MATHEMATICA, 62 (85), N° 1, 2020, pp. 33–38

RECTANGULAR TRANSFORMATIONS IN LATIN SQUARES

IVAN I. DERIYENKO

Abstract. To get another one from a given latin square, we have to change at least 4 entries. We show how to find these entries and how to change them.

MSC 2010. 05B15, 20N05.

Key words. Autotopism, latin square, quasigroup.

1. RESULTS

1. The *distance* between two latin squares $||a_{ij}||$ and $||b_{ij}||$ of the same size $n > 2$ is equal to the number of cells in which the corresponding elements a_{ij} and b_{ij} are not equal. The minimal distance between two latin squares is equal 4. Moreover, for any $n > 3$ there exist two latin squares of size n which differ in precisely four entries [10, Theorem 3.3.4]. In the case of latin squares defining groups the situation is more complicated. If two different Cayley tables of order $n \neq \{4, 6\}$ represent groups (not necessary distinct), then they differ from each other in at least $2n$ places. An arbitrary Cayley table of the cyclic group of order 4 differs in at least four places from an arbitrary Cayley table of Klein's 4-group (cf. [6, 7, 9, 10]).

The interesting question is: *when two latin squares which differ in precisely four entries are isomorphic or isotopic.* To solve this problem we will use autotopies of the corresponding quasigroups, i.e., three bijections α, β, γ of a quasigroup Q such that $\alpha(x) \cdot \beta(y) = \gamma(x \cdot y)$ for all $x, y \in Q$.

2. Let $Q = \{1, 2, 3, \ldots, n\}$ be a finite set. The multiplication (composition) of permutations φ and ψ of Q is defined as $\varphi\psi(x) = \varphi(\psi(x))$. All permutations will be written in the form of cycles and cycles will be separated by points, e.g.

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 2 & 5 & 4 & 6 & 8 & 7 \end{pmatrix} = (132.45.6.78.)$$

Permutations L_i $(i \in Q)$ of Q such that $L_i(x) = i \cdot x$, for all $x \in Q$, are called *left translations* of an element i. Such permutations were firstly investigated by V. D. Belousov (cf. [1]) in connection with some groups associated with quasigroups. Next, such translations were used by many authors to describe

DOI: 10.24193/mathcluj.2020.1.04

various properties of quasigroups, see for example [2], [5] or [11]. Left translations are applied in [3] to the construction of some polynomials that can be used to determine which quasigroups are isotopic. Namely, the main results of [3] shows that isotopic quasigroups have the same polynomials.

3. We say that elements $x, y, z, u \in Q$, $x \neq z$, $y \neq u$, determine a *rectangle* in a quasigroup Q if $xy = zu = a$ and $xu = zy = b$ for some $a, b \in Q$. Vertices of such rectangle have the form xy, xu, zx and zu (see example below). Such determined rectangle will be denoted by $\langle x, y, z, u\rangle$ or by $\langle x, u, z, y\rangle$. It is clear that $\langle x, u, z, y\rangle = \langle x,\ x\backslash a,\ a/(x\backslash b),\ x\backslash b\rangle$.

Example 1. The following quasigroup

$\cdot$	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	1	$\boxed{4}$	3	7	5	$\boxed{6}$
3	3	6	5	1	4	7	2
4	4	5	2	7	6	1	3
5	5	4	7	6	2	3	1
6	6	7	1	2	3	4	5
7	7	3	$\boxed{6}$	5	1	2	$\boxed{4}$

has the rectangle $\langle 2, 3, 7, 7\rangle$. Other rectangles of this quasigroup are calculated in Example 4.

Theorem 2. *A group has a rectangle if and only if it has an element of order two.*

Proof. Let x be an element of a group G such that $x^2 = e$ and $x \neq e$. Then $ee = xx = e$, $ex = xe = x$, so $< e, e, x, x >$ is a rectangle (square).

Conversely, let $< x, y, z, u >$ be a rectangle in a group G. Then $xyu^{-1} = xuy^{-1}$, and consequently $(yu^{-1})^2 = e$. So $a = yu^{-1} \neq e$ has order two. □

Lemma 3. *Isotopic* (*antiisotopic*) *quasigroups have the same number of rectangles.*

Proof. Let $(Q, \cdot)$ and $(Q, \circ)$ be isotopic quasigroups, i.e., $\gamma(x{\cdot}y) = \alpha(x){\circ}\beta(y)$ for some bijections of Q and all $x, y \in Q$. Then, as it is not difficult to see, $\langle x, y, z, u\rangle$ is a rectangle of $(Q, \cdot)$ if and only if $\langle\alpha(x), \beta(y), \alpha(z), \beta(u)\rangle$ is a rectangle of $(Q, \circ)$. □

4. Each quasigroup $Q = (Q, \cdot)$ determines five new quasigroups $Q_i = (Q, \circ_i)$ with the operations $\circ_i$ defined as follows:

$$
\begin{aligned}
x \circ_1 y = z &\longleftrightarrow x \cdot z = y \\
x \circ_2 y = z &\longleftrightarrow z \cdot y = x \\
x \circ_3 y = z &\longleftrightarrow z \cdot x = y \\
x \circ_4 y = z &\longleftrightarrow y \cdot z = x \\
x \circ_5 y = z &\longleftrightarrow y \cdot x = z
\end{aligned}
$$

Such defined (not necessarily distinct) quasigroups are called *parastrophes* or *conjugates* of Q. Traditionally they are denoted as

$$Q_1 = Q^{-1} = (Q, \backslash), \quad Q_2 = {}^{-1}Q = (Q, /), \quad Q_3 = {}^{-1}(Q^{-1}) = (Q_1)_2,$$
$$Q_4 = ({}^{-1}Q)^{-1} = (Q_2)_1 \ \text{ and } \ Q_5 = ({}^{-1}(Q^{-1}))^{-1} = ((Q_1)_2)_1 = ((Q_2)_1)_2.$$

From the above results and results obtained in [8] it follows that *a fixed IP-quasigroup and all its parastrophes have the same number of rectangles. Similarly, this holds for a quasigroup isotopic to a group and its parastrophes.*

5. Note that, if a commutative quasigroup has a rectangle $\langle x, y, z, u\rangle$ with $x = y$, then also $z = u$. Similarly, $z = u$ implies $x = y$. So, if in a commutative quasigroup Q one of vertices of the rectangle $\langle x, y, z, u\rangle$ lies on the diagonal of the multiplication table of Q, then this rectangle is a square and its diagonal coincides with the diagonal of the multiplication table.

In Boolean groups each two elements x, y determine the rectangle $\langle x, y, xy, e\rangle$ and each three elements x, y, z determine the rectangle $\langle x, y, z, xyz\rangle$.

An interesting question is how to find rectangles in a given quasigroup. Direct calculation of $\langle x,\ x\backslash a,\ a/(x\backslash b),\ x\backslash b\rangle$ is rather trouble. Below we present simplest method based on left translations.

Let $\langle x, y, z, u\rangle$ be a rectangle in a quasigroup $(Q, \cdot)$. Then, according to the definition, $xy = zu = a$ and $xu = zy = b$. Thus, the left translations L_x and L_z have the form

$$L_x = \begin{pmatrix} \dots & y & \dots & u & \dots \\ \dots & a & \dots & b & \dots \end{pmatrix}, \qquad L_z = \begin{pmatrix} \dots & y & \dots & u & \dots \\ \dots & b & \dots & a & \dots \end{pmatrix}.$$

Hence,

$$L_x L_z^{-1} = \begin{pmatrix} \dots & b & \dots & a & \dots \\ \dots & a & \dots & b & \dots \end{pmatrix}.$$

This means that the permutation $L_x L_z^{-1}$ used in the construction of indicators (for details see [3]) has the cycle (a, b). Thus vertices a, b of this rectangle are located in the x-th row, vertices b, a in the $a/(x\backslash b)$-th row. Since $L_z L_x^{-1} = (L_x L_z^{-1})^{-1}$, the permutation $L_x L_z^{-1}$ and $L_z L_x^{-1}$ have the same cycles of the length 2. So, it is sufficient to calculate $L_x L_z^{-1}$ for $x < z$ only.

Example 4. The quasigroup presented in Example 1 has the following left translations: $L_1 = (1.2.3.4.5.6.7.)$ and

$$L_2 = (12.34.576.), \qquad L_3 = (1354.267.), \qquad L_4 = (1473256.),$$
$$L_5 = (1524637.), \qquad L_6 = (1642753.), \qquad L_7 = (1745.236.).$$

Consequently,

$$L_1 L_2^{-1} = (12.34.576.), \qquad L_2 L_4^{-1} = (15.24.367.), \qquad L_3 L_4^{-1} = (17.25643.),$$
$$L_4 L_5^{-1} = (13.267.54.), \qquad L_2 L_7^{-1} = (17253.46.).$$

In other $L_x L_z^{-1}$ with $x < z$ there are no cycles of length 2.

Below, we present cycles (a, b) and rectangles generated by these cycles:

$(1, 2) : \langle 1, 1, 2, 2\rangle$, $(3, 4) : \langle 1, 3, 2, 4\rangle$, $(1, 5) : \langle 2, 2, 4, 6\rangle$,
$(2, 4) : \langle 2, 1, 4, 3\rangle$, $(1, 7) : \langle 3, 4, 4, 6\rangle$, $(1, 3) : \langle 4, 6, 5, 7\rangle$,
$(5, 4) : \langle 4, 1, 5, 2\rangle$, $(4, 6) : \langle 2, 3, 7, 7\rangle$.

Hence, this quasigroup has eight rectangles.

Note that one pair (a, b) can determine several rectangles.

Example 5. In the quasigroup

$\cdot$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	4	5	6	3
3	3	4	2	6	1	5
4	4	5	6	2	3	1
5	5	6	1	3	2	4
6	6	3	5	1	4	2

the pair $(1, 2)$ determines three rectangles: $\langle 1, 1, 2, 2\rangle$, $\langle 3, 5, 5, 3\rangle$, $\langle 4, 6, 6, 4\rangle$. Other rectangles are: $\langle 3, 3, 4, 4\rangle$, $\langle 3, 3, 6, 6\rangle$, $\langle 4, 4, 5, 5\rangle$ and $\langle 5, 5, 6, 6\rangle$.

6. A quasigroup $(Q, \circ)$ is a *rectangular transformation* of a quasigroup $(Q, \cdot)$ if in $(Q, \cdot)$ there exists a rectangle $\langle a, b, c, d\rangle$ such that

$$x \circ y = \begin{cases} a \cdot d & \text{if } x = a,\ y = b, \\ a \cdot b & \text{if } x = c,\ y = b, \\ c \cdot b & \text{if } x = c,\ y = d, \\ c \cdot d & \text{if } x = a,\ y = d, \\ x \cdot y & \text{in other cases.} \end{cases}$$

Example 6. This quasigroup is obtained from the quasigroup given in Example 1 as a rectangular transformation by $\langle 2, 3, 7, 7\rangle$:

$\circ$	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	1	$\boxed{6}$	3	7	5	$\boxed{4}$
3	3	6	5	1	4	7	2
4	4	5	2	7	6	1	3
5	5	4	7	6	2	3	1
6	6	7	1	2	3	4	5
7	7	3	$\boxed{4}$	5	1	2	$\boxed{6}$

Two rectangles $\langle x, y, z, u\rangle$ and $\langle x', y', z', u'\rangle$ of a quasigroup $(Q, \cdot)$ are *equivalent* if there exists an autotopism (α, β, γ) of $(Q, \cdot)$ such that $\alpha(x) = x'$, $\beta(y) = y'$, $\alpha(z) = z'$ and $\beta(u) = u'$.

Theorem 7. *A rectangular transformation by equivalent rectangles gives isotopic quasigroups.*

Proof. Let $(Q, \circ)$ and $(Q, *)$ be quasigroups obtained from $(Q, \cdot)$ as a rectangular transformation by $\langle a, b, c, d\rangle$ and $\langle \alpha(a), \beta(b), \alpha(c), \beta(d)\rangle$, where (α, β, γ) is an autotopy of a quasigroup $(Q, \cdot)$. Then $\gamma(a \circ b) = \gamma(a \cdot d) = \alpha(a) \cdot \beta(d) = \alpha(a) * \beta(b)$. Analogously, $\gamma(a \circ d) = \alpha(a) * \beta(d)$, $\gamma(c \circ b) = \alpha(c) * \beta(b)$ and $\gamma(c \circ d) = \alpha(c) * \beta(d)$. In other cases, $x \circ y = x \cdot y = x * y$. So, quasigroups $(Q, \circ)$ and $(Q, *)$ are isotopic. □

Example 8. Applying the condition $\gamma L_i \beta^{-1} = L_{\alpha(i)}$, $i = 1, 2 \ldots, 7$, to the quasigroup defined in Example 1, after long computations, we can see that this quasigroup has only one non-trival autotopism. It has the form (α, β, γ), where $\alpha = (15.24.37.6.)$, $\beta = (12.36.47.5.)$, $\gamma = (14.25.67.3.)$. Thus, the rectangle $\langle 1, 1, 2, 2\rangle$ is equivalent to the rectangle $\langle \alpha(1), \beta(1), \alpha(2), \beta(2)\rangle = \langle 5, 2, 4, 1\rangle = \langle 4, 1, 5, 2\rangle$. Also, rectangles $\langle 1, 3, 2, 4\rangle$ and $\langle 4, 6, 5, 7\rangle$, $\langle 2, 1, 4, 3\rangle$ and $\langle 2, 2, 4, 6\rangle$, $\langle 3, 4, 4, 6\rangle$ and $\langle 2, 3, 7, 7\rangle$ are pairwise equivalent. So, the quasigroup defined in Example 1 has four non-equivalent rectangles. Thus, by rectangular transformations, from this quasigroup we obtain four non-isotopic quasigroups.

Observe that by the converse rectrangular tansformations we obtain the same quasigroup. So, by the rectangular transformation from two non-isotopic quasigroups, we can obtain isotopic quasigroups. Hence, the converse of Theorem 7 is not true.

Finally, notice that many other methods of constructing quasigroups from the given quasigroup are known. All of these methods require changing more items in the corresponding latin square. For example, in [5], the method of construction of D-loops from a given IP-loop is presented. In [11], for the construction of new quasigroups, it is used the so-called gisotopism. In turn, in [4], it was shown how to obtain a quasigroup with $n + 1$ elements from a quasigroup with n elements. This method requires changing n items in the initial latin squares. So our method is a method that requires changing the smallest number of elements.

REFERENCES

[1] V.D. Belousov, *The group associated with a quasigroup* (in Russian), Mat. Issled., **4** (1969), 21–39.

[2] I.I. Deriyenko, *Necessary conditions of the isotopy of finite quasigroups* (in Russian), Mat. Issled., **120** (1991), 51–63.

[3] I.I. Deriyenko, *Indicators of quasigroups*, Quasigroups Related Systems, **19** (2011), 223–226.

[4] I.I. Deriyenko and W.A. Dudek, *On prolongations of quasigroups*, Quasigroups Related Systems, **16** (2008), 187–198.

[5] I.I. Deriyenko and W.A. Dudek, *D-loops*, Quasigroups Related Systems, **20** (2012), 183–196.

[6] D. Donovan, S. Oates-Williams and Ch. E. Praeger, *On the distance between distinct group latin squares*, J. Combin. Des., **5** (1997), 235–248.

[7] A. Drápal, *Hamming distances of groups and quasigroups*, Discrete Math., **235** (2001), 189–197.

[8] W.A. Dudek, *Parastrophes of quasigroups*, Quasigroups Related Systems, **23** (2015), 221–230.

[9] S.A. Frisch, *On the minimal distance between group tables*, Acta Sci. Math. (Szeged), **63** (1997), 341–351.

[10] D. Keedwell and J. Dénes, *Latin squares and their applications*, North-Holland, 2015.

[11] V. Shcherbacov, *Elements of quasigroup theory and applications*, CRC Press, 2017.

Received January 23, 2019
Accepted March 14, 2019

Kremenchuk State Polytechnic University
Department of Higher Mathematics and Informatics
39600 Kremenchuk, Ukraine
E-mail: ivan.deriyenko@gmail.com