Decomposition of principal autotopisms into triples of a Latin square

Falcón Ganfornina, R.M.

(rafalgan@us.es)
Departamento de Geometría y Topología
Facultad de Matemáticas (Universidad de Sevilla)
Avda. Reina Mercedes s/n
41080 - Sevilla

Abstract

Triples of a Latin square L and isotopisms of its autotopism group $\mathcal{U}(L)$ can be used to get a secret sharing scheme in Cryptography. Although the weight of information given by the latter is usually greater than that given by the former, the size of an isotopism is generally much larger than that of a triple. As this problem rises with n, it is necessary to identify an isotopism with a set of shares of a smaller size. In this paper we give an algorithm to decompose any non-trivial principal autotopism into triples of a Latin square.

Introduction

A *Latin square* L of order n is a $n \times n$ array with elements chosen from a set $N = \{x_1, ..., x_n\}$, such that each symbol occurs precisely once in each row and each column. In other words, a Latin square is the multiplication table of a quasigroup in abstract algebra. The set of Latin squares of order n is denoted by $LS(n)$.

In this paper we will consider $N = \{0, 1, ..., n-1\}$. So, if $L = (l_{ij})$, the *orthogonal array representation of* L is the set of n^2 triples $\{(i, j, l_{ij}) : i, j \in N\}$. An *isotopism* of a Latin square L is a triple $\Theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n = S_n \times S_n \times S_n$, where S_n is the symmetric group on N and α, β and γ are respectively, permutations of rows, columns and symbols of L. The resulting square L^Θ is also a Latin square and it is said to be *isotopic* to L. If $\gamma = \epsilon$, the identity map on N, Θ is called a *principal isotopism*. An isotopism which maps L to itself is an *autotopism*. $(\epsilon, \epsilon, \epsilon)$ is called the *trivial autotopism*. The stabilizer subgroup of L in $\mathcal{I}_n$ is its *autotopism group*, $\mathcal{U}(L) = \{\Theta \in \mathcal{I}_n : L^\Theta = L\}$. Fixed $\Theta \in \mathcal{I}_n$, the set of all Latin squares L such that $\Theta \in \mathcal{U}(L)$ is denoted by $LS(\Theta)$.

A *partial Latin square* P of order n is a $n \times n$ array with elements chosen from a set of n symbols, such that each symbol occurs at most once in each row and in each column. It is therefore the multiplication table of a partial quasigroup in abstract algebra. The *size* of P is the number of its *filled cells*, that is, the number of triples $(i, j, k) \in P$ such that

Actas del X Encuentro de Álgebra Computacional y Aplicaciones. Sevilla, 2006, pp. 95 - 98. ISBN: 84-611-2311-5.

$k \neq \emptyset$. The set of partial Latin squares of order n is denoted by $PLS(n)$. *Isotopisms* of partial Latin squares are defined in a similar way than that of Latin squares, although now $\gamma(\emptyset) = \emptyset$. In particular, the sets $\mathcal{U}(P)$ and $PLS(\Theta)$ are similarly defined. It is said that a fixed $P \in PLS(n)$ can be *uniquely completed* to a Latin square $L \in LS(n)$ if L is the unique Latin square such that $P \subseteq L$ and it is denoted $P \in UC(L)$. Besides, if any proper subset of P can be completed to two distinct Latin squares, it is said that P is a *critical set* of L and it is denoted $P \in CS(L)$. Fixed $L \in LS(n)$, $scs(L)$ denotes the size of the smallest critical set of L and $scs(n)$ denotes the minimum of $scs(L)$ for all $L \in LS(n)$.

A *secret sharing scheme* is a method of sharing a secret key K, by giving n pieces of information called *shares* to n participants, in such a way that K can be reconstructed from certain authorized groups of shares and it cannot be done from unauthorized groups of them. The *access structure* Γ is the set of all the previous authorized groups. An example of this by using Latin squares is the following [1, 4]: Fixed a Latin square $L = (l_{ij}) \in LS(n)$ as the secret key and made public its order n, each share is then a triple $(i, j, l_{ij}) \in L$ and the set of all the used triples is denoted by S. So, if some participants get a critical set of L by sharing its corresponding triples, they will obtain as consequence the secret key L. The access structure is then $\Gamma = \{P \in PLS(n) : P \subseteq \bigcup_S \{(i, j, l_{ij})\} \subseteq L$ and $\exists C \in CS(L)$ such that $C \subseteq P\}$.

Given $P \in PLS(n)$, contained in L, and $\mathfrak{F} \subseteq \mathcal{U}(L)$, it is defined the *extended autotopy* $P^{\mathfrak{F}} = \bigcup_{\Theta \in \mathfrak{F}} P^{\Theta} \in PLS(n)$. Fixed $L \in LS(n)$, $P \in PLS(n)$ contained in L and $\mathfrak{F} \subseteq \mathcal{U}(L)$, it is defined $\mathfrak{F}(P) = P^{<\mathfrak{F}>}$, where $< \mathfrak{F} >$ is the subgroup of $\mathcal{U}(L)$ generated by $\mathfrak{F}$. Then, P is *uniquely* $\mathfrak{F}$*-completable to* L, which is denoted as $P \in UC_{\mathfrak{F}}(L)$, if $\mathfrak{F}(P) \in UC(L)$. Furthermore, P is a $\mathfrak{F}$*-critical set* if $P \in UC_{\mathfrak{F}}(L)$ and $Q \notin UC_{\mathfrak{F}}(L)$ for all $Q \subset P$. The study of the size $scs_{\mathfrak{F}}(L)$ of the smallest $\mathfrak{F}$-critical set of L is then an open problem [2]. Besides, analogously to critical sets, it is expected that $\mathfrak{F}$-critical sets will have applications in Cryptography. In this way, in [3], fixed a Latin square $L \in LS(n)$ as the secret key and made public its order n, it is allowed to consider triples of L and a set $\digamma$ of principal autotopisms of L as shares of a secret sharing scheme. So, if some participants get a $\mathfrak{F}$-critical set of L, being $\mathfrak{F} \subseteq \digamma$, by sharing its corresponding triples and principal autotopisms, they will obtain L. Besides, the participants can get information about the symmetry of L by obtaining the set $LS(\Theta)$, which is easily computable by following the canonical construction path method (CCPM) [5]. Finally, although the weight of information given by Θ is usually greater than that given by the triples of L, the size of an isotopism is, however, much larger than that of a triple. As this problem rises with n, it is necessary to identify any autotopism with a set of shares of a smaller size. In this way, we give in this paper an algorithm to decompose any non-trivial principal autotopism into triples of a Latin square. It will allow us in the near future to tackle the calculus of the number $scs_{\{\Theta\}}(L)$ and so, that of $scs_{\mathfrak{F}}(L)$.

1 The canonical construction path method.

From now on, $\Theta = (\alpha, \beta, \epsilon) \in \mathcal{I}_n$ will be a non-trivial principal isotopism, such that $|LS(\Theta)| > 0$. From [3], this is equivalent to say that α and β have all their cycles of the same length and without fixed points, that is, $\alpha = C_0^{\alpha} \circ C_1^{\alpha} \circ ... \circ C_{k-1}^{\alpha}$ and

$\beta = C_0^{\beta} \circ C_1^{\beta} \circ ... \circ C_{k-1}^{\beta}$, where $C_i^{\delta} = \left(c_{i,0}^{\delta}\ c_{i,1}^{\delta}\ ...\ c_{i,\frac{n}{k}-1}^{\delta}\right)$ is a cycle of length $\frac{n}{k} \neq 1$ for all $\delta \in \{\alpha, \beta\}$ and $i \in \{0, 1, ..., k-1\}$, being $c_{i,j}^{\delta} \in N$, for all $j \in \{0, 1, ..., \frac{n}{k} - 1\}$. Moreover, it must be $c_{i,j}^{\delta} \neq c_{k,l}^{\delta}$, for all $(i,j) \neq (k,l)$. Besides, we will impose that $c_{0,0}^{\alpha} = c_{0,0}^{\beta} = 0$. Finally, fixed $i \in \{0, 1, ..., k-1\}$ and $\delta \in \{\alpha, \beta\}$, we will define the set $S_i^{\delta} = \{c_{i,j}^{\delta} : j \in \{0, 1, ..., \frac{n}{k} - 1\}\}$.

If we want to find a Latin square $L = (l_{ij}) \in LS(\Theta)$, then we can use the CCPM. This algorithm allows to decompose L in the subsquares $R_L^{i,j} = \{(c_{i,s}^{\alpha}, c_{j,t}^{\beta}, l_{c_{i,s}^{\alpha}\ c_{j,t}^{\beta}}) : s, t \in \{0, 1, ..., \frac{n}{k} - 1\}\}$, for all $i, j \in \{0, 1, ..., k-1\}$. These subsquares can be considered either as partial Latin squares contained in L or as Latin squares of order $\frac{n}{k}$. In this way, to find L, it is enough to determine $\frac{n}{k}$ triples of each subsquare $R_L^{i,j}$, because of the following:

Lemma 1.1. *Let $\left(c_{i,s}^{\alpha}, c_{j,t}^{\beta}, l_{c_{i,s}^{\alpha}\ c_{j,t}^{\beta}}\right)$ be a triple of $R_L^{i,j}$. Then, the $\frac{n}{k}$ cells (u, v, l_{uv}) of $R_L^{i,j}$ such that $l_{uv} = l_{c_{i,s}^{\alpha}\ c_{j,t}^{\beta}}$ are known.*

Now, fixed $\delta \in S_n$, we will define the sets $PLS_1(\delta) = \{P \in PLS(n) : \exists \gamma \in S_n$ such that $P \in PLS((\delta, \gamma, \epsilon))\}$ and $PLS_2(\delta) = \{P \in PLS(n) : \exists \gamma \in S_n$ such that $P \in PLS((\gamma, \delta, \epsilon))\}$. Let us observe that, given $L \in LS(n)$, we can extend the previous definitions to any Latin subsquare S of L by identifying it with the partial Latin square of order n such that its unique filled cells are those corresponding to S. In this way, keeping in mind the CCPM, the following result is immediate:

Lemma 1.2. *$R_L^{i,j} \in PLS_1(C_i^{\alpha}) \cap PLS_2(C_j^{\beta})$, for all $i, j \in \{0, 1, ..., k-1\}$.*

2 Partial Latin squares related to principal isotopisms

We will consider a particular case of Latin square included in $LS(\Theta)$. Specifically, we are interested in a Latin square $L_{\Theta} = (l_{ij}) \in LS(n)$ such that $l_{0j} = j$ for all $j \in N$. Besides, fixed $i \notin S_0^{\alpha} \cup S_0^{\beta}$, we impose $l_{i0} = i$. Then, we put in the natural order the elements of $S_0^{\alpha} \setminus S_0^{\beta}$ and we assign them consecutively to the elements l_{i0} (also in the natural order) which are still without an assigned value. In this way, keeping in mind Lemma 1.1 and the previous conditions, we can define the partial Latin square $P_{\Theta} = \bigcup_i R_{L_{\Theta}}^{i,0} \cup \bigcup_j R_{L_{\Theta}}^{0,j} \in PLS(n)$. Then, we can consider the equivalence relation in the set of principal isotopisms given by: $\Theta_1 \sim \Theta_2 \Leftrightarrow P_{\Theta_1} = P_{\Theta_2}$. The equivalence class of each principal isotopism Θ will be denoted by $[\Theta]$.

Lemma 2.1. *If $\Theta_1 \sim \Theta_2$ then $LS(\Theta_1) = LS(\Theta_2)$.*

The main result to prove in this paper is then the following:

Theorem 2.2. *There exists a bijection between the set of equivalence classes of non-trivial principal isotopisms Θ such that $|LS(\Theta)| > 0$ and the set of partial Latin squares $P = (p_{ij})$ of order n and size $(2k-1) \cdot \left(\frac{n}{k}\right)^2$, such that:*

i) In P, all the cells of its first row and column are filled. Besides, $p_{0j} = j\ \forall j \in N$.

ii) Indeed, there exist $\frac{n}{k}$ rows and $\frac{n}{k}$ columns in P such that all its cells are filled.

iii) There is an unique way of decomposing P in $2k-1$ disjoint blocks B_0, $B_1^r, ..., B_{k-1}^r$, $B_1^c, ..., B_{k-1}^c$, where the blocks corresponding to the filled rows (columns) of P are denoted with the r (c) index. B_0 denotes the intersection of filled rows and columns.

iv) There exist two $\frac{n}{k}$-cycles C_1 and C_2, such that $B_0 \in PLS((C_1, C_2, \epsilon))$. Besides, for all $i \in \{1, 2, ..., k-1\}$, $B_i^r \in PLS_1(C_1)$ and $B_i^c \in PLS_2(C_2)$.

Proof. It is enough to consider the map $\Theta \to P_\Theta$. Specifically, keeping in mind the CCPM, it is immediate that P_Θ is a partial Latin square which verifies all the properties of the theorem. Now, fixed a partial Latin square P verifying these properties, we can find a principal isotopism $\Theta = (\alpha, \beta, \epsilon)$ such that $P_\Theta = P$. To obtain it, let $(N, \cdot)$ be the partial quasigroup having P as its multiplication table. Now, we follow the next:

Algorithm 2.3.

i) We take $C_0^\alpha = C_1$ and $C_0^\beta = C_2$, in such a way that $c_{0,0}^\alpha = c_{0,0}^\beta = 0$.

ii) For i from 1 to $k-1$, let $c_{i,0}^\alpha$ be the minimum in the natural order of $N \setminus \bigcup_{j=0}^{i-1} S_j^\alpha$. So, $C_i^\alpha = (c_{i,0}^\alpha \;\; p_{c_{i,0}^\alpha 0}/c_{0,1}^\beta \;\; p_{c_{i,0}^\alpha 0}/c_{0,2}^\beta \; ... \; p_{c_{i,0}^\alpha 0}/c_{0,\frac{n}{k}-1}^\beta)$, where / denotes the right division on $(N, \cdot)$.

iii) For j from 1 to $k-1$, let $c_{j,0}^\beta$ be the minimum in the natural order of $N \setminus \bigcup_{i=0}^{j-1} S_i^\beta$. So, $C_j^\beta = (c_{j,0}^\beta \;\; c_{0,1}^\alpha \backslash c_{j,0}^\beta \;\; c_{0,2}^\alpha \backslash c_{j,0}^\beta \; ... \; c_{0,\frac{n}{k}-1}^\alpha \backslash c_{j,0}^\beta)$, where \ denotes the left division on $(N, \cdot)$. □

3 Final remarks

Keeping in mind Theorem 2.2, we have found a way to identify any non-trivial principal isotopism Θ such that $|LS(\Theta)| > 0$ with a set of triples: those corresponding to the filled cells of P_Θ. However, we can study the possibility of identifying Θ with a smaller set of triples. In this way, Algorithm 2.3 give us un upper bound of the size of the smallest set of triples equivalent to Θ. Indeed, if we denotes this last size as $scs(\Theta)$, we have the following:

Corollary 3.1. $scs(\Theta) \leq 2n - \frac{n}{k} - k$.

The study of the previous bound is related to that of the access structure of any secret sharing scheme using Latin squares and principal isotopisms.

References

[1] COOPER, J. A., DONOVAN, D., SEBERRY, J. *S*ecret Sharing Schemes arising from Latin squares. Bull. Inst. Combin. Appl. 12 (1994) 33 - 43.

[2] FALCÓN GANFORNINA, R. M. *S*tudy of Critical Sets in Latin Squares by using the Autotopism Group. Submitted (2005).

[3] FALCÓN GANFORNINA, R. M. *L*atin squares associated to principal autotopisms of long cycles. Application in Cryptography. Transgressive Computing 2006, Granada (Spain).

[4] LAYWINE, C. F., MULLEN, G. L. *D*iscrete mathematics using Latin Squares. Wiley-Interscience. Series in discrete mathematics and optimization, 1998. ISBN 0-471-24064-8.

[5] MCKAY, B. D. *I*somorph-free exhaustive generation. J. Algorithms 26 (1998) 306 - 324.