On the fractal dimension of strongly isotopism classes of Latin squares



Raúl M. Falcón

Department of Applied Maths I. Universidad de Sevilla. rafalgan@us.es

CDC 2021 Combinatorial Designs and Codes Rijeka, July 12, 2021.





▲ 同 ▶ ▲ 国 ▶ ▲ 国



CONTENTS

Preliminaries.

Standard sets of image patterns.

• The mean fractal dimension.

CONTENTS

• Preliminaries.

Standard sets of image patterns.

• The mean fractal dimension.

Quasigroups and Latin squares.



A quasigroup of order *n* is a pair (Q, \cdot) formed by

- a finite set Q of n elements
- a product · endowed of left and right division. Its multiplication table is a **Latin square**.

Ruth Moufang (1935)

$$S_n \equiv$$
 Symmetric group on $\{1, \ldots, n\}$.

Isotopism: $\Theta = (f, g, h) \in S_n^3$

Row-permutation (f), column-permutation (g), symbol-permutation (h).

- $f = g = h \Rightarrow$ Isomorphism.
- $f = g \Rightarrow$ Strong isotopism.

$$L \equiv \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix} \Rightarrow \begin{bmatrix} 2 & 3 & 1 \\ 2 & 3 & 1 \\ 1 & 2 & 3 \end{bmatrix}$$
$$\Theta = ((1 \ 2)(3), (1 \ 2)(3), (2 \ 3)(1)) \in S_3^3$$

Latin squares as scramblers in Cryptography.

[V. Dimitrova V., S. Markovski, 2007] Classification of quasigroups by image patterns. Proc. 5th CIIT, 152-160.



Vesna Dimitrova



Smile Markovski

 $\begin{cases} Q \equiv \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \\ T = 122333122333 \end{cases}$

- A quasigroup (Q, \cdot)
- A plaintext $T = t_1 \dots t_m$, with $t_i \in Q$
- A leader symbol $s \in Q$

Encryption: $E_s(T) = e_1 \dots e_m$

$$e_i := \left\{ egin{array}{ll} s \cdot t_1, & ext{if } i=1, \ e_{i-1} \cdot t_i, & ext{otherwise.} \end{array}
ight.$$

$$\Rightarrow \begin{cases} E_1(T) = 123213312132\\ E_2(T) = 231321123213\\ E_3(T) = 312132231321 \end{cases}$$

• • = • • = •

[V. Dimitrova V., S. Markovski, 2007] Classification of quasigroups by image patterns. Proc. 5th CIIT, 152-160.



• A quasigroup (Q, \cdot)

- A plaintext $T = t_1 \dots t_m$
- A tuple of leader symbols $S = (s_1, \ldots, s_{r-1})$

Vesna Dimitrova



Smile Markovski



Image pattern: $\mathcal{P}_{S,T} = (p_{ij})$

$$p_{ij} := \left\{ egin{array}{ll} t_j, & \mbox{if } i = 1, \ s_{i-1} \cdot p_{i-1,1}, & \mbox{if } i > 1 \ \mbox{and } j = 1, \ p_{i,j-1} \cdot p_{i-1,j}, & \mbox{otherwise.} \end{array}
ight.$$

Raúl M. Falcón

Fractal dimension of strongly isotopism classes of LS 6/32







 7×5 collage of image patterns arising from 35 Latin squares





Fractal quasigroups Designing error detecting codes.

Non-fractal quasigroups Designing cryptographic primitives.

Open problem: A comprehensive analysis of their fractal dimensions.

There is an interesting relation with Latin square isomorphisms:

Lemma (F., Álvarez, Gudiel, 2019)

- Two isomorphic Latin squares L_1 and L_2 by means of isomorphism f
- A plaintext T
- A tuple of leader symbols S

Then, $\mathcal{P}_{S,T}(L_1)$ and $\mathcal{P}_{f(S),f(T)}(L_2)$ coincide up to permutation f of their symbols.

Main question: Can we use image patterns for distinguishing non-isomorphic Latin squares?

CONTENTS

Preliminaries.

Standard sets of image patterns.

• The mean fractal dimension.

- $L \in \mathcal{LS}_n$.
- $T = s \dots s$ of length m, with $s \leq n$.
- $S = (s, \ldots, s)$ of length r 1.

s-standard $r \times m$ image pattern: $\mathcal{P}_{r,m;s}(L) = \mathcal{P}_{S,T}(L)$. Standard set of $r \times m$ image patterns of *L*: $\{\mathcal{P}_{r,m;s}(L): s \in \{1, ..., n\}\}$

$$n = 4$$
$$r = m = 90$$

1 2 4	2 1 3	3 4 1	4 3 2	\Rightarrow		
3	4	2	1		and a subar a s	

Proposition

The $r \times m$ standard sets of two isomorphic Latin squares coincide, up to permutation of colors.



1 2 3 4	1 2 3 4	1 2 3 4	1 2 3 4	1 2 3 4
2 1 4 3	2 1 4 3	2 3 4 1	3 1 4 2	3 4 1 2
4 3 1 2	4 3 2 1	4 1 2 3	4 3 2 1	4 3 2 1
3 4 2 1	3 4 1 2	3 4 1 2	2 4 1 3	2 1 4 3
L4.1	L4.2	L4.3	L4.4	L _{4.5}
1 2 4 3	1 2 4 3	1 2 4 3	1 2 4 3	1 2 4 3
2 1 3 4	2 1 3 4	2 1 3 4	2 1 3 4	2 3 1 4
3 4 1 2	3 4 2 1	4 3 1 2	4 3 2 1	3 4 2 1
4 3 2 1	4 3 1 2	3 4 2 1	3 4 1 2	4 1 3 2
L46	L47	L48	L4.9	L4 10
1 2 4 3	1 2 4 3	1 2 4 3	1 2 4 3	1 2 4 3
2 3 1 4	3 1 2 4	3 1 2 4	3 4 1 2	3 4 2 1
4 1 3 2	2 4 3 1	4 3 1 2	2 1 3 4	2 1 3 4
3 4 2 1	4 3 1 2	2 4 3 1	4 3 2 1	4 3 1 2
L4 11	L4 12	L4 13	L4 14	L4 15
1243	1243	1 2 4 3	1 3 4 2	1 3 4 2
3 4 2 1	3 4 2 1	3 4 2 1	2 1 3 4	2 1 3 4
2 3 1 4	4 1 3 2	4 3 1 2	3 4 2 1	4 2 1 3
4 1 3 2	2 3 1 4	2 1 3 4	4 2 1 3	3 4 2 1
L416	LA 17	L4.18	L4 10	L120
1 3 4 2	1342	1342	1342	2 1 3 4
2 4 2 1	2 4 3 1	3 1 2 4	4 2 1 2	1 3 4 2
2 1 3 1	4 2 1 2	4 2 1 2	7 2 1 3	2 4 2 1
3 1 2 4	4 2 1 3	4 2 1 3	2 4 3 1	3 4 2 1
4 2 1 5	5 1 2 4	2 4 5 1	5 1 2 4	4 2 1 5
421	L4.22	L4.23	L424	L4.25
2 1 3 4	2 1 3 4	2 1 3 4	2 1 3 4	2 1 3 4
1 3 4 2	3 4 1 2	3 4 2 1	3 4 2 1	3 4 2 1
4 2 1 3	1 2 4 3	1 2 4 3	1 3 4 2	4 2 1 3
3 4 2 1	4 3 2 1	4 3 1 2	4 2 1 3	1 3 4 2
L _{4.26}	L _{4.27}	L _{4.28}	L4.29	L _{4.30}
2 1 3 4	2 3 1 4	2 3 1 4	1 2 3 4	1 2 3 4
3 4 2 1	1 4 2 3	4 1 3 2	2 1 4 3	2 1 4 3
4 3 1 2	3 2 4 1	3 2 4 1	3 4 1 2	3 4 2 1
1 2 4 3	4 1 3 2	1 4 2 3	4 3 2 1	4 3 1 2
L _{4.31}	L _{4.32}	L4.33	L4.34	L4.35



3-standard image patterns

4-standard image patterns

Standard sets of 90×90 image patterns arising from the

35 isomorphism classes of Latin squares of order 4 > < >

Raúl M. Falcón

Fractal dimension of strongly isotopism classes of LS 14/32

i	$\sharp cs_i$	$\sharp \mathbf{fs}_i$	i	‡cs _i	$\sharp fs_i$	i	$\sharp cs_i$	 ♯fs _i
1	1	3	13	1	0	25	0	0
2	1	3	14	2	1	26	0	0
3	1	0	15	2	2	27	0	0
4	1	1	16	1	0	28	0	4
5	1	3	17	3	0	29	0	0
6	1	3	18	2	2	30	0	0
7	1	3	19	1	1	31	0	4
8	1	3	20	1	0	32	0	4
9	1	3	21	1	3	33	0	4
10	1	0	22	2	2	34	1	3
11	2	0	23	1	3	35	1	3
12	2	1	24	4	0			

Number of constant and fractal 90 \times 90 standard image patterns of the

35 isomorphism classes of Latin squares of order 4.

i	$\sharp cs_i$	$\sharp \mathbf{fs}_i$	i	‡cs _i	♯ fs _i	i	$\sharp cs_i$	₿fs _i
1	1	3	13	1	0	25	0	0
2	1	3	14	2	1	26	0	0
3	1	0	15	2	2	27	0	0
4	1	1	16	1	0	28	0	4
5	1	3	17	3	0	29	0	0
6	1	3	18	2	2	30	0	0
7	1	3	19	1	1	31	0	4
8	1	3	20	1	0	32	0	4
9	1	3	21	1	3	33	0	4
10	1	0	22	2	2	34	1	3
11	2	0	23	1	3	35	1	3
12	2	1	24	4	0			

Number of constant and fractal 90 \times 90 standard image patterns of the

35 isomorphism classes of Latin squares of order 4.









Standard sets of 90×90 image patterns arising from the

35 isomorphism classes of Latin squares of order 4. э

Raúl M. Falcón

Fractal dimension of strongly isotopism classes of LS 17 / 32



Standard 3×3 image patterns of five distinct isomorphism classes

Can we find an efficient method for distinguishing standard sets?

CONTENTS

Preliminaries.

Standard sets of image patterns.

• The mean fractal dimension.

Raúl M. Falcón Fractal dimension of strongly isotopism classes of LS 19/32

Homogenized standard sets.

 $\mathfrak{P}_n = \{c_1, \ldots, c_n\} \equiv \text{Grayscale palette such that Intensity}(c_i) = \frac{i}{n}$.

A standard set of image patterns of a Latin square of order n is said to be **homogenized** if the colors of \mathfrak{P}_n appear in natural order (according to their intensity) when the image pixels are read row by row then column by column.

 $\mathcal{H}_{r,m}(L) \equiv$ Set of homogenized standard sets of $L \in LS_n$.



Homogenized standard sets.

 $\mathfrak{P}_n = \{c_1, \ldots, c_n\} \equiv \text{Grayscale palette such that Intensity}(c_i) = \frac{i}{n}$.

A standard set of image patterns of a Latin square of order n is said to be **homogenized** if the colors of \mathfrak{P}_n appear in natural order (according to their intensity) when the image pixels are read row by row then column by column.

 $\mathcal{H}_{r,m}(L) \equiv$ Set of homogenized standard sets of $L \in LS_n$.



Differential box-counting fractal dimension.

 L∈ LS_n. Div(r, m)≡ Common divisors of r and m.
 I_{i,j,k}(P_{r,m;s}(L))≡ Range of gray-level intensities in the (i, j)-cell of the r/k × m/k grid of P_{r,m;s}(L), with k ∈ Div(r, m). I_k(P_{r,m;s}(L)) := ∑ (1 + I_{i,j,k}(P_{r,m;s}(L))).

Based on the *differential box-counting method*, we define the **differential box-counting fractal dimension** $D_B(\mathcal{P}_{r,m;s}(L))$ of $\mathcal{P}_{r,m;s}(L)$ as the slope of the linear regression line of the set of points

 $\{(\log(I_k(\mathcal{P}_{r,m;s}(L))), \log(1/k)): k \in \mathrm{Div}(r,m)\}.$



Mean fractal dimension.

The mean value of the *n* differential box-counting fractal dimensions, averaged over Div(r, m), is the **mean fractal dimension** $D_B(\mathcal{H}_{r,m}(L))$.

Theorem

• $L_1, L_2 \in LS_n$.

If L_1 and L_2 are isomorphic, then $D_B(\mathcal{H}_{r,m}(L_1)) = D_B(\mathcal{H}_{r,m}(L_2))$.

	$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$	$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$
$D_B(\mathcal{P}_{90;1}(L))$	2.00000	2.00000	2.00000
$D_B(\mathcal{P}_{90;2}(L))$	1.95165	1.95165	1.92136
$D_B(\mathcal{P}_{90;3}(L))$	1.8877	1.88873	1.92331
$D_B(P_{90;4}(L))$	1.8877	1.88873	1.90088
$D_B(\mathcal{H}_{90}(L))$	1.9317625	1.9322775	1.9363875



Mean fractal dimension.

п	\in	{3,	4
---	-------	-----	---

n	i	$D_B(n, i)$	n	i	$D_B(n, i)$	n	i	$D_B(n, i)$	n	i	$D_B(n, i)$
3	1	1.9285267	4	30	1.9212575	4	35	1.9338325	4	23	1.9428575
	5	1.9335900		29	1.9213650		19	1.9357400		15	1.9472450
	2	1.9524867		27	1.9215325		21	1.9359200		12	1.9476600
	3	1.9527467		25	1.9216950		4	1.9363875		22	1.9495350
	4	2.0000000		7	1.9230125		5	1.9366250		18	1.9504400
4	32	1.9072150		8	1.9274475		20	1.9411800		14	1.9511850
	28	1.9099250		9	1.9285825		13	1.9411950		11	1.9606500
	33	1.9137400		2	1.9296225		16	1.9413250		34	1.9637375
	31	1.9139600		1	1.9317625		10	1.9413500		17	1.9807250
	26	1.9210725		6	1.9322775		3	1.9413775		24	2.0000000

$$(r = m = 90)$$





Raúl M. Falcón Fractal dimension of strongly isotopism classes of LS 24 / 32

Mean fractal dimension.



Mean fractal dimension (r = m = 90): 1.88926

Run time: 81.63s in an Intel Core i7-8750H CPU (6 cores), with a 2.2 GHz processor and 8 GB of RAM.

$\mathbf{n} = \mathbf{3}$ (5 isomorphism classes)











Raúl M. Falcón Fractal dimension of strongly isotopism classes of LS 26 / 32

$\underline{\mathbf{n}} = \mathbf{3}$ (5 isomorphism classes)











↓ (Id, Id, (12))



 $\mathbf{n} = \mathbf{3}$ (5 isomorphism classes)



$\underline{\mathbf{n}} = \mathbf{3}$ (5 isomorphism classes)









 \downarrow (Id, Id, (12))



 $\mathbf{n} = \mathbf{3}$ (5 isomorphism classes)



$\mathbf{n} = \mathbf{3}$ (5 isomorphism classes)





 \downarrow (Id, Id, (12))



∃ >

 $\mathbf{n} = \mathbf{3}$ (5 isomorphism classes)



 $\mathbf{n} = \mathbf{3}$ (5 isomorphism classes)



2 strong isotopism classes.

 $\underline{\mathbf{n}} = \underline{\mathbf{4}}$ (35 isomorphism classes)



 $\mathbf{n} = \mathbf{4}$ (35 isomorphism classes)





< ∃ →

Raúl M. Falcón Fractal dimension of strongly isotopism classes of LS 27 / 32

(Id, Id, (12))



3



э

$\mathbf{n} = \mathbf{4}$ (6 strong isotopism classes)









 $\begin{array}{c} 1.9285825\\ 1.9338325\\ 1.9606500\end{array}$



1.9807250

イロト イボト イヨト イヨト



э

REFERENCES

- Dimitrova, V., Markovski, S. Classification of quasigroups by image patterns. In: Proceedings of the Fifth International Conference for Informatics and Information Technology, Bitola, Macedonia, 2007; 152–160.
- Falcón, R.M. A new quasigroup isomorphism invariant arising from fractal image patterns, Quasigroups and Related Systems. Accepted, 2021.
- Falcón, R.M. Recognition and analysis of image patterns based on Latin squares by means of Computational Algebraic Geometry, Mathematics 9 (2021), paper 666, 26 pp.
- Falcón, R.M., Álvarez, V., Gudiel, F. A Computational Algebraic Geometry approach to analyze pseudo-random sequences based on Latin squares, Adv. Comput. Math. 45 (2019), 1769–1792.
- Hulpke, A., Kaski, P., Östergård, P.R.J. The number of Latin squares of order 11, Math. Comp. 80 (2011) no. 274, 1197–1219.
- McKay, B.D., Meynert, A., Myrvold, W. Small Latin Squares, Quasigroups and Loops. J. Combin. Des. 15 (2007), 98–119.
- Sarkar, N., Chaudhuri, B.B., An efficient differential box-counting approach to compute fractal dimension of image, IEEE Trans. Syst. Man Cybern. 24 (1994), 115–120.

↓ ∃ ↓ 4 ∃ ↓ ∃ √Q (~

Many thanks!

On the fractal dimension of strongly isotopism classes of Latin squares



Raúl M. Falcón

Department of Applied Maths I. Universidad de Sevilla. rafalgan@us.es

CDC 2021 Combinatorial Designs and Codes Rijeka, July 12, 2021.





・ 同 ト ・ ヨ ト ・ ヨ



Raúl M. Falcón Fractal dimension of strongly isotopism classes of LS 32/32