Periodos asociados a los isotopismos de un cuadrado latino

M. J. Chávez [a], O. J. Falcón [a] y R. M. Falcón [a]

[a] *Dpto. Matemática Aplicada I. Escuela Universitaria de Arquitectura Técnica. Universidad de Sevilla.*

Resumen

En Criptografía, la eficacia de un generador de secuencias pseudo-aleatorias viene determinada por el periodo de crecimiento en la secuencia generada. En el caso concreto de generadores basados en elementos líderes y cuadrados latinos, existen diversos análisis estadísticos que confirman la importancia que adquiere una óptima elección del cuadrado latino en el que se basa el generador, si bien limitan su estudio a un único líder, que determina a su vez la secuencia de partida. En el presente trabajo, se desarrolla una alternativa al análisis del periodo de crecimiento, atendiendo a todo el conjunto de líderes y ampliando el de secuencias de partida, al mismo tiempo que se analiza la influencia que ejercen en dicho periodo las estructuras cíclicas de las simetrías de un cuadrado latino. Atendiendo a dicho análisis se obtiene explícitamente una clasificación de los cuadrados latinos de orden $n \leq 5$.

Key words: Scrambler, Cuadrado latino, Grupo de Autotopismos

1. Introducción

Se denomina *scrambler* a todo proceso que aumenta la aleatoriedad de una secuencia con probabilidad alta de contener cadenas de bits consecutivos repetidos. El máximo número de elementos consecutivos distintos que contiene una cadena C es su *periodo* $\mathcal{P}(C)$. Unas estructuras algebraicas que actúan [6][7] de forma efectiva como scramblers son los cuadrados latinos, matrices cuadradas cuyos elementos pertenecen a un conjunto de n símbolos distintos, apareciendo cada uno exactamente una vez en cada fila y en cada columna. En el presente trabajo, el conjunto de símbolos será $[n] = \{1, 2, ..., n\}$ y $\mathcal{CL}_n$ denotará el conjunto de cuadrados latinos de orden n. Dado $L = (l_{i,j}) \in \mathcal{CL}_n$, la *representación ortogonal de* L es el conjunto de n^2 triples $\{(i, j, l_{i,j}) \mid i, j \in [n]\}$.

Fijado un elemento inicial de $[n]$, denominado *líder*, se obtiene una implementación rápida de encriptación y generación de secuencias pseudo-aleatorias de igual longitud que las secuencias de entrada, que permiten aplicaciones prácticas en criptografía simétrica como puede ser la comunicación online [8]. En particular, dado $L = (l_{i,j}) \in \mathcal{CL}_n$ y fijados un líder $a \in [n]$ y una cadena de m elementos de $[n]$, $C = c_1c_2...c_m$, se genera la cadena cifrada $E_a(C) = d_1d_2...d_m$, donde $d_1 = l_{a,c_1}$ y $d_i = l_{d_{i-1},c_i}$, $\forall i \in [m] \setminus \{1\}$. En caso de ser C un *texto plano constante de base* c ($c_0 = c_1 = ... = c_{m-1} = c$), se cumple que $\mathcal{P}(E_a(C)) = \text{mín}\{i \in [m] \mid d_i = a\}$. Siendo un método robusto frente a errores, se tiene que, debido al ingente número de cuadrados latinos, este procedimiento es además resistente a ataques de fuerza bruta y estadísticos, incluso cuando se conoce tanto el texto plano como el cifrado, resultando seguir las secuencias de este último una distribución uniforme [9][10].

Atendiendo a la estructura de todo cuadrado latino, si $\mathcal{P}(C) = p$, entonces $\mathcal{P}(E_a(C)) = q \cdot p$, para algún $q \in [n]$, con lo que, en caso de querer aumentar la aleatoriedad del resultado, basta fijar una secuencia de líderes $a_1, a_2, ..., a_k$ y repetir iterativamente el procedimiento, obteniendo la encriptación, $E_{a_1}E_{a_2}...E_{a_k}$. El aumento proporcional del periodo de una encriptación a la siguiente recibe el nombre de *periodo de crecimiento* y determina la eficacia del generador. Dicho periodo ha sido analizado estadísticamente [1] [11], en aquellos casos en los que se toma un líder común a y se considera como cadena de partida un texto plano constante de base a y longitud n.

* Corresponsal

Email addresses: mjchavez@us.es (M. J. Chávez), oscfalgan@yahoo.es (O. J. Falcón), rafalgan@us.es (R. M. Falcón).

URL: http:www.personal.us.es/raufalgan (R. M. Falcón).

Para evitar que el texto cifrado vuelva a tener periodo 1, se analizan únicamente cuadrados latinos $L = (l_{i,j})$, tales que $l_{a,a} \neq a$, con lo que no se tiene en cuenta la influencia que ejerce la elección de distintos líderes o de distintas bases en la cadena de partida, al mismo tiempo que se limitan los cuadrados latinos a usar como scramblers. En el presente artículo se comprobará que estas limitaciones pueden solventarse obteniendo la media de los periodos de las cadenas resultantes al variar tanto los posibles líderes como los textos planos constantes. Se comprobará además que la estructura cíclica del conjunto de permutaciones de L, determina el conjunto de tales periodos.

El grupo de permutaciones de $[n]$ será denotado por S_n. Todo $\delta \in S_n$ puede ser unívocamente escrito como composición de $\mathbf{n}_\delta$ ciclos disjuntos, $\delta = C_1^\delta C_2^\delta ... C_{\mathbf{n}_\delta}^\delta$, donde, $\forall i \in [\mathbf{n}_\delta]$, $C_i^\delta = \left(c_{i,1}^\delta \; c_{i,2}^\delta \; ... \; c_{i,\;\lambda_i^\delta}^\delta\right)$, con $c_{i,1}^\delta = \min_j\{c_{i,j}^\delta\}$. La *estructura cíclica de* δ es la secuencia $\mathbf{l}_\delta = (\mathbf{l}_1^\delta, \mathbf{l}_2^\delta, ..., \mathbf{l}_n^\delta)$, donde $\mathbf{l}_i^\delta$ es el número de ciclos de longitud i en δ. La *representación polinómica de* $\mathbf{l}_\delta$ es el polinomio $x_1^{\mathbf{l}_1^\delta} x_2^{\mathbf{l}_2^\delta} \cdot ... \cdot x_n^{\mathbf{l}_n^\delta}$. Dados $\delta_1, \delta_2 \in S_n$, se cumple que $\mathbf{l}_{\delta_1\delta_2\delta_1^{-1}} = \mathbf{l}_{\delta_2}$. Si $\mathbf{l}_{\delta_1} = \mathbf{l}_{\delta_2}$, se define la permutación $\delta_1 * \delta_2$, tal que $\delta_1 * \delta_2(c_{i,j}^{\delta_1}) = c_{i,j}^{\delta_2}, \forall i \in [\mathbf{n}_{\delta_1}]$ y $j \in [\lambda_i^{\delta_1}]$. Se verifica entonces que $\delta_2 = (\delta_1 * \delta_2)\delta_1(\delta_1 * \delta_2)^{-1}$.

Dado $L = (l_{i,j}) \in \mathcal{CL}_n$, un *isotopismo* de L es una terna $\Theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n = S_n^3$, donde α, β y γ son permutaciones de filas, columnas y símbolos de L, respectivamente. Se denomina *estructura cíclica* de Θ a la terna $\mathbf{l}_\Theta = (\mathbf{l}_\alpha, \mathbf{l}_\beta, \mathbf{l}_\gamma)$, cuya *representación polinómica* es $x_1^{\mathbf{l}_1^\alpha} x_2^{\mathbf{l}_2^\alpha} \cdot ... \cdot x_n^{\mathbf{l}_n^\alpha} + y_1^{\mathbf{l}_1^\beta} y_2^{\mathbf{l}_2^\beta} \cdot ... \cdot y_n^{\mathbf{l}_n^\beta} + z_1^{\mathbf{l}_1^\gamma} z_2^{\mathbf{l}_2^\gamma} \cdot ... \cdot z_n^{\mathbf{l}_n^\gamma}$. Al aplicar Θ a L, resulta su cuadrado latino *isotópico*, $L^\Theta = \{(\alpha(i), \beta(j), \gamma(l_{i,j})) \mid i, j \in [n]\} \in \mathcal{CL}_n$. El conjunto de cuadrados latinos isotópicos a L constituye su *clase isotópica* $[L]$. Si $L^\Theta = L$, entonces Θ se denomina *autotopismo* de L, siendo $\mathcal{A}_n$ el conjunto de todos los posibles autotopismos de $\mathcal{CL}_n$, $\mathcal{A}_L$ el subgrupo estabilizador de L en $\mathcal{A}_n$ y $\mathcal{A}_\mathbf{l}$ el subconjunto de autotopismos de $\mathcal{A}_n$ que tienen estructura cíclica $\mathbf{l}$. Las posibles estructuras cíclicas de $\mathcal{A}_n$ han sido determinadas [2], para todo $n \leq 11$. Dado $\Theta \in \mathcal{A}_n$, $\mathcal{CL}_\Theta$ representa el conjunto de todos los cuadrados latinos L tales que $\Theta \in \mathcal{A}_L$, denotándose su cardinal como Δ_Θ, el cual ha sido determinado para $n \leq 7$ [3]. Finalmente, dados $\Theta_1 = (\alpha_1, \beta_1, \gamma_1), \Theta_2 = (\alpha_2, \beta_2, \gamma_2) \in \mathcal{A}_n$ tales que $\mathbf{l}_{\Theta_1} = \mathbf{l}_{\Theta_2}$, sea $\Theta^* = (\alpha_1 * \alpha_2, \beta_1 * \beta_2, \gamma_1 * \gamma_2)$. Resulta entonces que $\Delta_{\Theta_1} = \Delta_{\Theta_2}$ y que $\mathcal{CL}_{\Theta_2} = \mathcal{CL}_{\Theta_1}^{\Theta^*} = \{L^{\Theta^*} \mid L \in \mathcal{CL}_{\Theta_1}\}$.

2. Periodos absoluto, relativo y de crecimiento de un cuadrado latino

El periodo de una cadena cifrada depende del líder y de la cadena de partida:

Ejemplo 1 *Sea* $L = \begin{pmatrix} 1&2&3&4 \\ 2&1&4&3 \\ 3&4&2&1 \\ 4&3&1&2 \end{pmatrix} \in \mathcal{CL}_4$. *En la siguiente tabla se muestran las cadenas cifradas con sus respectivos periodos, obtenidas usando distintos líderes y textos planos constantes:*

Líder \ *Texto*	1111	2222	3333	4444
1	$\mathcal{P}(1111) = 1$	$\mathcal{P}(2121) = 2$	$\mathcal{P}(3241) = 4$	$\mathcal{P}(4231) = 4$
2	$\mathcal{P}(2222) = 1$	$\mathcal{P}(1212) = 2$	$\mathcal{P}(4132) = 4$	$\mathcal{P}(3142) = 4$
3	$\mathcal{P}(3333) = 1$	$\mathcal{P}(4343) = 2$	$\mathcal{P}(2413) = 4$	$\mathcal{P}(1423) = 4$
4	$\mathcal{P}(4444) = 1$	$\mathcal{P}(3434) = 2$	$\mathcal{P}(1324) = 4$	$\mathcal{P}(2314) = 4$

◁

En la diagonal de la tabla anterior, los periodos asociados a las cadenas cifradas de textos planos constantes de base el líder, depende de la elección de este último. De esta forma, es razonable afirmar que los análisis estadísticos a los que se ha hecho referencia en el epígrafe anterior y que se basan en la previa fijación de un líder, no reflejan fielmente la eficacia del generador de secuencias pseudo-aleatorias basado en un cuadrado latino. Con vistas a solventar esta circunstancia, presentamos la siguiente:

Definición 2 *Dado* $L \in \mathcal{CL}_n$*, definimos los* periodos absoluto y relativo *de* L*, respectivamente como:*

$$\mathcal{P}(L) = \sum_{a,b \in [n]} \mathcal{P}(E_a(C_{b,n})), \qquad \mathcal{P}_r(L) = \frac{\mathcal{P}(L)}{n^2},$$

donde $C_{b,n}$ *denota el texto plano constante de base* b *y longitud* n*.*

El periodo absoluto de L puede tomar como máximo el valor n^3, siendo su periodo relativo la media de los periodos de las cadenas cifradas por cualquier líder y de cualquier texto plano constante. Puede comprobarse que, en el Ejemplo 1, $\mathcal{P}(L) = 44$ y $\mathcal{P}_r(L) = \frac{11}{4}$.

Sea δ_c^L la permutación definida por la columna c de L, es decir, $\delta_c^L(i) = l_{i,c}, \forall\, i \in [n]$. Se tiene que:

Lema 3 *Dados* $L = (l_{i,j}) \in \mathcal{CL}_n$*,* $\Theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$ *y* $c \in [n]$*, se cumple que* $\delta_c^{L^\Theta} = \gamma \delta_{\beta^{-1}(c)}^L \alpha^{-1}$.

Demostración: Dados $L^\Theta = (l'_{i,j})$ e $i \in [n]$, resulta $\delta_c^{L^\Theta}(i) = l'_{i,c} = \gamma(l_{\alpha^{-1}(i),\beta^{-1}(c)}) = \gamma \delta_{\beta^{-1}(c)}^L \alpha^{-1}(i)$. □

Dado que $C_{b,n}$ es un texto plano constante, $\mathcal{P}(E_a(C_{b,n})) = \min\{m \in [n] \mid \left(\delta_b^L\right)^m(a) = a\}$. Se obtienen entonces los siguientes resultados:

Lema 4 *Dados $a, a', t \in [n]$ tales que $\left(\delta_b^L\right)^t(a) = a'$, se tiene que $\mathcal{P}(E_a(C_{b,n})) = \mathcal{P}(E_{a'}(C_{b,n}))$.*

Demostración: Sea $p = \mathcal{P}(E_a(C_{b,n}))$. Basta comprobar que $p = \min\{m \in [n] \mid \left(\delta_b^L\right)^m(a') = a'\}$. Ahora bien, $\left(\delta_b^L\right)^p(a') = \left(\delta_b^L\right)^p\left(\left(\delta_b^L\right)^t(a)\right) = \left(\delta_b^L\right)^t\left(\left(\delta_b^L\right)^p(a)\right) = \left(\delta_b^L\right)^t(a) = a$. Si existe $p' < p$ tal que $\left(\delta_b^L\right)^{p'}(a') = a'$, entonces, $\left(\delta_b^L\right)^{p'}(a) = a$, que no es posible, por ser p el mínimo entero con dicha propiedad. Debe ser por tanto $p = \mathcal{P}(E_a(C_{b,n}))$. □

Proposición 5 $\mathcal{P}(L) = \sum_{b,j\in[n]} j^2 \cdot \mathbf{l}_j^{\delta_b^L}$.

Demostración: Fijado $a \in [n]$, el conjunto de elementos $a' \in [n]$ que verifican las hipótesis del Lema 4 son justamente los que aparecen en el ciclo de δ_b^L que contiene a a, una vez realizada la descomposición en ciclos disjuntos de dicha permutación, coincidiendo por tanto la longitud de dicho ciclo con el periodo correspondiente a todos sus elementos. De esta forma, $\sum_{a\in[n]} \mathcal{P}(E_a(C_{b,n})) = \sum_{j\in[n]} j^2 \cdot \mathbf{l}_j^{\delta_b^L}$, obteniéndose el resultado como consecuencia inmediata. □

Teorema 6 *Sean $L = (l_{i,j}) \in \mathcal{CL}_n$ y $\alpha, \beta \in S_n$. Si $\Theta = (\alpha, \beta, \alpha)$, se verifica que $\mathcal{P}(L^\Theta) = \mathcal{P}(L)$.*

Demostración: Atendiendo a la Proposición 5 y al Lema 3, se tiene que $\mathcal{P}(L^\Theta) = \sum_{b,j\in[n]} j^2 \cdot \mathbf{l}_j^{\delta_b^{L^\Theta}} = \sum_{b,j\in[n]} j^2 \cdot \mathbf{l}_j^{\alpha\delta_{\beta^{-1}(b)}^L\alpha^{-1}} = \sum_{b,j\in[n]} j^2 \cdot \mathbf{l}_j^{\delta_{\beta^{-1}(b)}^L} = \sum_{\beta(b),j\in[n]} j^2 \cdot \mathbf{l}_j^{\delta_b^L} = \sum_{b,j\in[n]} j^2 \cdot \mathbf{l}_j^{\delta_b^L} = \mathcal{P}(L)$. □

Teorema 7 *Si $L = (l_{i,j}) \in \mathcal{CL}_n$ y $L^{(13)} = \{(l_{i,j}, j, i) \mid i, j \in [n]\}$, entonces $\mathcal{P}(L^{(13)}) = \mathcal{P}(L)$.*

Demostración: Si $b \in [n]$, entonces $\delta_b^{L^{(13)}} = \left(\delta_b^L\right)^{-1}$, con lo que, por la Proposición 5, se tiene que $\mathcal{P}(L^{(13)}) = \sum_{b,j\in[n]} j^2 \cdot \mathbf{l}_j^{\left(\delta_b^L\right)^{-1}} = \sum_{b,j\in[n]} j^2 \cdot \mathbf{l}_j^{\delta_b^L} = \mathcal{P}(L)$. □

Con vistas a determinar la eficacia como scrambler de un cuadrado latino, cabe plantearse la siguiente:

Definición 8 *Dado $L \in \mathcal{CL}_n$, definimos el m-*periodo de crecimiento de L *como:*

$$\mathcal{PC}_m(L) = \frac{\sum_{a,b\in[n]} \mathcal{P}(E_a^m(C_{b,n}))}{\sum_{a,b\in[n]} \mathcal{P}(E_a^{m-1}(C_{b,n}))}.$$

En concreto, en el Ejemplo 1, $\mathcal{PC}_2(L) = \frac{87}{44}$, $\mathcal{PC}_3(L) = \frac{109}{87}$, $\mathcal{PC}_4(L) = \frac{181}{117}$, etc.

3. Estructura periódica de un autotopismo

Estamos interesados ahora en comprobar si el grupo de autotopismos asociado a cada cuadrado latino tiene alguna influencia en el conjunto de periodos correspondientes al mismo. Para ello presentamos en primer lugar la siguiente:

Definición 9 *Dado $\Theta \in \mathcal{I}_n$, definimos los* periodos absoluto y relativo *de Θ, respectivamente como:*

$$\mathcal{P}(\Theta) = \frac{\sum_{L\in\mathcal{CL}_\Theta} \mathcal{P}(L)}{\Delta_\Theta}, \qquad \mathcal{P}_r(\Theta) = \frac{\mathcal{P}(\Theta)}{n^2}.$$

Sea $\Delta_{\Theta,m} = |\{L \in \mathcal{CL}_\Theta \mid \mathcal{P}(L) = m\}|$. Definimos la estructura periódica *de Θ como el polinomio:*

$$p_\Theta = \sum_{m\in[n^3]} \Delta_{\Theta,m} \cdot p_m.$$

Finalmente, dados $\Theta_1, \Theta_2 \in \mathcal{A}_\mathbf{l}$, definimos la relación de equivalencia en $\mathcal{A}_n$, dada por $\Theta_1 \sim \Theta_2 \Leftrightarrow \mathbf{l}_{\Theta_1} = \mathbf{l}_{\Theta_2}$ y $p_{\Theta_1} = p_{\Theta_2}$. La clase de equivalencia de $\Theta \in \mathcal{A}_n$ será denotada por $[\Theta]$.

Veamos un ejemplo:

Ejemplo 10 *Sea $\Theta = ((13)(2), (13)(2), (13)(2)) \in \mathcal{I}_3$. El conjunto $\mathcal{CL}_\Theta$ consta de los siguientes cuatro cuadrados latinos:*

$$L_1 = \begin{pmatrix} 2&3&1\\ 1&2&3\\ 3&1&2 \end{pmatrix}, \qquad L_2 = \begin{pmatrix} 1&3&2\\ 3&2&1\\ 2&1&3 \end{pmatrix},$$

$$L_3 = \begin{pmatrix} 2&1&3\\ 3&2&1\\ 1&3&2 \end{pmatrix}, \qquad L_4 = \begin{pmatrix} 3&1&2\\ 1&2&3\\ 2&3&1 \end{pmatrix}.$$

Puede comprobarse que $\mathcal{P}(L_1) = \mathcal{P}(L_2) = 15$, $\mathcal{P}(L_3) = \mathcal{P}(L_4) = 21$, $\mathcal{P}_r(L_1) = \mathcal{P}_r(L_2) = \frac{5}{3}$ y $\mathcal{P}_r(L_3) = \mathcal{P}_r(L_4) = \frac{7}{3}$. Con lo cual, $\mathcal{P}(\Theta) = \frac{72}{4} = 18$, $\mathcal{P}_r(\Theta) = 2$ y $p_\Theta = 2 \cdot (p_{15} + p_{21})$.

Con vistas a estudiar el conjunto $\mathcal{A}_n/\sim$, observamos los siguientes resultados:

Lema 11 *Dados $\Theta, \Theta' \in \mathcal{A}_n$, tales que $[\Theta] = [\Theta']$, los periodos absolutos y relativos de Θ y Θ' coinciden.*

Demostración: El resultado es inmediato, pues, como $\mathbf{l}_{\Theta_1} = \mathbf{l}_{\Theta_2}$, debe ser $\Delta_\Theta = \Delta_{\Theta'}$. □

Teorema 12 *Dados $\Theta = (\alpha, \beta, \gamma), \Theta' = (\alpha, \beta', \gamma) \in \mathcal{I}_n$ tales que $\mathbf{l}_\beta = \mathbf{l}_{\beta'}$, se verifica que $[\Theta] = [\Theta']$.*

Demostración: Es inmediato que $\mathbf{l}_\Theta = \mathbf{l}_{\Theta'}$. Sean ahora $\beta^* = \beta * \beta'$ y $\Theta^* = (Id, \beta^*, Id)$. Por el Teorema 6, se tiene en particular que $\mathcal{P}(L^{\Theta^*}) = \mathcal{P}(L)$, para todo $L \in \mathcal{CL}_\Theta$. Dado que $\mathcal{CL}_{\Theta'} = \mathcal{CL}_\Theta^{\Theta^*}$, debe ser $p_\Theta = p_{\Theta'}$. □

Teorema 13 *Dados $\alpha, \beta \in \mathcal{S}_n$ y $\Theta' = (\alpha', \beta', \gamma') \in \mathcal{I}_n$, tales que $\mathbf{l}_{\alpha'} = \mathbf{l}_\alpha$ y $\mathbf{l}_{\beta'} = \mathbf{l}_\beta$, existe $\gamma \in \mathcal{S}_n$, tal que $\mathbf{l}_\gamma = \mathbf{l}_{\gamma'}$ y $[(\alpha, \beta, \gamma)] = [\Theta']$.*

Demostración: Por el Teorema 12, $\mathcal{P}(\Theta') = \mathcal{P}((\alpha', \beta, \gamma'))$. Sean $\alpha^* = \alpha' * \alpha$ y $\gamma = \alpha^* \gamma' (\alpha^*)^{-1}$, resultando que $\mathbf{l}_\gamma = \mathbf{l}_{\gamma'}$. Sean $\Theta = (\alpha, \beta, \gamma)$ y $\Theta^* = (\alpha^*, Id, \alpha^*)$. Dado que $\mathcal{CL}_\Theta = \mathcal{CL}_{(\alpha', \beta, \gamma')}^{\Theta^*}$, basta aplicar el Teorema 6. □

Teorema 14 *Dados $\Theta = (\alpha, \beta, \gamma), \Theta' = (\gamma, \beta, \alpha) \in \mathcal{I}_n$, se verifica que $p_\Theta = p_{\Theta'}$.*

Demostración: Dado que $\mathcal{CL}_{\Theta'} = \{L \in \mathcal{CL}_n \mid L^{(13)} \in \mathcal{CL}_\Theta\}$, basta aplicar el Teorema 7. □

4. Estructuras periódicas para $n \leq 5$.

Atendiendo a la clasificación de estructuras cíclicas dada en [2] y al Teorema 13, cabe observar que, dada una estructura cíclica $\mathbf{l} = (\mathbf{l}_1, \mathbf{l}_2, \mathbf{l}_3)$ de $\mathcal{A}_n$, basta fijar $\alpha, \beta \in S_n$ tales que $\mathbf{l}_\alpha = \mathbf{l}_1$ y $\mathbf{l}_\beta = \mathbf{l}_2$, para que, recorriendo todas las permutaciones $\gamma \in S_n$ tales que $\mathbf{l}_\gamma = \mathbf{l}_3$, se obtengan todas las posibles estructuras periódicas correspondientes a los autotopismos de $\mathcal{A}_\mathbf{l}$. Además, por el Teorema 14, basta analizar sólo aquellas estructuras cíclicas tales que el número de ciclos de $\mathbf{l}_1$ es menor o igual que el de $\mathbf{l}_3$.

Para $n \leq 5$, fijada una estructura $\mathbf{l}$ y un autotopismo $\Theta \in \mathcal{A}_\mathbf{l}$, se ha obtenido $\mathcal{CL}_\Theta$, haciendo uso de la librería [4], desarrollada [3] para su uso en SINGULAR. Posteriormente, se han calculado los periodos absolutos de dichos cuadrados latinos, permitiendo obtener las estructuras periódicas de cada autotopismo y, como consecuencia, la correspondiente clasificación de las distintas clases de equivalencia de $\mathcal{A}_n/\sim$. Presentamos a continuación los resultados obtenidos, indicando, para cada clase de equivalencia su estructura cíclica, su cardinal, su periodo absoluto y su estructura periódica:

$\mathbf{l}$	$\lvert[\Theta]\rvert$	$\mathcal{P}(\Theta)$	p_Θ
$x_2 + y_2 + z_1^2$	1	6	$2p_6$
$x_2 + y_1^2 + z_2$	1	6	$2p_6$

Cuadro 1
Estructuras periódicas de $\mathcal{A}_2$.

$\mathbf{l}$	$\lvert[\Theta]\rvert$	$\mathcal{P}(\Theta)$	p_Θ
$x_3 + y_3 + z_3$	4	15	$3p_{15}$
	4	21	$3p_{21}$
$x_3 + y_3 + z_1^3$	4	18	$3p_{15} + 3p_{21}$
$x_3 + y_1^3 + z_3$	2	15	$6p_{15}$
	2	21	$6p_{21}$
$x_1x_2^2 + y_1y_2^2 + z_1z_2^2$	27	18	$2p_{15} + 2p_{21}$

Cuadro 2
Estructuras periódicas de $\mathcal{A}_3$.

$\mathbf{l}$	$\lvert[\Theta]\rvert$	$\mathcal{P}(\Theta)$	p_Θ
$x_4 + y_4 + z_2^2$	36	36	$4p_{28} + 4p_{44}$
	72	42	$8p_{42}$
$x_4 + y_2^2 + z_4$	18	28	$8p_{28}$
	72	42	$8p_{42}$
	18	44	$8p_{44}$
$x_4 + y_4 + z_1^2z_2$	72	36	$4p_{28} + 4p_{44}$
	144	42	$4p_{40} + 4p_{44}$
$x_4 + y_1^2y_2 + z_4$	72	36	$4p_{28} + 4p_{44}$
	144	42	$4p_{40} + 4p_{44}$
$x_4 + y_4 + z_1^4$	36	40	$4p_{28} + 16p_{42} + 4p_{44}$
$x_4 + y_1^4 + z_4$	6	28	$24p_{28}$
	24	42	$24p_{42}$
	6	44	$24p_{44}$
$x_2^2 + y_2^2 + z_2^2$	18	39	$8p_{28} + 8p_{40} + 16p_{44}$
	9	42	$16p_{40} + 16p_{44}$
$x_2^2 + y_2^2 + z_1^2z_2$	36	39	$8p_{28} + 16p_{42} + 8p_{44}$
	18	42	$32p_{42}$
$x_2^2 + y_1^2y_2 + z_2^2$	18	39	$8p_{28} + 16p_{42} + 8p_{44}$
	36	40.5	$8p_{28} + 24p_{42}$
$x_2^2 + y_2^2 + z_1^4$	9	40	$16p_{28} + 16p_{40} + 32p_{42} + 32p_{44}$
$x_2^2 + y_1^4 + z_2^2$	3	36	$48p_{28} + 48p_{44}$
	6	42	$24p_{40} + 48p_{42} + 24p_{44}$
$x_1x_3 + y_1y_3 + z_1z_3$	256	36	$3p_{28} + 6p_{40}$
	256	44	$9p_{44}$
$x_1^2x_2 + y_1^2y_2 + z_1^2z_2$	72	36	$8p_{28} + 8p_{44}$
	144	42	$4p_{40} + 8p_{42} + 4p_{44}$

Cuadro 3
Estructuras periódicas de $\mathcal{A}_4$.

1	$\|[\Theta]\|$	$\mathcal{P}(\Theta)$	p_Θ
$x_5+y_5+z_5$	576	$\frac{215}{3}$	$5p_{45}+10p_{85}$
	5760		$10p_{67}+5p_{81}$
	5760	$\frac{229}{3}$	$5p_{67}+10p_{81}$
	1152	$\frac{235}{3}$	$5p_{45}+5p_{85}+5p_{105}$
	576	$\frac{275}{3}$	$10p_{85}+5p_{105}$
$x_5+y_5+z_1^5$	576	75	$5p_{45}+50p_{67}+50p_{81}+10p_{85}+5p_{105}$
$x_5+y_1^5+z_5$	24	45	$120p_{45}$
	240	67	$120p_{67}$
	240	81	$120p_{81}$
	48	85	$120p_{85}$
	24	105	$120p_{105}$
$x_1x_4+y_1y_4+$ $+z_1z_4$	7200	74	$16p_{67}+16p_{81}$
	18900	77	$4p_{45}+8p_{67}+8p_{81}+8p_{85}+4p_{105}$
	900	80	$8p_{45}+16p_{85}+8p_{105}$
$x_1x_2^2+y_1y_2^2+$ $+z_1z_2^2$	450	74	$32p_{57}+64p_{67}+64p_{75}+64p_{81}+32p_{89}$
	900		$16p_{59}+64p_{67}+48p_{69}+16p_{75}+$ $+32p_{79}+64p_{81}+16p_{93}$
	1800	75.5	$8p_{45}+8p_{51}+16p_{59}+48p_{67}+$ $+24p_{71}+16p_{75}+32p_{79}+48p_{81}+$ $+16p_{85}+24p_{89}+8p_{93}+8p_{105}$
	225	77	$16p_{45}+16p_{57}+32p_{67}+32p_{75}+48p_{77}+$ $32p_{81}+32p_{85}+32p_{89}+16p_{105}$
$x_1^2x_3+y_1^2y_3+$ $+z_1^2z_3$	400	67	$72p_{59}+72p_{75}$
	400	71	$24p_{51}+48p_{57}+24p_{75}+48p_{93}$
	2400	73	$12p_{51}+24p_{59}+24p_{69}+12p_{71}+$ $+48p_{79}+12p_{89}+12p_{93}$
	2400		$12p_{57}+12p_{59}+24p_{69}+24p_{71}+$ $+36p_{75}+12p_{77}+24p_{89}$
	2400	81	$12p_{71}+36p_{75}+48p_{79}+36p_{89}+12p_{93}$

Cuadro 4
Estructuras periódicas de $\mathcal{A}_5/\sim$.

5. Periodos de cuadrados latinos de orden $n \leq 5$.

Para finalizar nuestro estudio, a partir de los resultados obtenidos en el epígrafe anterior y de la estructura de diseño de bloque formada por una clase isotópica $[L]$ junto a sus autotopismos [5], hemos obtenido, para cada posible periodo absoluto p, el número $\Delta^p_{[L]}$ de cuadrados latinos de $[L]$ con dicho periodo:

n	$\|\mathcal{CL}_n\|$	$\Delta^6_{[L]}$	$\Delta^{15}_{[L]}$	$\Delta^{21}_{[L]}$
2	2	2	0	0
3	12	0	6	6

Cuadro 5
Periodos absolutos de $\mathcal{CL}_2$ y $\mathcal{CL}_3$. Ambos constan de una única clase isotópica.

$[L]$	$\|[L]\|$	$\Delta^{28}_{[L]}$	$\Delta^{40}_{[L]}$	$\Delta^{42}_{[L]}$	$\Delta^{44}_{[L]}$
$c_{4,1}$	432	72	0	288	72
$c_{4,2}$	144	24	48	0	72
Total	576	96	48	288	144

Cuadro 6
Periodos absolutos de $\mathcal{CL}_4$, donde:

$$c_{4,1}=\left[\begin{pmatrix}1&2&3&4\\2&1&4&3\\3&4&2&1\\4&3&1&2\end{pmatrix}\right],\ c_{4,2}=\left[\begin{pmatrix}1&2&3&4\\2&1&4&3\\3&4&1&2\\4&3&2&1\end{pmatrix}\right].$$

$[L]$	$\|[L]\|$	$\Delta^{45}_{[L]}$	$\Delta^{67}_{[L]}$	$\Delta^{81}_{[L]}$	$\Delta^{85}_{[L]}$	$\Delta^{105}_{[L]}$
$c_{5,1}$	17280	720	7200	7200	1440	720

$[L]$	$\|[L]\|$	$\Delta^{51}_{[L]}$	$\Delta^{57}_{[L]}$	$\Delta^{59}_{[L]}$	$\Delta^{69}_{[L]}$	$\Delta^{71}_{[L]}$	$\Delta^{75}_{[L]}$	$\Delta^{77}_{[L]}$	$\Delta^{79}_{[L]}$	$\Delta^{89}_{[L]}$	$\Delta^{93}_{[L]}$
$c_{5,2}$	144000	4800	6000	14400	14400	14400	26400	3600	28800	21600	9600

Cuadro 7
Periodos absolutos de $\mathcal{CL}_5$, donde:

$$c_{5,1}=\left[\begin{pmatrix}1&2&3&4&5\\2&3&4&5&1\\3&4&5&1&2\\4&5&1&2&3\\5&1&2&3&4\end{pmatrix}\right],\ c_{5,2}=\left[\begin{pmatrix}1&2&3&4&5\\2&1&4&5&3\\3&4&5&1&2\\4&5&2&3&1\\5&3&1&2&4\end{pmatrix}\right].$$

Referencias

[1] V. Dimitrova, J. Markovski. "On Quasigroup Pseudo Random Sequence Generator". *Proc. of the 1-st Balkan Conference in Informatics, Y Manolopoulos and P. Spirakis eds., 21-23 Nov. 2004, Thessaloniki, 393-401.*

[2] R. M. Falcón, "Cycle structures of autotopisms of the Latin squares of order up to 11". *Ars Combinatoria* (en imprenta). Disponible en `http://arxiv.org/abs/0709.2973`.

[3] R. M. Falcón, J. Martín-Morales. "Gröbner bases and the number of Latin squares related to autotopisms of order ≤ 7". *Journal of Symbolic Computation 42 (2007), 1142-1154.*

[4] R. M. Falcón, J. Martín-Morales. `http://www.personal.us.es/raufalgan/LS/latinSquare.lib`.

[5] R. M. Falcón. "Designs based on the cycle structure of a Latin square autotopism". *Proc. of the 1-st Hispano-Moroccan Days on Applied Mathematics and Statistics. Tetouan, 2008.*

[6] C. Koscielny. "A method of constructing quasigroup-based stream-ciphers". *Appl. Math. And Comp. Sci., vol. 6, No. 1, 109-121 (1996).*

[7] C. Koscielny et al. "A quasigroup-based public-key cryptosystem". *Int. J. Appl. Math And Comp. Scit, vol. 9, No. 4, 955-963 (1999).*

[8] S. Markovski, D. Gligoroski, S. Andova. "Using quasigroups for one-one secure encoding". *Proc. of Eight Conference Logic and Computer Science (LIRA), Novi Sad, 157-162 (1997).*

[9] S. Markovski, D. Gligoroski, V. Bakeva. "Quasigroup string processing: Part 1". *Proc. of Maced. Acad. of Sci. and Arts for Math. and Tech. Sci., XX 1-2, 13-28 (1999).*

[10] S. Markovski, V. Kusakatov. "Quasigroup string processing: Part 2". *Proc. of Maced. Acad. of Sci. and Arts for Math. and Tech. Sci., XXI, 1-2, pp. 15-32 (2000).*

[11] S. Markovski, D. Gligoroski, J. Markovski, "Classification of Quasigroups by Random Walk on Torus". *J.Appl. Math. & Computing Vol. 19(2005), No. 1 2, pp. 57 75.*