Structural patterns of autotopisms of maximum rank quasigroups.

R. M. Falcón
rafalgan@us.es
Department of Applied Mathematics I.
University of Seville (Spain).

ABSTRACT: In this paper, some properties of the set $\mathcal{Q}_n$ of those quasigroups of n elements having maximum rank n are studied. Although one such a quasigroup Q must be a loop, the reciprocal is false in general. So, the existence of an unit element of Q can be used in order to study the symmetrical structure of its multiplication table, given by the autotopism group of Q. Moreover, by imposing the condition of having maximum rank, a classification of all possible structural patterns of $\mathcal{Q}_n$ can be obtained. Finally, it is given an outline about the application of all the previous results in the calculus of the character tables of the quasigroups of $\mathcal{Q}_n$ and their corresponding determinant groups.

1 Basic definitions.

• A ***quasigroup*** is a nonempty set Q endowed with a product $\cdot$, such that if any two of the three symbols a, b, c in the equation $a \cdot b = c$ are given as elements of Q, the third is uniquely determined as an element of Q. It is equivalent to say that Q is endowed with a left $\backslash$ and a right $/$ division. If there exists $e \in Q$ such that $a \cdot e = e \cdot a = a$, for all $a \in Q$, then $(Q, \cdot)$ is a ***loop*** with ***unit element*** e.

• Johnson and Smith [4] extended the traditional character theory for finite groups to finite quasigroups. To do it, given a quasigroup $(Q, \cdot)$, they defined the ***conjugacy class*** of a pair $(i,j) \in Q^2$ as the orbit $\mathfrak{o}(i,j) = \{((x\cdot i)\cdot y, (x \cdot j) \cdot y) \mid x, y \in Q\} \cup \{(x \cdot (i \cdot y), x \cdot (j \cdot y)) \mid x, y \in Q\}$ of the diagonal action of the multiplication group G on Q^2. The number of conjugacy classes of a quasigroup is its ***rank*** and it is verified that almost all finite quasigroups have rank 2 [6]. $\mathcal{Q}_n$ denotes the set of those quasigroups of n elements having maximum rank n. The conjugacy classes of a quasigroup constitute an association scheme of Q^2, such that the linear span of the set $\{A_1 = Id_n, A_2, ..., A_m\}$ of their incidence matrices in the algebra of $n \times n$ complex matrices is a commutative Bose-Mesner algebra, called the ***centralizer ring*** $V(G,Q)$ of G in its multiplicity-free action on Q.

Let $\{E_1 = J_n/n, E_2, ..., E_m\}$ a basis of idempotent matrices of $V(G,Q)$ obtained by diagonalizing this algebra, where J_n is the $n \times n$ all-ones matrix. If $|C_i| = nn_i$, $tr(E_i) = f_i$ and $A_i = \sum_{j=1}^{m} \xi_{i,j} E_j$, for all $i \in [m]$, then the ***character table*** of $(Q,\cdot)$ is the $m \times m$ matrix $\Psi = (\psi_{i,j})$, such that $\psi_{i,j} = \frac{\sqrt{f_i}}{n_j}\xi_{ji}$.

• The multiplication or Caley's table of any quasigroup with n elements is a ***Latin square*** of order n, that is to say, an $n \times n$ array with elements chosen from a set of n distinct symbols such that each symbol occurs precisely once in each row and once in each column. From now on, let us assume $[n] = \{1, 2, ..., n\}$ as this set of symbols and let us denote the set of Latin squares of order n by $\mathcal{LS}_n$. Given $L = (l_{i,j}) \in \mathcal{LS}_n$, the ***orthogonal array representation of*** L is the set of n^2 triples $\{(i, j, l_{i,j}) : i, j \in [n]\}$. Thus, if L is the Caley's table of a quasigroup $([n], \cdot)$, then $a \cdot b = c \in [n]$ if and only if $(a, b, c) \in L$. The set of Latin squares of order n associated to loops is denoted by $\mathcal{L}_n$.

• The symmetric group on $[n]$ is denoted by S_n. Every permutation $\delta \in S_n$ can be uniquely written as a composition of pairwise disjoint cycles, $\delta = C_1^\delta \circ C_2^\delta \circ ... \circ C_{n_\delta}^\delta$, such that for all $i \in [n_\delta]$, one has $C_i^\delta = \left(c_{i,1}^\delta \; c_{i,2}^\delta \; ... \; c_{i,\lambda_i^\delta}^\delta\right)$. Given $\delta \in S_n$, the ***cycle structure of*** δ is the sequence $\mathbf{l}_\delta = (\mathbf{l}_1^\delta, \mathbf{l}_2^\delta, ..., \mathbf{l}_n^\delta)$, where $\mathbf{l}_i^\delta$ is the number of cycles of length i in δ, for all $i \in [n]$.

• An ***isotopism*** of a Latin square $L \in \mathcal{LS}_n$ is a triple $\Theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n = \mathcal{S}_n^3$, in such a way that $L^\Theta = \{(\alpha(i), \beta(j), \gamma(l_{i,j})) \mid i, j \in [n]\}$ is also a Latin square. The ***cycle structure*** of Θ is the triple $\mathbf{l}_\Theta = (\mathbf{l}_\alpha, \mathbf{l}_\beta, \mathbf{l}_\gamma)$. It is said that two Latin squares $L_1, L_2 \in \mathcal{LS}_n$ are ***isotopic*** if there exists $\Theta \in \mathcal{I}_n$ such that $L_1^\Theta = L_2$. To be isotopic is an equivalence relation and the set of Latin squares being isotopic to a given $L \in \mathcal{LS}_n$ is its ***isotopism class***, which will be denoted by $[L]$. The number of isotopism classes of the set $\mathcal{LS}_n$ is known for all $n \leq 10$ [5].

• Given $\Theta \in \mathcal{I}_n$, if $L^\Theta = L$, then Θ is called an ***autotopism*** of L. $\mathfrak{A}_n$ is the set of all possible autotopisms of Latin squares of order n and the set of cycle structures of $\mathfrak{A}_n$ is denoted by $\mathcal{CS}_n$, which was determined in [2] for $n \leq 11$. The stabilizer subgroup of L in $\mathfrak{A}_n$ is its ***autotopism group*** $\mathfrak{A}_L = \{\Theta \in \mathcal{I}_n \mid L^\Theta = L\}$. Given $L \in \mathcal{LS}_n$, $\Theta = (\alpha, \beta, \gamma) \in \mathfrak{A}_L$ and $\sigma \in \mathcal{S}_3$, it is verified that $\Theta^\sigma = (\pi_{\sigma(1)}(\Theta), \pi_{\sigma(2)}(\Theta), \pi_{\sigma(3)}(\Theta)) \in \mathfrak{A}_{L^\sigma}$, where π_i gives the i^{th} component of Θ, for all $i \in [3]$. Given $\Theta \in \mathfrak{A}_n$, the set of all Latin squares L such that $\Theta \in \mathfrak{A}_L$ is denoted by $\mathcal{LS}_\Theta$ and the cardinality of $\mathcal{LS}_\Theta$ is denoted by $\Delta(\Theta) = |\mathcal{LS}_\Theta|$. Given $\mathbf{l} \in \mathcal{CS}_n$, it is defined the set $\mathfrak{A}_\mathbf{l} = \{\Theta \in \mathfrak{A}_n \mid \mathbf{l}_\Theta = \mathbf{l}\}$. If $\Theta_1, \Theta_2 \in \mathfrak{A}_\mathbf{l}$, then $\Delta(\Theta_1) = \Delta(\Theta_2)$. Thus, given $\mathbf{l} \in \mathcal{CS}_n$, $\Delta(\mathbf{l})$ denotes the cardinality of $\mathcal{LS}_\Theta$ for all $\Theta \in \mathfrak{A}_\mathbf{l}$. Gröbner bases were used in [1] in order to obtain the number $\Delta(\mathbf{l})$ for autotopisms of Latin squares of order up to 7.

2 Cycle structures of loop autotopisms.

Let us observe that $(Q, \cdot) \in \mathcal{Q}_n$ if and only if, given $i, j, k \in Q$, it is verified that $\begin{cases} (i,k) \in \mathfrak{o}(i,j) \Leftrightarrow k = j, \\ (k,j) \in \mathfrak{o}(i,j) \Leftrightarrow k = i. \end{cases}$ Since Q is a quasigroup, given $i \in Q$, it exists $e, e' \in Q$ such that $i \cdot e = i = e' \cdot i$. But then, it must be $j \cdot e = j = e' \cdot j$, for all $j \in Q$.

Lemma 1. *Every maximum rank quasigroup is a loop.*

Given $\Theta \in \mathcal{I}_n$, let $\mathcal{L}_\Theta = \{L \in \mathcal{L}_n : \Theta \in \mathfrak{A}_L\}$ and let $\Delta_\mathcal{L}(\Theta)$ be the cardinality of the previous set.

Lemma 2. $\Delta_\mathcal{L}(\Theta^{(01)}) = \Delta_\mathcal{L}(\Theta)$, *for all* $\Theta \in \mathcal{I}_n$.

Proposition 1. *Let* $\alpha_1, \alpha_2 \in \mathcal{S}_n$ *be such that* $\mathbf{l}_{\alpha_1} = \mathbf{l}_{\alpha_2}$. *There exists a bijection* φ *between the sets of autotopisms* $S_1(\alpha_1) = \{(\alpha, \beta, \gamma) \in \mathfrak{A}_n \mid \alpha = \alpha_1\}$ *and* $S_1(\alpha_2) = \{(\alpha, \beta, \gamma) \in \mathfrak{A}_n \mid \alpha = \alpha_2\}$, *such that* $\Delta_\mathcal{L}(\varphi(\Theta)) = \Delta_\mathcal{L}(\Theta)$, *for all* $\Theta \in S_1(\alpha_1)$.

Proposition 2. *Let* $L = (l_{i,j}) \in \mathcal{L}_n$ *be the Caley's table of a loop* $([n], \cdot)$ *with unit element* e *and let* $\Theta = (\alpha, \beta, \gamma) \in \mathfrak{A}(L)$.

a) $\gamma(\alpha^{-1}(e)) = \beta(e)$ *and* $\gamma(\beta^{-1}(e)) = \alpha(e)$

b) Let $m \in [n]$. *If* $e \in Fix(\alpha^m)$, *then* $\gamma^m = \beta^m$. *Analogously, if* $e \in Fix(\beta^m)$, *then* $\gamma^m = \alpha^m$.

c) Let $m \in [n]$. *If* $e \notin Fix(\alpha^m)$, *then* $\gamma^m(a) \neq \beta^m(a), \forall a \in [n]$. *Analogously, if* $e \notin Fix(\beta^m)$, *then* $\gamma^m(a) \neq \alpha^m(a), \forall a \in [n]$.

d) Given $t \in [n_\gamma]$ *and* $w \in [\lambda_{n_\gamma}]$, *let* $r \in [n_\alpha]$ *and* $u \in [\lambda_{n_\alpha}]$ *be such that* $c_{r,u}^\alpha = c_{t,w}^\gamma$. *Let* $s \in [n_\beta]$ *and* $v \in [\lambda_{n_\beta}]$ *be such that* $c_{s,v}^\beta = e$. *If there exists* $h \in [l.c.m.(\lambda_s^\beta, \lambda_t^\gamma)]$ *such that* $c_{s,v+h \; (mod \; \lambda_s^\beta)}^\beta = c_{t,w+h \; (mod \; \lambda_t^\gamma)}^\gamma$, *then,* $c_{r,u+h \; (mod \; \lambda_r^\alpha)}^\alpha = e$.

e) Given $t \in [n_\gamma]$ *and* $w \in [\lambda_{n_\gamma}]$, *let* $s \in [n_\beta]$ *and* $v \in [\lambda_{n_\beta}]$ *be such that* $c_{s,v}^\beta = c_{t,w}^\gamma$. *Let* $r \in [n_\alpha]$ *and* $u \in [\lambda_{n_\alpha}]$ *be such that* $c_{r,u}^\alpha = e$. *If there exists* $h \in [l.c.m.(\lambda_r^\alpha, \lambda_t^\gamma)]$ *such that* $c_{r,u+h \; (mod \; \lambda_r^\alpha)}^\alpha = c_{t,w+h \; (mod \; \lambda_t^\gamma)}^\gamma$, *then,* $c_{s,v+h \; (mod \; \lambda_s^\beta)}^\beta = e$.

Theorem 1. *Let* $\Theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n(\mathbf{l}_\alpha, \mathbf{l}_\beta, \mathbf{l}_\gamma)$ *be such that* $\Delta_\mathcal{L}(\Theta) > 0$. *If* $\mathbf{l}_1^\alpha = 0$, *then* $\gamma(a) \neq \beta(a)$, *for all* $a \in [n]$. *Analogously, if* $\mathbf{l}_1^\beta = 0$, *then* $\gamma(a) \neq \alpha(a)$, *for all* $a \in [n]$.

Theorem 2. *Let* $\Theta = (\alpha, \beta, \gamma) \in \mathcal{LI}_n(\mathbf{l}_\alpha, \mathbf{l}_\beta, \mathbf{l}_\gamma)$ *be such that* $\mathbf{l}_1^\alpha = \mathbf{l}_1^\beta = \mathbf{l}_1^\gamma = 1$ *and let us consider* $L \in \mathcal{L}(\Theta)$. *Let* $a, b, c \in [n]$ *be such that* $Fix(\alpha) = \{a\}$, $Fix(\beta) = \{b\}$ *and* $Fix(\gamma) = \{c\}$. *If* $a = c$, *then* b *is the unit element of* L. *Analogously, if* $b = c$, *then* a *is the unit element of* L.

n	$\mathbf{l}_\alpha$	$\mathbf{l}_\beta$	$\mathbf{l}_\gamma$	$\Delta_\mathcal{L}(\Theta)$
2	(0,1)	$(0,1)$	$(2,0)$	2
		$(2,0)$	$(0,1)$	
3	$(0,0,1)$	$(0,0,1)$	$(0,0,1)$	3
		$(0,0,1)$	$(3,0,0)$	
		$(3,0,0)$	$(0,0,1)$	
	$(1,1,0)$	$(1,1,0)$	$(1,1,0)$	1

n	$\mathbf{l}_\alpha$	$\mathbf{l}_\beta$	$\mathbf{l}_\gamma$	$\Delta_\mathcal{L}(\Theta)$
4	(0,0,0,1)	$(0,0,0,1)$	$(0,2,0,0))$	4
		$(0,2,0,0)$	$(0,0,0,1)$	
		$(0,0,0,1)$	$(2,1,0,0)$	2
		$(2,1,0,0)$	$(0,0,0,1)$	
		$(0,0,0,1)$	$(4,0,0,0)$	4
		$(4,0,0,0)$	$(0,0,0,1)$	
	(0,2,0,0)	$(0,2,0,0)$	$(0,2,0,0)$	
		$(0,2,0,0)$	$(2,1,0,0)$	2
		$(2,1,0,0)$	$(0,2,0,0)$	
		$(0,2,0,0)$	$(4,0,0,0)$	4
		$(4,0,0,0)$	$(0,2,0,0)$	
	$(1,0,1,0)$	$(1,0,1,0)$	$(1,0,1,0)$	1
	$(2,1,0,0)$	$(2,1,0,0)$	$(2,1,0,0)$	2

Table 1: Classification of non-trivial autotopisms of loops of order up to 4.

3 The set $\mathcal{Q}_n$.

Let $(Q, \cdot) \in \mathcal{Q}_n$ with unit element e. It is verified that $(i, j \cdot i) = (e \cdot i, j \cdot i), (i, i \cdot j) = (i \cdot e, i \cdot j) \in \mathfrak{o}(e, j)$, for all $i, j \in Q$.

Lemma 3. *Every maximum rank quasigroup is abelian.*

Let $\mathcal{Q}_n^\Theta$ be the subset of $\mathcal{L}_\Theta$, whose elements are Caley's tables of a maximum rank quasigroup and let $\Delta_{\mathcal{Q}_n}(\Theta)$ be the cardinality of the previous set.

Lemma 4. $\Delta_{\mathcal{Q}_n}(\Theta^{(01)}) = \Delta_{\mathcal{Q}_n}(\Theta)$, *for all* $\Theta \in \mathcal{I}_n$.

From the previous result, it is enough to study the cycle structures of those autotopisms (α, β, γ) such that $n_\alpha \leq n_\beta$.

Proposition 3. $(Q, \cdot) \in \mathcal{Q}_n$ *if and only if it is abelian and, given* $i \in Q$, *it is verified that, for all* $x, y \in Q$, $(i \cdot x) \cdot y = i \Leftrightarrow (j \cdot x) \cdot y = j$, *for all* $j \in Q$.

Theorem 3. *Every abelian group has maximum rank.*

Since every loop of order up to 4 is an abelian group, Table 1 shows the classification of the autotopisms of the maximum rank quasigroups of these orders. Now, given a quasigroup $(Q, \cdot)$ with left $\backslash$ and right $/$ division, it is $(i \cdot j) \cdot ((i \cdot j) \backslash j) = j$, for all $i, j \in Q$.

Theorem 4. $(Q, \cdot) \in \mathcal{Q}_n$ *if and only if it is abelian and* $(i \cdot k) \cdot ((i \cdot j) \backslash j) = k$, *for all* $i, j, k \in Q$.

By adding the condition of Theorem 4 to those of Proposition 2, we obtain the number of maximum rank quasigroups having a given isotopism in its autotopism group. Specifically, we show in Tables 2 and 3 this number for quasigroups of order 5 and 6.

$\mathbf{l}_\alpha$	$\mathbf{l}_\beta$	$\mathbf{l}_\gamma$	$\Delta_{\mathcal{Q}_n}(\Theta)$
(0,0,0,0,1)	(0,0,0,0,1)	$(0,0,0,0,1)$	5
		$(5,0,0,0,0)$	
	$(5,0,0,0,0)$	$(0,0,0,0,1)$	
$(1,0,0,1,0)$	$(1,0,0,1,0)$	$(1,0,0,1,0)$	1, 2
$(1,2,0,0,0)$	$(1,2,0,0,0)$	$(1,2,0,0,0)$	1, 2
$(2,0,1,0,0)$	$(2,0,1,0,0)$	$(2,0,1,0,0)$	2, 4, 32

Table 2: Classification of non-trivial autotopisms of maximum rank quasigroups of order 5.

$\mathbf{l}_\alpha$	$\mathbf{l}_\beta$	$\mathbf{l}_\gamma$	$\Delta_{\mathcal{Q}_n}(\Theta)$
(0,0,0,0,0,1)	$(0,0,0,0,0,1)$	$(0,0,2,0,0,0)$	2, 6
	$(0,0,2,0,0,0)$	$(0,0,0,0,0,1)$	
	$(0,0,0,0,0,1)$	$(1,1,1,0,0,0)$	1
	$(1,1,1,0,0,0)$	$(0,0,0,0,0,1)$	1, 3
	$(0,0,0,0,0,1)$	$(2,2,0,0,0,0)$	3
	$(2,2,0,0,0,0)$	$(0,0,0,0,0,1)$	2
	$(0,0,0,0,0,1)$	$(3,0,1,0,0,0)$	
	$(3,0,1,0,0,0)$	$(0,0,0,0,0,1)$	1, 3
	$(0,0,0,0,0,1)$	$(4,1,0,0,0,0)$	3
	$(4,1,0,0,0,0)$	$(0,0,0,0,0,1)$	1, 3
	$(0,0,0,0,0,1)$	$(6,0,0,0,0,0)$	6
	$(6,0,0,0,0,0)$	$(0,0,0,0,0,1)$	
	$(0,0,2,0,0,0)$	$(0,3,0,0,0,0)$	3, 6
	$(0,3,0,0,0,0)$	$(0,0,2,0,0,0)$	1, 2
$(0,3,0,0,0,0)$	$(0,0,2,0,0,0)$	$(0,0,0,0,0,1)$	12
(0,0,2,0,0,0)	$(0,0,2,0,0,0)$	$(0,0,2,0,0,0)$	2, 18
	$(0,0,2,0,0,0)$	$(6,0,0,0,0,0)$	18, 36
	$(6,0,0,0,0,0)$	$(0,0,2,0,0,0)$	72
$(1,0,0,0,1,0)$	$(1,0,0,0,1,0)$	$(1,0,0,0,1,0)$	1, 3
$(0,3,0,0,0,0)$	$(0,3,0,0,0,0)$	$(6,0,0,0,0,0)$	64, 96
$(0,3,0,0,0,0)$	$(6,0,0,0,0,0)$	$(0,3,0,0,0,0)$	240, 144

Table 3: Classification of non-trivial autotopisms of maximum rank quasigroups of order 6.

It is easy to prove that the incidence matrices corresponding to any quasigroup of orders 2 or 3 are, respectively:

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}, \quad \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \right\}$$

Thus, the Bose-Mesner algebra and, therefore, the character table of these quasigroups are univocally determined. Although it is not true for higher orders, we can restrict the general case to a particular one. Specifically, every $(Q, \cdot) \in \mathcal{Q}_n$ is isotopic to a maximum rank quasigroup such that the incidence matrices of their conjugacy classes are the n circulant matrices with ones in their secondary diagonals. It is enough to study the Bose-Mesner algebra related to these quasigroups because of the following: Given $L = (l_{i,j}) \in \mathcal{LS}_n$, it is defined its ***associated matrix*** X_L, which is obtained by replacing each element $l_{i,j}$ by the variable $x_{l_{i,j}}$. The ***determinant*** $\det(L)$ of L is the homogeneous polynomial of degree n in n variables $\det(X_L)$. The factors of these polynomials determine the character table of the corresponding quasigroup [4]. Two polynomials p_1 and p_2 in $\{x_1, x_2, ..., x_n\}$ are said to be ***similar***, if there exists a permutation $\sigma \in S_n$ such that $p_1(x_1, x_2, ..., x_n) = \pm p_2(x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)})$. Thus, it is verified that isotopic and transposed Latin squares have similar determinants and therefore, their character tables have the same structure.

References

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

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

[3] Falcón, R. M. *Incidence structures based on Latin squares autotopisms of a given cycle structure.* Under preparation.

[4] Johnson, K. W. and Smith, J. D. H., *Characters of finite quasigroups.* Eur. J. Comb., **5** (1984), 43–50.

[5] McKay, B. D., Meynert, A. and Myrvold, W. *Small Latin Squares, Quasigroups and Loops.* Journal of Combinatorial Designs 15 (2007) 98-119.

[6] Smith, J. D. H. *An introduction to quasigroups and their representations.* Chapman and Hall/CRC, Boca Raton, FL, 2006.