Characterizing isomorphism classes of Latin squares by fractal dimensions of image patterns

Raúl M. Falcón

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

Portorož, Slovenia.
June 24, 2021.
CONTENTS

1 Preliminaries.

2 Standard sets of image patterns.

3 The mean fractal dimension.

4 Some computations.
CONTENTS

1 Preliminaries.

2 Standard sets of image patterns.

3 The mean fractal dimension.

4 Some computations.
A quasigroup of order $n$ is a pair $(Q, \cdot)$ formed by

- a finite set $Q$ of $n$ elements
- a product $\cdot$

such that both equations

$$a \cdot x = b \quad \text{and} \quad y \cdot a = b$$

have unique solutions $x, y \in S$, for all $a, b \in S$.

- Its multiplication table is a Latin square.

$$L = (l_{ij}) \equiv 
\begin{array}{ccc}
1 & 2 & 3 \\
2 & 3 & 1 \\
3 & 1 & 2 \\
\end{array} \in \text{LS}_3$$

**Entry set:** $\text{Ent}(L) := \{(\text{row}, \text{column}, \text{symbol})\} = \{(i, j, l_{ij})\}$.

$$\text{Ent}(L) = \{(1, 1, 1), (1, 2, 2), (1, 3, 3), (2, 1, 2), (2, 2, 3), (2, 3, 1), (3, 1, 2), (3, 2, 3), (3, 3, 1)\}.$$
Latin square isomorphism.

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

Isomorphism:

$$\begin{cases} f \in S_n \\ L \in L S_n \end{cases} \implies \text{Ent}(L^f) = \{(f(i), f(j), f(k)) \mid (i, j, k) \in \text{Ent}(L)\}.$$ 

Row-permutations ($f$), column-permutations ($f$), symbol-permutations ($f$).

\[ L \equiv \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix} \implies L^f \equiv \begin{bmatrix} 3 & 1 & 2 \\ 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \]

\[ f = (1\,2)(3) \in S_3 \]

\begin{center}
\begin{tabular}{c|c}
$n$ & |Isomorphism classes| \\
\hline
1 & 1 \\
2 & 1 \\
3 & 5 \\
4 & 35 \\
5 & 1411 \\
6 & 1130531 \\
7 & 12198455835 \\
8 & 2697818331680661 \\
9 & 15224734061438247321497 \\
10 & 2750892211809150446995735533513 \\
11 & 19464657391668924966791023043937578299025 \\
\end{tabular}
\end{center}
• A quasigroup \((Q, \cdot)\)
• A plaintext \(T = t_1 \ldots t_m\), with \(t_i \in Q\)
• A leader symbol \(s \in Q\)

**Encryption:** \(E_s(T) = e_1 \ldots e_m\)

\[
e_i := \begin{cases} 
s \cdot t_1, & \text{if } i = 1, \\
e_{i-1} \cdot t_i, & \text{otherwise.}
\end{cases}
\]

\[
\begin{align*}
Q &\equiv \begin{pmatrix} 1 & 2 & 3 \\
2 & 3 & 1 \\
3 & 1 & 2 \\
\end{pmatrix} \\
T &\equiv 122333122333 \\
E_1(T) &\equiv 123213312132 \\
E_2(T) &\equiv 231321123213 \\
E_3(T) &\equiv 312132231321
\end{align*}
\]
Image patterns arising from Latin squares.


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

**Image pattern:** \(P_{S,T} = (p_{ij})\)

\[
p_{ij} := \begin{cases} 
  t_j, & \text{if } i = 1, \\
  s_{i-1} \cdot p_{i-1,1}, & \text{if } i > 1 \text{ and } j = 1, \\
  p_{i,j-1} \cdot p_{i-1,j}, & \text{otherwise}.
\end{cases}
\]

\[
Q \equiv \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} \\
T = 122333122333 \\
S = 123123
\]

\[
\Rightarrow P_{S,T} = \begin{pmatrix} 1 & 2 & 2 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 \\ 1 & 2 & 3 & 2 & 1 & 3 & 3 & 3 & 1 & 2 & 1 & 3 & 2 \\ 1 & 3 & 1 & 3 & 2 & 3 & 3 & 2 & 1 & 2 & 2 & 1 & 2 \\ 1 & 3 & 2 & 3 & 3 & 3 & 1 & 2 & 3 & 1 & 2 & 1 & 1 \\ 1 & 3 & 3 & 2 & 3 & 2 & 1 & 3 & 3 & 3 & 2 & 3 & 3 \\ 1 & 2 & 1 & 3 & 1 & 3 & 1 & 1 & 3 & 2 & 2 & 3 & 3 \\ 1 & 1 & 3 & 3 & 2 & 2 & 1 & 2 & 3 & 3 & 2 & 1 \end{pmatrix}
\]
Image patterns arising from Latin squares.


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

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

\[
p_{ij} := \begin{cases} t_j, & \text{if } i = 1, \\ s_{i-1} \cdot p_{i-1,1}, & \text{if } i > 1 \text{ and } j = 1, \\ p_{i,j-1} \cdot p_{i-1,j}, & \text{otherwise.} \end{cases}
\]

\[
Q \equiv \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix} \\
T = 111111111111 \\
S = 222222
\]

\[
\Rightarrow \mathcal{P}_{S,T} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 3 & 1 & 2 & 3 & 1 & 2 & 3 & 1 & 2 & 3 \\ 1 & 1 & 2 & 1 & 1 & 2 & 1 & 1 & 2 & 1 \\ 3 & 1 & 2 & 3 & 1 & 2 & 3 & 1 & 2 & 3 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 3 & 1 & 3 & 2 & 1 & 1 & 1 & 2 & 3 & 1 \\ 1 & 1 & 3 & 1 & 1 & 1 & 1 & 2 & 1 & 3 \\ 1 & 1 & 3 & 1 & 1 & 1 & 1 & 2 & 1 & 3 \end{bmatrix}
\]
Image patterns arising from Latin squares.

\[
\begin{align*}
Q & \equiv \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} \\
T & = 111111111111 \\
S & = 2\ldots2
\end{align*}
\]
Image patterns arising from Latin squares.

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

Fractal quasigroups
Designing error detecting codes.

Non-fractal quasigroups
Designing cryptographic primitives.

Open problem: A comprehensive analysis of their fractal dimensions.
Image patterns arising from Latin squares.

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

1 Preliminaries.

2 Standard sets of image patterns.

3 The mean fractal dimension.

4 Some computations.
Standard sets of $r \times m$ image patterns.

- Four positive integers $m$, $n$, $r$ and $s$ such that $s \leq n$.
- A Latin square $L \in \mathcal{L}S_n$.
- A plaintext $T = s \ldots s$ of length $m$.
- An $(r - 1)$-tuple of leader symbols $S = (s, \ldots, s)$.

$s$-standard $r \times m$ image pattern: $P_{r,m;s}(L) = P_{S,T}(L)$.

Standard sets of $r \times m$ image patterns of $L$:

$$\{P_{r,m;s}(L) : s \in \{1, \ldots, n\}\}$$

$n = 4$

$r = m = 90$
Standard sets of $r \times m$ image patterns.

Proposition

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

Standard sets of $90 \times 90$ image patterns arising from the 35 isomorphism classes of Latin squares of order 4.
Standard sets of $r \times m$ image patterns.

<table>
<thead>
<tr>
<th>i</th>
<th>$#cs_i$</th>
<th>$#fs_i$</th>
<th>i</th>
<th>$#cs_i$</th>
<th>$#fs_i$</th>
<th>i</th>
<th>$#cs_i$</th>
<th>$#fs_i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>3</td>
<td>13</td>
<td>1</td>
<td>0</td>
<td>25</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>3</td>
<td>14</td>
<td>2</td>
<td>1</td>
<td>26</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>0</td>
<td>15</td>
<td>2</td>
<td>2</td>
<td>27</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>1</td>
<td>16</td>
<td>1</td>
<td>0</td>
<td>28</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>3</td>
<td>17</td>
<td>3</td>
<td>0</td>
<td>29</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>3</td>
<td>18</td>
<td>2</td>
<td>2</td>
<td>30</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>3</td>
<td>19</td>
<td>1</td>
<td>1</td>
<td>31</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>3</td>
<td>20</td>
<td>1</td>
<td>0</td>
<td>32</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>3</td>
<td>21</td>
<td>1</td>
<td>3</td>
<td>33</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
<td>0</td>
<td>22</td>
<td>2</td>
<td>2</td>
<td>34</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>11</td>
<td>2</td>
<td>0</td>
<td>23</td>
<td>1</td>
<td>3</td>
<td>35</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>

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 $r \times m$ image patterns.

<table>
<thead>
<tr>
<th>$i$</th>
<th>$#cs_i$</th>
<th>$#fs_i$</th>
<th>$i$</th>
<th>$#cs_i$</th>
<th>$#fs_i$</th>
<th>$i$</th>
<th>$#cs_i$</th>
<th>$#fs_i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>3</td>
<td>13</td>
<td>1</td>
<td>0</td>
<td>25</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>3</td>
<td>14</td>
<td>2</td>
<td>1</td>
<td>26</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>0</td>
<td>15</td>
<td>2</td>
<td>2</td>
<td>27</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>1</td>
<td>16</td>
<td>1</td>
<td>0</td>
<td>28</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>3</td>
<td>17</td>
<td>3</td>
<td>0</td>
<td>29</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>3</td>
<td>18</td>
<td>2</td>
<td>2</td>
<td>30</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>3</td>
<td>19</td>
<td>1</td>
<td>1</td>
<td>31</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>3</td>
<td>20</td>
<td>1</td>
<td>0</td>
<td>32</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>3</td>
<td>21</td>
<td>1</td>
<td>3</td>
<td>33</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
<td>0</td>
<td>22</td>
<td>2</td>
<td>2</td>
<td>34</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>11</td>
<td>2</td>
<td>0</td>
<td>23</td>
<td>1</td>
<td>3</td>
<td>35</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>12</td>
<td>2</td>
<td>1</td>
<td>24</td>
<td>4</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 $r \times m$ image patterns.

$\Rightarrow$

Standard sets of $90 \times 90$ image patterns arising from the 35 isomorphism classes of Latin squares of order 4.
Standard sets of $r \times m$ image patterns.

Standard $3 \times 3$ image patterns of five distinct isomorphism classes

Can we find an efficient method for distinguishing standard sets?
CONTENTS

1 Preliminaries.

2 Standard sets of image patterns.

3 The mean fractal dimension.

4 Some computations.
Homogenized standard sets.

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

A standard set of image patterns of a Latin square of order \( n \) is said to be **homogenized** if the colors of \( \mathcal{P}_n \) 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.

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

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

\[ \mathcal{H}_{r,m}(L) \equiv \text{Set of homogenized standard sets of } L \in \text{LS}_n. \]
Differential box-counting fractal dimension.

- $L \in \text{LS}_n$.
- $\text{Div}(r, m) \equiv$ Set of common divisors of $r$ and $m$.
- For each $k \in \text{Div}(r, m)$: $I_{i,j,k}(P_{r,m,s}(L)) \equiv$ Range of gray-level intensities within the region of $P_{r,m,s}(L)$ that is bounded by the $(i, j)$-cell of the $\frac{r}{k} \times \frac{m}{k}$ grid formed by two-dimensional boxes of side length $k$.

\[
I_k(P_{r,m,s}(L)) := \sum_{(i,j) \in \left[\frac{r}{k}\right] \times \left[\frac{m}{k}\right]} (1 + I_{i,j,k}(P_{r,m,s}(L))).
\]

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

\[
\{(\ln(I_k(P_{r,m,s}(L))), \ln(1/k)) : k \in \text{Div}(r, m)\}.
\]
Mean fractal dimension.

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

**Theorem**

- $L_1, L_2 \in \text{LS}_n$.

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

\[
\begin{array}{|c|c|c|c|}
\hline
& 1 & 2 & 3 & 4 \\
\hline
1 & 2 & 3 & 4 & 3 \\
2 & 1 & 4 & 3 & 4 \\
3 & 4 & 2 & 1 & 2 \\
4 & 3 & 1 & 2 & 1 \\
\hline
\end{array}
\]

\[
\begin{array}{|c|c|c|c|}
\hline
D_B(\mathcal{P}_{90;1}(L)) & 2.00000 & 2.00000 & 2.00000 \\
D_B(\mathcal{P}_{90;2}(L)) & 1.95165 & 1.95165 & 1.92136 \\
D_B(\mathcal{P}_{90;3}(L)) & 1.8877 & 1.88873 & 1.92331 \\
D_B(\mathcal{P}_{90;4}(L)) & 1.8877 & 1.88873 & 1.90088 \\
D_B(\mathcal{H}_{90}(L)) & 1.9317625 & 1.9322775 & 1.9363875 \\
\hline
\end{array}
\]
Mean fractal dimension.

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

Theorem

- $L_1, L_2 \in \mathbb{LS}_n$.

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

<table>
<thead>
<tr>
<th>$D_B(\mathcal{P}_{90:1}(L))$</th>
<th>2.00000</th>
<th>2.00000</th>
<th>2.00000</th>
</tr>
</thead>
<tbody>
<tr>
<td>$D_B(\mathcal{P}_{90:2}(L))$</td>
<td>1.95165</td>
<td>1.95165</td>
<td>1.92136</td>
</tr>
<tr>
<td>$D_B(\mathcal{P}_{90:3}(L))$</td>
<td>1.8877</td>
<td>1.8873</td>
<td>1.92331</td>
</tr>
<tr>
<td>$D_B(\mathcal{P}_{90:4}(L))$</td>
<td>1.8877</td>
<td>1.8873</td>
<td>1.90088</td>
</tr>
<tr>
<td>$D_B(\mathcal{H}_{90}(L))$</td>
<td>1.9317625</td>
<td>1.9322775</td>
<td>1.9363875</td>
</tr>
</tbody>
</table>
Proposition

The mean fractal dimension of the homogenized standard set of image patterns based on idempotent Latin squares is 2.
CONTENTS

1 Preliminaries.

2 Standard sets of image patterns.

3 The mean fractal dimension.

4 Some computations.
Some computations.

\[ n \in \{3, 4\} \quad (r = m = 90) \]

<table>
<thead>
<tr>
<th>n</th>
<th>i</th>
<th>( D_B(n, i) )</th>
<th>n</th>
<th>i</th>
<th>( D_B(n, i) )</th>
<th>n</th>
<th>i</th>
<th>( D_B(n, i) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1</td>
<td>1.9285267</td>
<td>4</td>
<td>35</td>
<td>1.9338325</td>
<td>4</td>
<td>23</td>
<td>1.9428575</td>
</tr>
<tr>
<td>5</td>
<td>1.9335900</td>
<td>20</td>
<td>1.921850</td>
<td>19</td>
<td>1.9357400</td>
<td>15</td>
<td>1.9472450</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1.9524867</td>
<td>27</td>
<td>1.9215825</td>
<td>21</td>
<td>1.9359200</td>
<td>12</td>
<td>1.9476600</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1.9527467</td>
<td>25</td>
<td>1.9216950</td>
<td>4</td>
<td>1.9363875</td>
<td>22</td>
<td>1.9495350</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>2.0000000</td>
<td>7</td>
<td>1.9230125</td>
<td>5</td>
<td>1.9366250</td>
<td>18</td>
<td>1.9504400</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>1.9072150</td>
<td>8</td>
<td>1.9274475</td>
<td>20</td>
<td>1.9411800</td>
<td>14</td>
<td>1.9511850</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>1.9090925</td>
<td>9</td>
<td>1.9285825</td>
<td>13</td>
<td>1.9411950</td>
<td>11</td>
<td>1.9606500</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>1.9137400</td>
<td>2</td>
<td>1.9296225</td>
<td>16</td>
<td>1.9413250</td>
<td>34</td>
<td>1.9637375</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>1.9139600</td>
<td>1</td>
<td>1.9317625</td>
<td>10</td>
<td>1.9413500</td>
<td>17</td>
<td>1.9807250</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>1.9210725</td>
<td>6</td>
<td>1.9322775</td>
<td>3</td>
<td>1.9413775</td>
<td>24</td>
<td>2.0000000</td>
<td></td>
</tr>
</tbody>
</table>

Run time of each computation: < 1s in an \textit{Intel Core i7-8750H CPU (6 cores), with a 2.2 GHz processor and 8 GB of RAM}. 

Raúl M. Falcón
Fractal dimensions and Latin square isomorphisms 29 / 33
Some computations.

\[ n = 5 \quad (r = m = 90) \]

Run time of each computation: \(< 1\text{s}\) in an *Intel Core i7-8750H CPU (6 cores)*, with a 2.2 GHz processor and 8 GB of RAM.
Some computations.

\[ n = 256 \quad (r = m = 90) \]

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.
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.


Many thanks!

Characterizing isomorphism classes of Latin squares by fractal dimensions of image patterns

Raúl M. Falcón

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

Portorož, Slovenia.
June 24, 2021.