$  is the orbit of  $\lambda$ . For a given number  $n$ , we denote the number of orbits on  $R_n$  by  $v$ .

**Remark 1:** Note that in the composition of the maps  $m$ , some can be applied on rows while others can be applied on columns.

**Proposition 3:** If  $\lambda_2 \notin H_{\lambda_1}$ , then  $H_{\lambda_1} \cap H_{\lambda_2} = \emptyset$ .

**Conjecture 1:** For a given number  $n$ , let  $\lambda_1, \dots, \lambda_v$  be representants of the  $v$  distinct orbits on  $R_n$ . Then  $R_n \setminus (H_{\lambda_1} \cup \dots \cup H_{\lambda_v}) \subseteq R_{\text{even}}$ .

In other words, we conjecture that  $m: R_{\text{even}} \rightarrow R_{\text{odd}}$  is surjective.

## 4. Generating Latin squares

In this section, we introduce an algorithm for the fast generation of Latin squares. This algorithm is based on the map introduced in Section 3.1. Further, we give some application possibility for the introduced algorithm and investigate its performance.

#### 4.1 Algorithm

##### Algorithm 1 Generation of Latin squares with $n$ rows and columns

**Require:**  $\lambda$  Latin square with  $n$  rows and columns, natural number  $s$

**Ensure:** other Latin square with  $n$  rows and columns

```

1:  $(i_1/j_1), \dots, (i_s/j_s) \leftarrow (\{2, \dots, n\} \times \{2, \dots, n\})^s$ 
2:  $b \leftarrow \{0, 1\}^s$ 
3:  $k \leftarrow 0$ 
4: while  $k \leq s$  do
5:    $k \leftarrow k + 1$ 
6:   if  $b[k] = 0$  then
7:     apply  $m_{ik,jk}$  on the rows of  $\lambda$ 
8:      $\lambda := m_{ik',jk}(\lambda)$ 
9:   end if
10:  if  $b[k] = 1$  then
11:    apply  $m_{ik',jk}$  on the columns of  $\lambda$ 
12:     $\lambda := m_{ik,jk}(\lambda)$ 
13:  end if
14: end while
15:  $\lambda \leftarrow m_{is,js}(\lambda)$ 

```

#### 4.2 Application in cryptography

If a cryptographic scheme uses Latin squares, the algorithm described in Section 4.1 can help to make it more secure.

Given a Latin square  $\lambda$ , we can determine a composition of maps  $m_{i_1/j_1}, \dots, m_{i_s/j_s}$  and in the cryptographic scheme the Latin square  $m_{i_1/j_1} \circ \dots \circ m_{i_s/j_s}(\lambda)$  is used.

**Public key:** the pairs  $(i_1/j_1), \dots, (i_s/j_s)$

**Private key:**  $b = (b_1, \dots, b_s) \in \{0, 1\}^s$

The vector  $b$  contains the information if  $m_{ik,jk}$  should be applied on the rows or on the columns of the previous square in the composition.

The advantage of this method is that  $\lambda$  and the pairs  $(i_1/j_1), \dots, (i_s/j_s)$  can be shared on different channels.

**Remark 2:** For a successful application one needs to make sure previously that  $m_{i_1/j_1} \circ \dots \circ m_{i_s/j_s}(\lambda)$  is defined, i.e. this Latin square exists.

4.3 The case  $n = 6$ 

In the case of Latin squares of order 6, we can show by computation that Conjecture 1 is true. In this case, we have 21 orbits, details below. We give a representant  $\lambda$  for each orbit by its row permutations  $\sigma_2, \dots, \sigma_6$ .

**Table 1**  
**The 21 orbits on  $R_6$**

| Odd  | Even | $\sigma_2$   | $\sigma_3$   | $\sigma_4$   | $\sigma_5$   | $\sigma_6$   |
|------|------|--------------|--------------|--------------|--------------|--------------|
| 24   | 24   | (12)(34)(56) | (135)(246)   | (14)(25)(36) | (153)(264)   | (16)(23)(45) |
| 216  | 288  | (12)(34)(56) | (135)(246)   | (142536)     | (154)(263)   | (164523)     |
| 216  | 288  | (12)(34)(56) | (135)(246)   | (145263)     | (154236)     | (164)(253)   |
| 216  | 288  | (12)(34)(56) | (135)(246)   | (145326)     | (152364)     | (163)(254)   |
| 216  | 288  | (12)(34)(56) | (135246)     | (1425)(36)   | (153264)     | (1623)(45)   |
| 24   | 24   | (12)(34)(56) | (135246)     | (145)(263)   | (154)(236)   | (164253)     |
| 24   | 24   | (12)(34)(56) | (136245)     | (146)(253)   | (154263)     | (164)(235)   |
| 24   | 24   | (12)(34)(56) | (136)(245)   | (14)(26)(35) | (15)(23)(46) | (163)(254)   |
| 1152 | 1800 | (12)(34)(56) | (13)(25)(46) | (14)(26)(35) | (15)(24)(36) | (16)(23)(45) |
| 216  | 288  | (12)(3456)   | (135)(246)   | (142653)     | (152364)     | (16)(2543)   |
| 216  | 288  | (12)(3456)   | (13)(25)(46) | (142365)     | (154326)     | (1624)(35)   |
| 24   | 24   | (12)(35)(46) | (134)(256)   | (143)(265)   | (15)(24)(36) | (16)(23)(45) |
| 24   | 24   | (12)(35)(46) | (136254)     | (145263)     | (156)(243)   | (165)(234)   |
| 24   | 24   | (123)(456)   | (132)(465)   | (14)(25)(36) | (15)(26)(34) | (16)(24)(35) |
| 216  | 288  | (123)(456)   | (135)(246)   | (143652)     | (153426)     | (163254)     |
| 216  | 288  | (123)(456)   | (136524)     | (1435)(26)   | (154632)     | (16)(2534)   |
| 216  | 288  | (123)(456)   | (136254)     | (146532)     | (15)(2634)   | (16)(2435)   |
| 216  | 288  | (123456)     | (132465)     | (14)(25)(36) | (1543)(26)   | (1642)(35)   |
| 24   | 24   | (124)(356)   | (13)(25)(46) | (142)(365)   | (15)(26)(34) | (16)(23)(45) |
| 24   | 24   | (125)(346)   | (13)(24)(56) | (14)(26)(35) | (152)(364)   | (16)(23)(45) |
| 24   | 24   | (126)(345)   | (13)(24)(56) | (14)(25)(36) | (15)(23)(46) | (162)(354)   |

It is known (A000315) that  $R_6 = 9408$ . In Table 1 we found in sum 8472 reduced Latin squares. The missing 936 squares are all even and are not images of any other Latin square by the map  $m$ . Therefore, the map  $m: R_{\text{odd}} \rightarrow R_{\text{even}}$  is not surjective.

It is interesting, that there are ten orbits of size 48 and ten orbits of size 504, one of size 2952. All orbits of size 48 have the same number of odd and even squares, whereas in the other orbits there are more even squares than odd squares.

#### 4.4 Performance

An orbit as described in Section 3.2 can be considered as a graph. Therefore, in order to compute all possible images of a given Latin square, one can use any graph searching algorithm.

For  $n \geq 8$ , the computation of all orbits seems to take a lot of time. Therefore we give some measurements of how many squares we can compute by our implementation of a breadth-first search.

**Table 2**  
**Performance of a breadth-first search of orbits on 4.3 GHz processor**

| n  | number of generated squares | time in sec |
|----|-----------------------------|-------------|
| 8  | 1000                        | 0.0824      |
| 8  | 10000                       | 0.8361      |
| 8  | 100000                      | 8.3486      |
| 10 | 1000                        | 0.1049      |
| 10 | 10000                       | 0.9876      |
| 10 | 100000                      | 9.6497      |
| 12 | 1000                        | 0.2109      |
| 12 | 10000                       | 2.1682      |
| 12 | 100000                      | 28.1867     |

### 5. Upper bound for the number of Latin squares

For a given number  $n$ , we denote the number of orbits induced by the maps  $m$  by  $\nu$ . Further, the longest orbit has length  $l$ , then the following upper bound applies

$$\#R_n \leq l \cdot \nu,$$

and therefore we have the following upper bound for the number of Latin squares of order  $n$ :

$$\#L_n \leq (n-1)! \cdot n! \cdot l \cdot \nu.$$

In the case  $n = 6$ , we get here

$$\#R_6 \leq 2952 \cdot 21 = 61992,$$

which is a much smaller upper bound than the best known upper bound  $R_6 \leq 9953280$ , since  $n!$  by Alter [9].

$$R_n \leq \prod_{k=1}^{n-1} (n-k)^{k-1} (n-k)$$

The given upper bound is rather theoretical, since for  $n \geq 8$  we could not succeed in computing all orbits yet.

## 6. Connection to Alon-Tarsi conjecture

If  $n$  is an even (positive) integer, then the size of the set containing all even Latin squares with  $n$  rows and columns is not equal to the size of the set containing all odd Latin squares for known cases [10], [11]. The Alon-Tarsi conjecture says that this statement is true for all even positive integers  $n$ . The conjecture is known to be true in a special case in [12], but remains unsolved in general.

If  $n$  is odd, then it is well known that the number of odd squares is equal to the number of even squares, since switching two rows or two columns changes the sign and every permutation can be obtained by the composition of transpositions [2]. Switching rows or columns does not change the sign of a Latin square for even  $n$ .

For  $n = 6$ , we have proven in Table 1 that  $\#R_{\text{even}} > \#R_{\text{odd}}$  by showing that the map  $m: R_{\text{even}} \rightarrow R_{\text{odd}}$  is surjective. This makes us believe that for all even  $n$ , the number of even reduced Latin squares may be greater than the number of odd reduced Latin squares.

**Conjecture 2:**  $\#R_{\text{even}} > \#R_{\text{odd}}$  for even  $n$ .

## 7. Conclusion

In this paper, we gave the mathematical background of a new map on Latin squares. This map can be used to generate Latin squares of opposite parity. Further, we introduce an algorithm built up on the introduced map which makes it possible to generate many Latin squares fast. The introduced construction can be applied in cryptographic schemes since the map's data can be used as private and public keys. In addition, we found a new theoretical upper bound for the number of Latin squares of order  $n$ . The numbers of even and odd reduced Latin squares of a given order  $n$  seem to behave not in direct proportion to the numbers of even and odd Latin squares, which need to be investigated further in more

detail. Furthermore, cryptographic schemes based on the given mathematical construction can be developed and investigated.

**Supplementary information:** A program for the computation of the 21 orbits can be found here: Python program - orbits (txt file)

A program of the computation of 936 even squares which are not images of the map and a program for computing running times can be found here Python program - non images and runtimes (zip file)

## Declarations

**Conflict of interests:** None of the authors has to disclose any financial or non-financial interest.

## References

- [1] G. Tarry, "Le probleme des 36 officiers," *Comptes rendus Ass. Fr. pour l'Avancement de Science Naturel*, vol. 1, pp. 122–123 (1900).
- [2] A. D. Keedwell and J. Dénes, *Latin Squares and Their Applications*. Amsterdam, Netherlands: North-Holland (2015).
- [3] N. O. Schmidt, "Latin squares and their applications to cryptography," M.Sc. thesis, Boise State University, Idaho, USA (2016).
- [4] Y. Ren, F. Liu, T. Guo, R. Feng, and D. Lin, "Cheating prevention visual cryptography scheme using Latin square," *IET Information Security*, vol. 11, no. 4, pp. 211–219 (2017).
- [5] S. K. Pal, S. Kapoor, A. Arora, R. Chaudhary, and J. Khurana, "Design of strong cryptographic schemes based on Latin squares," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 13, no. 3, pp. 233–256 (2010).
- [6] A. Desoky, H. Ammar, G. Fahmy, S. El-Sappagh, A. Hendawi, and S. H. Basha, "Latin square and artificial intelligence cryptography for blockchain and centralized systems," in *Proc. Int. Conf. on Advanced Intelligent Systems and Informatics*, pp. 444–455 (2023).
- [7] S. S. Kumar and S. A. Sherfin, "A cryptographic encryption technique byte – spiral rotation encryption algorithm," *Journal of Discrete Math-*

- ematical Sciences and Cryptography*, vol. 22, no. 3, pp. 371–376 (2019).  
<https://doi.org/10.1080/09720529.2019.1578083>.
- [8] N. Jacobson, *Basic Algebra I*. New York, NY, USA: Courier Corporation (2012).
- [9] R. Alter, “How many Latin squares are there?” *The American Mathematical Monthly*, vol. 82, no. 6, pp. 632–634 (1975).
- [10] N. Alon and M. Tarsi, “Colorings and orientations of graphs,” *Combinatorica*, vol. 12, pp. 125–134 (1992).
- [11] A. A. Drisko, “On the number of even and odd Latin squares of order  $p + 1$ ,” *Advances in Mathematics*, vol. 128, no. 1, pp. 20–35 (1997).
- [12] A. A. Drisko, “Proof of the Alon-Tarsi conjecture for  $n = 2^r p$ ,” *Electronic Journal of Combinatorics*, vol. 5, no. 1, p. 28 (1998).

*Received September, 2024*