Quasigroups and Related Systems **18** (2010), 127 – 136

Once more about Brualdi's conjecture

Ivan Deriyenko

Abstract. A new algorithm for finding quasi-complete or complete mappings for Latin squares is presented. This algorithm is a modification of the previous algorithm by this author from 1988.

1. Introduction

In 1988 the author published the paper [3], where he proved the Brualdi's conjecture. In 2005 P. J. Cameron and I. M. Wanless disproved in [1] the author's proof and gave a counter-example. The author agrees with them that his proof presented in [3] is not complete. However, the author does not agree with the counter-example given in [1]. Problems seem to have appeared because the paper was written in Russian, the algorithm was described by the author in a complicated form and it was translated to English without the author's consultancy and not quite correctly (as well as the author's surname which should be Deriyenko, not Derienko). In the present paper the author again describes the algorithm in a simpler form, reveals the groundlessness of the counter-example given in the paper [1]. The way the algorithm works is presented on a concrete example.

The author does not claim that this algorithm gives the final confirmation of the Brualdi's conjecture, but believes that his algorithm gives significant progress in solution to this problem.

2. Preliminaries

$Q(\cdot)$ always denotes a quasigroup, Q – a finite set $\{1,2,3,\dots,n\}$, φ,ψ – permutations of Q, S_Q – the set of all permutations of Q. The composi-

2010 Mathematics Subject Classification: 05B15, 20N05
Keywords: quasigroup, complete mapping, quasicomplete mapping, algorithm, Brualdi's conjecture.

tion of permutations is defined as $\varphi\psi(x) = \varphi(\psi(x))$. Permutations will be written as a composition of cycles; cycles will be separated by dots, e.g.

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 4 & 6 \end{pmatrix} = (132.45.6.)$$

Any permutation φ of Q defines on a quasigroup $Q(\cdot)$ a mapping

$$\overline{\varphi}(x) = x \cdot \varphi(x).$$

By the *range* $rg(\varphi)$ *of a permutation* $\varphi \in S_X$ we mean the number of elements of the set $\overline{\varphi}(X) = \{\overline{\varphi}(x) : x \in X \subseteq Q\}$.

If $|\overline{\varphi}(X)| = |X|$, then we say that φ is a *complete mapping* on the set X. In this case $\overline{\varphi}$ is one-to-one. If $|\overline{\varphi}(X)| < |X|$, then we say that φ is *incomplete* on the set X. In particular, when $|\overline{\varphi}(X)| = |X| - 1$ we say that φ is a *quasicomplete mapping.*

The Brualdi's conjecture (see for example [2])
Every finite quasigroup has a complete or quasicomplete mapping.

In other words, for every finite quasigroup $Q(\cdot)$ there is a permutation φ such that

$$|\overline{\varphi}(Q)| \geqslant |Q| - 1.$$

Some results on the Brualdi's conjecture are known. For example:

- *All groups of odd order have a complete mapping* (see [2]).
- *All symmetric groups* S_n $(n > 3)$ *have a complete mapping* (see [2]).
- *A finite group order* n *which has a cyclic Sylow* 2*-subgroup does not possess a complete mapping* (see [2]).
- *If a quasigroup of order* $4k + 2$ *has a subquasigroup of order* $2k + 1$, *then its multiplication table is without complete mappings* (see [5]).

Some known approximations of the range $t = rg(\varphi)$ of a permutation φ of a quasigroup of order n.

a) $t \geqslant [n - O(\log_2 n)]$, (Sade, 1963, [6])

b) $t \geqslant \left[\frac{2n+1}{3}\right]$ for $n > 7$, (Koksma, 1969, [4])

c) $t \geqslant [n - \sqrt{n}]$, (Woolbrighte, 1978, [9])

d) $t \geqslant \left[n - 5{,}5(\ln n)^2\right]$. (Shor, 1982, [7])

3. D-algorithm

In this section we describe the algorithm which gives the possibility to find a quasicomplete or complete mapping for a given finite quasigroup. But first we prove some auxiliary results.

Let $Q(\cdot)$ be a quasigroup, $X \subseteq Q$, φ some fixed permutation of Q. By the *block* $B_k = \{X, \varphi\}$ of a quasigroup $Q(\cdot)$, where $k = |X|$, we mean the subtable

$$B_k = X \times \varphi(X)$$

contained in the multiplication table of $Q(\cdot)$. The set X is called a *basis* of the block B_k. Note that the same block can be determined by two different permutations φ and ψ. This situation takes place when $\varphi(X) = \psi(X)$. The block $B_k = \{X, \varphi\}$ is called *complete* if

$$|X| = |\overline{\varphi}(X)|.$$

In this case, $\overline{\varphi}$ is one-to-one. If $|\overline{\varphi}(X)| < |X|$, then the block B_k is called *incomplete*. An incomplete block B_k is called *quasicomplete*, if

$$|\overline{\varphi}(X)| = |X| - 1,$$

and a *lopped block*, if

$$|\overline{\varphi}(X)| = |X| - 2. \tag{1}$$

In such block there exists at least one element $z^* \in \overline{\varphi}(X)$, called a *star-element*, such that

$$|\overline{\varphi}^{-1}(z^*)| > 1.$$

The following fact is obvious.

Lemma 3.1. *A lopped block has one or two star-elements.* □

Let Z^* be the set of all star-elements of a lopped block $B = \{X, \varphi\}$ and $\overline{\varphi}^{-1}(Z^*) = S$. If a lopped block B has one star-element z^*, then, obviously

$$S = \overline{\varphi}^{-1}(z^*) = \{s_1, s_2, s_3\}.$$

If it has two star-elements z_1^* and z_2^*, then we have

$$S' = \overline{\varphi}^{-1}(z_1^*) = \{s_1, s_2\}, \qquad S'' = \overline{\varphi}^{-1}(z_2^*) = \{s_3, s_4\},$$

$$S' \cup S'' = S, \qquad S' \cap S'' = \emptyset.$$

So, $|S| = r$, where $r \in \{3,4\}$.

A transposition $\alpha = (s_i, s_j)$ such that $s_i, s_j \in S$ if $|S| = 3$ and $s_i \in S'$, $s_j \in S''$, if $|S| = 4$, is called a *star-transposition.* In the case $|S| = 3$ we have three possibilities to build α, in the case $|S| = 4$ we have four possibilities.

Lemma 3.2. *For a lopped block $B = \{X, \varphi\}$ the following inequality is true:*

$$rg(\varphi\alpha) \geqslant rg(\varphi)$$

Proof. Indeed, since $\varphi\alpha(x) = \varphi(x)$ for $x \in X \setminus S$, we have $\overline{\varphi\alpha}(x) = \overline{\varphi}(x)$ for all $x \in X \setminus S$. Hence $|\overline{\varphi\alpha}(X \setminus S)| = |\overline{\varphi}(X \setminus S)|$. For $s_i, s_j \in S$ elements $\overline{\varphi\alpha}(s_i)$ and $\overline{\varphi\alpha}(s_j)$ may not be in $\overline{\varphi}(X)$. So, $|\overline{\varphi\alpha}(X)| \geqslant |\overline{\varphi}(X)|$. □

Now, let us describe our D-algorithm which gives the possibility to find a quasicomplete or complete mapping.

D-ALGORITHM

Let $Q(\cdot)$ be a fixed quasigroup of order $n \geqslant 3$, $B_k = \{X, \varphi_0\}$ its arbitrary lopped block, $|X| = k$.

STEP 1.

(a) Determine the set S_0 according to $\overline{\varphi}_0$.
Let $S_0 = \{s_{01}, s_{02}, ..., s_{0r}\}$, where $r \in \{3,4\}$.

(b) Determine all star-transpositions $\alpha_1^{(t)} = (s_{0i}, s_{0j})$, $1 \leqslant t \leqslant r$.

(c) Calculate all r permutations $\varphi_1^{(t)} = \varphi_0\alpha_1^{(t)}$.

(d) If $rg(\varphi_1^{(q)}) > rg(\varphi_0)$ for some $\varphi_1^{(q)}$, $1 \leqslant q \leqslant r$, then the goal has been achieved. If not, i.e.,

$$rg(\varphi_1^{(t)}) = rg(\varphi_0) \qquad (2)$$

holds for all $1 \leqslant t \leqslant r$, then we can take one of the star-transpositions, say $\alpha_1 = \alpha_1^{(t_0)}$, calculated in ($b$), put $\varphi_1 = \varphi_0\alpha_1$ and we state in the same block $B_k = \{X, \varphi_1\}$ (with the same set X and $\varphi_1(X) = \varphi_0(X)$), which in view of (2), also will be a lopped block.

STEP $j+1$.

First we start with $j = 1$.

(a) Determine the set S_j according to $\overline{\varphi}_j$, where φ_j was calculated in the previous step.

(b) Determine all star-transpositions $\alpha_{j+1}^{(t)}$.
One of the transpositions $\alpha_{j+1}^{(t)}$ will coincide with the transposition

$\alpha_j^{(t_0)}$ used in the previous step. Suppose that it is $\alpha_{j+1}^{(r)}$. We exclude it from further consideration because it returns us back to φ_j. So, in the future we will consider only permutations of the form

$$\varphi_{j+1}^{(t)} = \varphi_j \alpha_{j+1}^{(t)},$$

where $t = 1, 2, \ldots, r-1, \;\; r = |S_j|$.

(c) If $rg(\varphi_{j+1}^{(t)}) > rg(\varphi_j)$ for some $\varphi_{j+1}^{(t)}$, then the goal has been achieved. If not, i.e.,

$$rg(\varphi_{j+1}^{(t)}) = rg(\varphi_j) \tag{3}$$

for all $1 \leqslant t \leqslant r-1$, then we can take one of the star-transpositions, say $\alpha_{j+1} = \alpha_{j+1}^{(t_0)}$, calculated in (b), put $\varphi_{j+1} = \varphi_j \alpha_{j+1}$ and we state in the same block $B_k = \{X, \varphi_{j+1}\}$ (with the same set X such that $\varphi_{j+1}(X) = \varphi_j(X)$), which in view of (3), also will be a lopped block.

Next we go back to the beginning of the STEP $j+1$ replacing j by $j+1$, i.e., we go back to (a) taking φ_{j+1} instead of φ_j and so on, until we find a permutation $\varphi_m = \varphi_0 \alpha_1 \alpha_2 \ldots \alpha_m$ such that

$$rg(\varphi_m) > rg(\varphi_{m-1}). \tag{4}$$

Now, we can go to the block of higher order.

Inequality (4) admits of two possibilities:

$$rg(\varphi_m) - rg(\varphi_{m-1}) = 2,$$
$$rg(\varphi_m) - rg(\varphi_{m-1}) = 1.$$

In the first case we can add to the set $X = \{x_1, \ldots, x_k\}$ two new elements $x_{k+1}, x_{k+2} \in Q \setminus X$. In this way we obtain the set

$$X_1 = X \cup \{x_{k+1}, x_{k+2}\}.$$

In the second case we add only one element.

This set together with φ_m gives a new lopped block $B' = \{X_1, \varphi_m\}$. We mark it as $B_k = \{X, \varphi_0\}$ and repeat the above algorithm for this block starting from the STEP 1.

After several repetitions, the algorithm stops. The goal will be achieved.

4. Comments

This D-algorithm is not identical with our old algorithm described in [3]. These algorithms have common principles, but they are significantly different. In our old algorithm, each step, starting from the second is uniquely determined. Only in the first step, we have several possibilities to select the initial transposition α_1. In our D-algorithm on each step we have two or three possibilities to select the star-transposition α_j.

In [1] is given the counter-example to the work of our old algorithm. This counter-example shows that our old algorithm can cause a return to the beginning of the procedure. The author agrees with this counter-example, but he do not think that it is a "fatal error" (see [8]) because in each return to the beginning, we can choose a new value of α_1 and repeat the whole procedure. Then we get different results. This algorithm can be repeated in such a way six or eight times.

Our new D-algorithm gives even more possibilities. In this algorithm, in every step the transposition α_j can be chosen in two or three ways. This algorithm can be returned to the start many times and after that we can many times change the way of it works.

The author tested this algorithm on many examples and in each case he received a positive solution. He received a positive solution also in the case of quasigroups of large orders.

The author understands that it is not a complete proof of the Brualdi's conjecture, but if we can show that this D-algorithm gives the possibility to "look" $(k-2)^2+1$ cells from among k^2 cells of a block B_k, then it will be the proof of the Brualdi's conjecture or at least proof that our this algorithm always leads to the goal.

5. Counter-example

The counter-example to our old algorithm was given in [1]. This counter-example is built on "the partial Latin square of order 15". We complete this Latin square and present it below. Elements calculated in [1] are marked here.

$$\left|\begin{array}{ccccccccccccccc}
\boxed{10} & 1 & 3 & 9 & 6 & 7 & 14 & 2 & 15 & 5 & 8 & 11 & 12 & 4 & 13 \\
1 & \boxed{15} & 2 & \boxed{14} & 3 & \boxed{12} & 7 & 4 & 6 & 9 & 10 & 8 & 11 & 13 & 5 \\
2 & \boxed{13} & \boxed{14} & 4 & 7 & 6 & 5 & 10 & 1 & 11 & 15 & 3 & 8 & 9 & 3 \\
3 & 4 & 1 & \boxed{13} & \boxed{14} & \boxed{15} & 6 & 5 & 8 & 2 & 9 & 12 & 7 & 10 & 11 \\
4 & 6 & \boxed{11} & 1 & \boxed{12} & 8 & \boxed{15} & 7 & 13 & 10 & 5 & 9 & 2 & 14 & 3 \\
5 & 3 & \boxed{12} & \boxed{15} & 4 & \boxed{11} & \boxed{13} & 6 & 9 & 1 & 2 & 14 & 10 & 8 & 7 \\
6 & 5 & 4 & 7 & 9 & 3 & \boxed{2} & \boxed{11} & 10 & 8 & 1 & 13 & 14 & 12 & 15 \\
8 & \boxed{11} & \boxed{13} & \boxed{10} & \boxed{15} & \boxed{14} & \boxed{12} & \boxed{1} & \boxed{4} & \boxed{6} & \boxed{7} & \boxed{2} & \boxed{5} & \boxed{3} & 9 \\
7 & 9 & 8 & 5 & 1 & 4 & 10 & \boxed{3} & \boxed{2} & 12 & 14 & 15 & 13 & 11 & 6 \\
9 & 10 & 15 & 11 & 2 & 1 & 8 & 13 & \boxed{5} & \boxed{3} & 12 & \boxed{7} & \boxed{4} & 6 & 14 \\
11 & 14 & 6 & 12 & 5 & 2 & 1 & 9 & \boxed{7} & 13 & \boxed{4} & 10 & \boxed{3} & 15 & 8 \\
12 & 8 & 9 & 2 & 13 & 10 & 3 & 14 & 11 & \boxed{7} & \boxed{6} & \boxed{5} & 15 & 1 & 4 \\
13 & 7 & 10 & 3 & 8 & 9 & 4 & 12 & 14 & 15 & 11 & 1 & \boxed{6} & \boxed{5} & 2 \\
14 & 2 & 5 & 8 & 11 & 13 & 9 & 15 & 12 & \boxed{4} & 3 & \boxed{6} & 1 & \boxed{7} & 10 \\
15 & 12 & 7 & 6 & 10 & 5 & 11 & 8 & 3 & 14 & 13 & 4 & 9 & 2 & \boxed{1}
\end{array}\right|$$

Let us analyze the work of the algorithm using this counter-example.

STEP 1.

We start with the identity permutation $\varphi_0 = \varepsilon$. In this case

$$\overline{\varphi}_0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 10 & 15 & 14 & 13 & 12 & 11 & 2^* & 1^* & 2^* & 3 & 4 & 5 & 6 & 7 & 1^* \end{pmatrix},$$

$Z_0^* = \{1^*, 2^*\}$, $\overline{\varphi}_0^{-1}(1^*) = \{8, 15\} = S_0'$, $\overline{\varphi}_0^{-1}(2^*) = \{7, 9\} = S_0''$. Thus $rg(\varphi_0) = 13$.

Since $S = S' \cup S'' = \{7, 8, 9, 15\}$, we can choose x_0 in four ways. For each selected x_0 we have two possibilities to build a star-transposition α. Hence, we have eight ways to do the first step.

We we select $x_0 = 8$. This element will be fixed for this block in whole our procedure. In the next block another element will be selected and fixed.

For $x_0 = 8$ we have two star-transpositions:

$$\alpha_1^{(1)} = (8, 15) \quad \text{and} \quad \alpha_1^{(2)} = (8, 9).$$

Let us choose the second transposition $\alpha_1 = (8, 9)$. Then

$$\varphi_1 = \varphi_0 \alpha_1 = \varepsilon \alpha_1 = (8, 9).$$

STEP 2.

Now we have

$$\overline{\varphi}_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 10 & 15 & 14 & 13 & 12 & 11 & 2 & 4^* & 3^* & 3^* & 4^* & 5 & 6 & 7 & 1 \end{pmatrix},$$

$Z_1^* = \{3^*, 4^*\}$, $\overline{\varphi}_1^{-1}(3^*) = \{9, 10\} = S_1'$, $\overline{\varphi}_1^{-1}(4^*) = \{8, 1\} = S_1''$ which means that $rg(\varphi_1) = 13$.

Since $x_0 = 8 \in S_1''$, the second element of a star-transposition α_2 should be in S_1'. From the fact that $\alpha_2 \neq \alpha_1$, we obtain

$$\alpha_2 = (8, 10).$$

Hence $\varphi_2 = \varphi_1\alpha_2 = (8, 9)(8, 10) = (8\ 10\ 9.)$.

STEP 3.

$$\overline{\varphi}_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 10 & 15 & 14 & 13 & 12 & 11 & 2 & 6^* & 3 & 5^* & 4 & 5^* & 6^* & 7 & 1 \end{pmatrix},$$

$Z_2^* = \{5^*, 6^*\}$, $\overline{\varphi}_2^{-1}(5^*) = \{10, 12\} = S_2'$, $\overline{\varphi}_2^{-1}(6^*) = \{8, 13\} = S_2''$. Thus $rg(\varphi_2) = 13$.

Then $\alpha_3 = (8, 12)$ and $\varphi_3 = \varphi_2\alpha_3 = (8\ 12\ 10\ 9.)$.

STEP 4.

$$\overline{\varphi}_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 10 & 15 & 14 & 13 & 12 & 11 & 2^* & 2^* & 3 & 5 & 4 & 7^* & 6 & 7^* & 1 \end{pmatrix},$$

$Z_3^* = \{2^*, 7^*\}$, $\overline{\varphi}_3^{-1}(2^*) = \{7, 8\} = S_3'$, $\overline{\varphi}_3^{-1}(7^*) = \{12, 14\} = S_3''$. Hence $rg(\varphi_3) = 13$.

Then $\alpha_4 = (8, 14)$ and $\varphi_4 = \varphi_3\alpha_4 = (8\ 14\ 12\ 10\ 9.)$ and so on.

Continuing this procedure we obtain $\varphi_{48} = \varphi_0$, which means that we return to the start. After that we have seven possibilities to choose α_1. Now we again take $\alpha_1 = (8, 9)$, but in this case we select $x_0 = 9$ as a fixed element.

NEW STEP 1.

$\varphi_1 = \varphi_0\alpha_1 = \varepsilon\alpha_1 = (8, 9)$,

$$\overline{\varphi}_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 10 & 15 & 14 & 13 & 12 & 11 & 2 & 4^* & 3^* & 3^* & 4^* & 5 & 6 & 7 & 1 \end{pmatrix},$$

$Z_1^* = \{3^*, 4^*\}$, $\overline{\varphi}_1^{-1}(3^*) = \{9, 10\} = S_1'$, $\overline{\varphi}_1^{-1}(4^*) = \{8, 11\} = S_1''$. Thus $rg(\varphi_1) = 13$.

Then $\alpha_2 = (9, 11)$ and $\varphi_2 = \varphi_1\alpha_2 = (8\ 9\ 11.)$.

New step 2.

$$\overline{\varphi}_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 10 & 15 & 14^* & 13 & 12 & 11 & 2 & 4 & 14^* & 3 & 9 & 5 & 6 & 7 & 1 \end{pmatrix},$$

$rg(\varphi_2) = 14$.

The goal has been achieved. $\overline{\varphi}_2$ is a quasicomplete mapping.

Remark 5.1. Note that in our old algorithm every step, beginning from the second one, was uniquely determined. In our new algorithm at each stage we have two or three possibilities to perform the next step. Number of possibilities depends on the number of elements of the set S.

Acknowledgments. The author highly values attention paid by Ian Wanless and Peter Cameron to the paper [3] and appreciates the efforts to study this paper written in Russian. The author looks forward to further fruitful cooperation.

Special thanks are due to Wieslaw A. Dudek for helping us writing the final version of the D-algorithm.

Added after publication (February 24, 2011). The citation [6] on page 128 is incorrect. The approximation $t \geqslant [n - O(\log_2 n)]$ was obtained by P. Hatami and P. W. Shor in the article *A lower bound for the length of a partial transversal in Latin square*, J. Comb. Theory, Ser. A, **115** (2008), 1103 – 1113.

References

[1] **P. J. Cameron and I. M. Wanless**, *Covering radius for sets of permutations*, Discrete Math. **293** (2005), 91 – 109.

[2] **J. Dénes and A. D. Keedwell**, *Latin squares and their applications*, Akadémiai Kiadó, Budapest, 1974.

[3] **I. I. Deriyenko**, *On the Brualdi hypothesis*, (Russian), Mat. Issled. **102** (1988), 53 – 65.

[4] **K. K. Koksma**, *A lower bound for the order of a partial transversal in a Latin square*, J. Comb. Theory **7** (1969), 94 – 95.

[5] **H. B. Mann**, *The construction of orthogonal Latin squares*, Ann. Math. Stat. **13** (1942), 418 – 423.

[6] **A. Sade**, *Isotopies d'un groupoide avec son conjont*, Rend. Circ. Mat. Palermo, II Ser. **12** (1963), 357 – 381.

[7] **P. W. Shor**, *A lower bound for the length of a partial transversal in a Latin square*, J. Comb. Theory, Ser A **33** (1982), 1 – 8.

[8] **I. M. Wanless**, *Transversals in Latin squares*, Quasigroups and Related Systems **15** (2007), 169 – 190.

[9] **D. E. Woolbright**, *An $n \times n$ Latin square has a transversal with at least $n - \sqrt{n}$ distinct symbols*, J. Comb. Theory **24** (1978), 235 – 237.

Received November 30, 2010

Department of Higher Mathematics and Informatics
Kremenchuk National University
20 Pervomayskaya str.
39600 Kremenchuk
Ukraine
E-mail: ivan.deriyenko@gmail.com