Quasigroups and Related Systems **16** (2008), 55 – 67

On reconstructing reducible n-ary quasigroups and switching subquasigroups

Denis S. Krotov, Vladimir N. Potapov, Polina V. Sokolova

Abstract

(1) We prove that, provided $n \geqslant 4$, a permutably reducible n-ary quasigroup is uniquely specified by its values on the n-ples containing zero. (2) We observe that for each $n, k \geqslant 2$ and $r \leqslant \lfloor k/2 \rfloor$ there exists a reducible n-ary quasigroup of order k with an n-ary subquasigroup of order r. As corollaries, we have the following: (3) For each $k \geqslant 4$ and $n \geqslant 3$ we can construct a permutably irreducible n-ary quasigroup of order k. (4) The number of n-ary quasigroups of order $k > 3$ has double-exponential growth as $n \to \infty$; it is greater than $\exp\exp(n \ln\lfloor k/3 \rfloor)$ if $k \geqslant 6$, and $\exp\exp(\frac{\ln 3}{3}n - 0.44)$ if $k = 5$.

1. Introduction

An n-ary operation $f : \Sigma^n \to \Sigma$, where Σ is a nonempty set, is called an *n-ary quasigroup* or *n-quasigroup* (*of order* $|\Sigma|$) iff in the equality $z_0 = f(z_1, \ldots, z_n)$ knowledge of any n elements of z_0, z_1, ..., z_n uniquely specifies the remaining one [2].

An n-ary quasigroup f is *permutably reducible* iff

$$f(x_1, \ldots, x_n) = h\left(g(x_{\sigma(1)}, \ldots, x_{\sigma(k)}), x_{\sigma(k+1)}, \ldots, x_{\sigma(n)}\right)$$

where h and g are $(n-k+1)$-ary and k-ary quasigroups, σ is a permutation, and $1 < k < n$. In what follows we omit the word "permutably" because we consider only such type of reducibility.

2000 Mathematics Subject Classification: 20N15 05B15
Keywords: irreducible quasigroups, latin hypercubes, n-ary quasigroups, reducibility, subquasigroup
The first and the second authors were partially supported by the Russian Foundation for Basic Research (Grants 08-01-00673 and 08-01-00671 respectively)

We will use the following standard notation: x_i^j denotes $x_i, x_{i+1}, \ldots, x_j$.

In Section 2 we show that a reducible n-quasigroup can be reconstructed by its values on so-called 'shell'. 'Shell' means the set of variable values with at least one zero.

In Section 3 we consider the questions of imbedding n-quasigroups of order r into n-quasigroups of order $k \geqslant 2r$.

In Section 4 we prove that for all $n \geqslant 3$ and $k \geqslant 4$ there exists an irreducible n-quasigroup of order k. Before, the question of existence of irreducible n-quasigroups was considered by Belousov and Sandik [3] ($n = 3$, $k = 4$), Frenkin [5] ($n \geqslant 3$, $k = 4$), Borisenko [4] ($n \geqslant 3$, composite finite k), Akivis and Goldberg [7, 8, 1] (local differentiable n-quasigroups), Glukhov [6] ($n \geqslant 3$, infinite k).

In Sections 5 and 6 we prove the double-exponential ($\exp\exp(c(k)n)$) lower bound on the number $|Q(n, k)|$ of n-quasigroups of finite order $k \geqslant 4$. Before, the following asymptotic results on the number of n-quasigroups of fixed finite order k were known:

- $|Q(n, 2)| = 2$.
- $|Q(n, 3)| = 3 \cdot 2^n$, see, e.g., [13]; a simple way to realize this fact is to show by induction that the values on the shell uniquely specify an n-quasigroup of order 3.
- $|Q(n, 4)| = 3^{n+1}2^{2^n+1}(1 + o(1))$ [15, 11].

Note that by the "number of n-quasigroups" we mean the number of mutually different n-ary quasigroup operations $\Sigma^n \to \Sigma$ for a fixed Σ, $|\Sigma| = k$ (sometimes, by this phrase one means the number of isomorphism classes). As we will see, for every $k \geqslant 4$ there is $c(k) > 0$ such that $|Q(n, k)| \geqslant 2^{2^{c(k)n}}$. More accurately (Theorem 3), if $k = 5$ then $|Q(n, 5)| \geqslant 2^{3^{n/3-const}}$; for even k we have $|Q(n, k)| \geqslant 2^{(k/2)^n}$; for $k \equiv 0 \bmod 3$ we have $|Q(n, k)| \geqslant 2^{n(k/3)^n}$; and for every k we have $|Q(n, k)| \geqslant 2^{1.5\lfloor k/3\rfloor^n}$. Observe that dividing by the number (e.g., $(n + 1)!(k!)^n$) of any natural equivalences (isomorphism, isotopism, paratopism,...) does not affect these values notably; so, for the number of equivalence classes almost the same bounds are valid. For the known exact numbers of n-quasigroups of order k with small values of n and k, as well as the numbers of equivalence classes for different equivalences, see the recent paper of McKay and Wanless [14].

2. On reconstructing reducible n-quasigroups

In what follows the constant tuples $\bar{o}$, $\bar{\theta}$ may be considered as all-zero tuples. From this point of view, the main result of this section states that a reducible n-quasigroup is uniquely specified by its values on the 'shell', where the 'shell' is the set of n-ples with at least one zero. Lemma 1 and its corollary concern the case when the groups of variables in the decomposition of a reducible n-quasigroup are fixed. In Theorem 1 the groups of variables are not specified; we have to require $n \geqslant 4$ in this case.

Lemma 1 (a representation of a reducible n-quasigroup by the superposition of retracts). *Let h and g be an $(n-m+1)$- and m-quasigroups, let $\bar{o} \in \Sigma^{m-1}$, $\bar{\theta} \in \Sigma^{n-m}$, and let*

$$f(x,\bar{y},\bar{z}) \stackrel{\mathrm{def}}{=} h(g(x,\bar{y}),\bar{z}),$$
$$h_0(x,\bar{z}) \stackrel{\mathrm{def}}{=} f(x,\bar{o},\bar{z}), \qquad g_0(x,\bar{y}) \stackrel{\mathrm{def}}{=} f(x,\bar{y},\bar{\theta}), \qquad \delta(x) \stackrel{\mathrm{def}}{=} f(x,\bar{o},\bar{\theta}) \quad (1)$$

where $x \in \Sigma$, $\bar{y} \in \Sigma^{m-1}$, $\bar{z} \in \Sigma^{n-m}$. Then

$$f(x,\bar{y},\bar{z}) \equiv h_0(\delta^{-1}(g_0(x,\bar{y})),\bar{z}). \quad (2)$$

Proof. It follows from (1) that

$$h_0(\cdot,\bar{z}) \equiv h(g(\cdot,\bar{o}),\bar{z}), \quad g_0(x,\bar{y}) \equiv h(g(x,\bar{y}),\bar{\theta}), \quad \delta^{-1}(\cdot) \equiv g^{-1}(h^{-1}(\cdot,\bar{\theta}),\bar{o}).$$

Substituting these representations of h_0, g_0, δ^{-1} to (2), we can readily verify its validity. □

Corollary 1. *Let $q_{in}, q_{out}, f_{in}, f_{out} : \Sigma^2 \to \Sigma$ be some quasigroups, $q \stackrel{\mathrm{def}}{=} q_{out}(x_1, q_{in}(x_2,x_3))$, $f \stackrel{\mathrm{def}}{=} f_{out}(x_1, f_{in}(x_2,x_3))$, and $(o_1,o_2,o_3) \in \Sigma^3$. Assume that for all $(x_1,x_2,x_3) \in \Sigma^3$ it holds*

$$q(o_1,x_2,x_3) = f(o_1,x_2,x_3), \quad q(x_1,o_2,x_3) = f(x_1,o_2,x_3).$$

Then $q(\bar{x}) = f(\bar{x})$ for all $\bar{x} \in \Sigma^3$.

Theorem 1. *Let $q, f : \Sigma^n \to \Sigma$ be reducible n-quasigroups, where $n \geqslant 4$; and let $o_1^n \in \Sigma^n$. Assume that for all $i \in \{1,\ldots,n\}$ and for all $x_1^n \in \Sigma^n$ it holds*

$$q(x_1^{i-1}, o_i, x_{i+1}^n) = f(x_1^{i-1}, o_i, x_{i+1}^n). \quad (3)$$

Then $q(x_1^n) = f(x_1^n)$ for all $x_1^n \in \Sigma^n$.

Proof. (*) We first proof the claim for $n = 4$. Without loss of generality (up to coordinate permutation and/or interchanging q and f), we can assume that one of the following holds for some quasigroups $q_{in}, q_{out}, f_{in}, f_{out}$:

Case 1) $q(x_1^4) = q_{out}(x_1, q_{in}(x_2, x_3, x_4))$, $f(x_1^4) = f_{out}(x_1, f_{in}(x_2, x_3, x_4))$;
Case 2) $q(x_1^4) = q_{out}(x_1, q_{in}(x_2, x_3, x_4))$, $f(x_1^4) = f_{out}(x_1, f_{in}(x_2, x_3), x_4)$;
Case 3) $q(x_1^4) = q_{out}(x_1, q_{in}(x_2, x_3), x_4)$, $f(x_1^4) = f_{out}(x_1, f_{in}(x_2, x_3), x_4)$;
Case 4) $q(x_1^4) = q_{out}(x_1, q_{in}(x_2, x_3, x_4))$, $f(x_1^4) = f_{out}(f_{in}(x_1, x_2, x_3), x_4)$;
Case 5) $q(x_1^4) = q_{out}(x_1, q_{in}(x_2, x_3, x_4))$, $f(x_1^4) = f_{out}(f_{in}(x_1, x_4), x_2, x_3)$;
Case 6) $q(x_1^4) = q_{out}(x_1, x_2, q_{in}(x_3, x_4))$, $f(x_1^4) = f_{out}(x_1, f_{in}(x_2, x_3), x_4)$;
Case 7) $q(x_1^4) = q_{out}(x_1, q_{in}(x_2, x_3), x_4)$, $f(x_1^4) = f_{out}(f_{in}(x_1, x_4), x_2, x_3)$.

1,2,3) Take an arbitrary x_4 and denote $q'(x_1, x_2, x_3) \stackrel{\text{def}}{=} q(x_1, x_2, x_3, x_4)$ and $f'(x_1, x_2, x_3) \stackrel{\text{def}}{=} f(x_1, x_2, x_3, x_4)$. Then, by Corollary 1, we have $q'(\bar{x}) = f'(\bar{x})$ for all $\bar{x} \in \Sigma^3$; this proves the statement.

4) Fixing $x_4 := o_4$ and applying (3) with $i = 4$, we have

$$f_{out}(f_{in}(x_1, x_2, x_3), o_4) = q_{out}(x_1, q_{in}(x_2, x_3, o_4)),$$

which leads to the representation $f_{in}(x_1, x_2, x_3) = h_{out}(x_1, h_{in}(x_2, x_3))$ where $h_{out}(x_1, \cdot) \stackrel{\text{def}}{=} f_{out}^{-1}(q_{out}(x_1, \cdot), o_4)$ and $h_{in}(x_2, x_3) \stackrel{\text{def}}{=} q_{in}(x_2, x_3, o_4)$. Using this representation, we find that f satisfies the condition of Case 2) for some f_{in}, f_{out}. So, the situation is reduced to the already-considered case.

5) Fixing $x_4 := o_4$ and using (3), we obtain the decomposition $f_{out}(\cdot, \cdot, \cdot) = h_{out}(\cdot, h_{in}(\cdot, \cdot))$ for some h_{in}, h_{out}. We find that q and f satisfy the conditions of Case 2).

6) Fixing $x_4 := o_4$ and using (3), we get the decomposition $q_{out}(\cdot, \cdot, \cdot) = h_{out}(\cdot, h_{in}(\cdot, \cdot))$. Then, we again reduce to Case 2).

7) Fixing $x_4 := o_4$ we derive the decomposition $f_{out}(\cdot, \cdot, \cdot) = h_{out}(\cdot, h_{in}(\cdot, \cdot))$, which leads to Case 3).

(**) Assume $n > 4$. It is straightforward to show that we always can choose four indexes $1 \leqslant i < j < k < l \leqslant n$ such that for all x_1^{i-1}, x_{i+1}^{j-1}, x_{j+1}^{k-1}, x_{k+1}^{l-1}, x_{l+1}^n the 4-quasigroups

$$q'_{x_1^{i-1} x_{i+1}^{j-1} x_{j+1}^{k-1} x_{k+1}^{l-1} x_{l+1}^n}(x_i, x_j, x_k, x_l) \stackrel{\text{def}}{=} q(x_1^n),$$
$$f'_{x_1^{i-1} x_{i+1}^{j-1} x_{j+1}^{k-1} x_{k+1}^{l-1} x_{l+1}^n}(x_i, x_j, x_k, x_l) \stackrel{\text{def}}{=} f(x_1^n)$$

are reducible. Since these 4-quasigroups satisfy the hypothesis of the lemma, they are identical, according to (*). Since they coincide for every values of the parameters, we see that q and f are also identical. □

Remark 1. If $n = 3$ then the claim of Lemma 1 can fail. For example, the reducible 3-quasigroups $q(x_1^3) \stackrel{\text{def}}{=} (x_1 * x_2) * x_3$ and $f(x_1^3) \stackrel{\text{def}}{=} x_1 * (x_2 * x_3)$ where $*$ is a binary quasigroup with an identity element 0 (i. e., a loop) coincide if $x_1 = 0$, $x_2 = 0$, or $x_3 = 0$; but they are not identical if $*$ is nonassociative.

3. Subquasigroup

Let $q : \Sigma^n \to \Sigma$ be an n-quasirgoup and $\Omega \subset \Sigma$. If $g = q|_{\Omega^n}$ is an n-quasirgoup then we will say that g is a *subquasigroup* of q and q is Ω-*closed*.

Lemma 2. *For each finite Σ with $|\Sigma| = k$ and $\Omega \subset \Sigma$ with $|\Omega| \leqslant \lfloor k/2 \rfloor$ there exists a reducible n-quasigroup $q : \Sigma^n \to \Sigma$ with a subquasigroup $g : \Omega^n \to \Omega$.*

Proof. By Ryser theorem on completion of a Latin $s \times r$ rectangular up to a Latin $k \times k$ square (2-quasigroup) [16], there exists a Ω-closed 2-quasigroup $q : \Sigma^2 \to \Sigma$.

To be constructive, we suggest a direct formula for the case $\Sigma = \{0, \ldots, k-1\}$, $\Omega = \{0, \ldots, r-1\}$ where $k \geqslant 2r$ and $k - r$ is odd:

$$\begin{aligned}
q_{k,r}(i,j) &= (i+j) \bmod r, && i < r, j < r;\\
q_{k,r}(r+i,j) &= (i+j) \bmod (k-r) + r, && j < r;\\
q_{k,r}(i,r+j) &= (2i+j) \bmod (k-r) + r, && i < r;\\
q_{k,r}(r+i,r+j) &= \begin{cases} (i-j) \bmod (k-r) & \text{if } (i-j) \bmod (k-r) < r,\\ (2i-j) \bmod (k-r) + r & \text{otherwise.} \end{cases}
\end{aligned}$$

In the following four examples the second and the fourth value arrays correspond to $q_{5,2}$ and $q_{7,2}$:

$$4:\ \begin{array}{|cc|cc|} \hline 0 & 1 & 2 & 3\\ 1 & 0 & 3 & 2\\ \hline 2 & 3 & 0 & 1\\ 3 & 2 & 1 & 0\\ \hline \end{array} \qquad 5:\ \begin{array}{|cc|ccc|} \hline 0 & 1 & 2 & 3 & 4\\ 1 & 0 & 3 & 4 & 2\\ \hline 2 & 4 & 0 & 1 & 6\\ 3 & 2 & 4 & 0 & 1\\ 4 & 3 & 1 & 5 & 0\\ \hline \end{array} \qquad 6:\ \begin{array}{|cc|cccc|} \hline 0 & 1 & 2 & 3 & 4 & 5\\ 1 & 0 & 3 & 2 & 5 & 4\\ \hline 4 & 5 & 0 & 1 & 2 & 3\\ 5 & 4 & 1 & 0 & 3 & 2\\ 2 & 3 & 4 & 5 & 0 & 1\\ 3 & 2 & 5 & 4 & 1 & 0\\ \hline \end{array} \qquad 7:\ \begin{array}{|cc|ccccc|} \hline 0 & 1 & 2 & 3 & 4 & 5 & 6\\ 1 & 0 & 3 & 4 & 5 & 6 & 2\\ \hline 2 & 4 & 0 & 1 & 6 & 3 & 5\\ 3 & 5 & 6 & 0 & 1 & 2 & 4\\ 4 & 6 & 5 & 2 & 0 & 1 & 3\\ 5 & 2 & 4 & 6 & 3 & 0 & 1\\ 6 & 3 & 1 & 5 & 2 & 4 & 0\\ \hline \end{array} \tag{4}$$

Now, the statement follows from the obvious fact that a superposition of Ω-closed 2-quasigroups is an Ω-closed n-quasigroup. $\square$

The next obvious lemma is a suitable tool for obtaining a large number of n-quasigroups, most of which are irreducible.

Lemma 3 (switching subquasigroups). *Let $q : \Sigma^n \to \Sigma$ be an Ω-closed n-quasigroup with a subquasigroup $g : \Omega^n \to \Omega$, $g = q|_{\Omega^n}$, $\Omega \subset \Sigma$. And let $h : \Omega^n \to \Omega$ be another n-quasigroup of order $|\Omega|$. Then*

$$f(\bar{x}) \stackrel{\text{def}}{=} \begin{cases} h(\bar{x}) & \text{if } \bar{x} \in \Omega^n \\ q(\bar{x}) & \text{if } \bar{x} \notin \Omega^n \end{cases} \tag{5}$$

is an n-quasigroup of order $|\Sigma|$.

4. Irreducible n-quasigroups

Lemma 4. *A subquasigroup of a reducible n-quasigroup is reducible.*

Proof. Let $f : \Sigma^n \to \Sigma$ be a reducible Ω-closed n-quasigroup. Without loss of generality we assume that

$$f(x, \bar{y}, \bar{z}) \equiv h(g(x, \bar{y}), \bar{z})$$

for some $(n - m + 1)$- and m-quasigroups h and g where $1 < m < n$. Take $\bar{o} \in \Omega^{m-1}$ and $\theta \in \Omega^{n-m}$. Then the quasigroups h_0, g_0, and δ defined by (1) are Ω-closed. Therefore, the representation (2) proves that $f|_{\Omega^n}$ is reducible. □

Theorem 2. *For each $n \geqslant 3$ and $k \geqslant 4$ there exists an irreducible n-quasigroup of order k.*

Proof. (*) First we consider the case $n \geqslant 4$. By Lemma 2 we can construct a reducible n-quasigroup $q : \{0, \ldots, k-1\}^n \to \{0, \ldots, k-1\}$ of order k with a subquasigroup $g : \{0, 1\}^n \to \{0, 1\}$ of order 2. Let $h : \{0, 1\}^n \to \{0, 1\}$ be the n-quasigroup of order 2 different from g; and let f be defined by (5). By Theorem 1 with $\bar{o} = (2, \ldots, 2)$, the n-quasigroup f is irreducible.

(**) $n = 3$, $k = 4, 5, 6, 7$. In each of these cases we will construct an irreducible 3-quasigroup f, omitting the verification, which can be done, for example, using the formulas (1), (2). Let quasigroups $q_{4,2}$, $q_{5,2}$, $q_{6,2}$, and $q_{7,2}$ be defined by the value arrays (4). For each case $k = 4, 5, 6, 7$ we define the ternary quasigroup $q(x_1, x_2, x_3) \stackrel{\text{def}}{=} q_{k,2}(q_{k,2}(x_1, x_2), x_3)$, which have the subquasigroup $q|_{\{0,1\}^3}(x_1, x_2, x_3) = x_1 + x_2 + x_3 \bmod 2$. Using (5), we replace this subquasigroup by the ternary quasigroup $h(x_1, x_2, x_3) = x_1 + x_2 + x_3 + 1 \bmod 2$. The resulting ternary quasigroup f is irreducible.

(***) $n = 3$, $8 \leqslant k < \infty$. Using Lemma 2, Lemma 3, and (**), we can easily construct a ternary quasigroup of order $k \geqslant 8$ with an irreducible subquasigroup of order 4. By Lemma 4, such quasigroup is irreducible.

(****) The case of infinite order. Let $q : \Sigma_\infty^n \to \Sigma_\infty$ be an n-quasigroup of infinite order K and $g : \Sigma^n \to \Sigma$ be any irreducible n-quasigroup of finite order (say, 4). Then, by Lemma 4, their direct product $g{\times}q : (\Sigma \times \Sigma_\infty)^n \to (\Sigma \times \Sigma_\infty)$ defined as

$$g{\times}q\ \big([x_1, y_1], \dots, [x_n, y_n]\big) \stackrel{\text{def}}{=} \big[g(x_1, \dots, x_n), q(y_1, \dots, y_n)\big]$$

is an irreducible n-quasigroup of order K. $\square$

Remark 2. Using the same arguments, it is easy to construct for any $n \geqslant 4$ and $k \geqslant 4$ an irreducible n-quasigroup of order k such that fixing one argument (say, the first) by (say) 0 leads to an $(n-1)$-quasigroup that is also irreducible. This simple observation naturally blends with the following context. Let $\kappa(q)$ be the maximal number such that there is an irreducible $\kappa(q)$-quasigroup that can be obtained from q or one of its inverses by fixing $n - \kappa(q) > 0$ arguments. In this remark we observe that (for any n and k when the question is nontrivial) there is an irreducible n-quasigroup q with $\kappa(q) = n - 1$. In [10] for $k \vdots 4$ and even $n \geqslant 4$ an irreducible n-quasigroup with $\kappa(q) = n - 2$ is constructed. In [9, 12] it is shown that $\kappa(q) \leqslant n - 3$ (if k is prime then $\kappa(q) \leqslant n - 2$) implies that q is reducible.

5. On the number of n-quasigroups, I

We first consider a simple bound on the number of n-quasigroups of composite order.

Proposition 1. *The number $|Q(n, sr)|$ of n-quasigroups of composite order sr satisfies*

$$|Q(n, sr)| \geqslant |Q(n, r)| \cdot |Q(n, s)|^{r^n} > |Q(n, s)|^{r^n}. \qquad (6)$$

Proof. Let $g : Z_r^n \to Z_r$ be an arbitrary n-quasigroup of order r; and let $\omega\langle\cdot\rangle$ be an arbitrary function from Z_r^n to the set $Q(n, s)$ of all n-quasigroups of order s. It is straightforward that the following function is an n-quasigroup of order sr:

$$f(z_1^n) \stackrel{\text{def}}{=} g\left(y_1^n\right) \cdot s + \omega\left\langle y_1^n\right\rangle\left(x_1^n\right) \quad \text{where } y_i \stackrel{\text{def}}{=} \lfloor z_i/s \rfloor, \quad x_i \stackrel{\text{def}}{=} z_i \bmod s.$$

Moreover, different choices of $\omega\langle\cdot\rangle$ result in different n-quasigroups. So, this construction, which is known as the ω-product of g, obviously provides the bound (6). $\square$

If the order is divided by 2 or 3 then the bound (6) is the best known. Substituting the known values $|Q(n,2)| = 2$ and $|Q(n,3)| = 3 \cdot 2^n$, we get

Corollary 2. *If* $k \vdots 2$ *then* $|Q(n,k)| \geqslant 2^{(k/2)^n}$;

if $k \vdots 3$ *then* $|Q(n,k)| \geqslant (3 \cdot 2^n)^{(k/3)^n} > 2^{n(k/3)^n}$.

The next statement is weaker than the bound considered in the next section. Nevertheless, it provides simplest arguments showing that the number of n-quasigroup of fixed order k grows double-exponentially, even for prime $k \geqslant 8$. The cases $k = 5$ and $k = 7$ will be covered in the next section.

Proposition 2. *The number* $|Q(n,k)|$ *of* n*-quasigroups of order* $k \geqslant 8$ *satisfies*

$$|Q(n,k)| \geqslant 2^{\lfloor k/4 \rfloor^n}. \tag{7}$$

Proof. By Lemma 2, there is an n-quasigroup of order k with subquasigroup of order $2\lfloor k/4 \rfloor$. This subquasigroup can be switched (see Lemma 3) in $|Q(n, 2\lfloor k/4 \rfloor)|$ ways. By Proposition 1, we have

$$|Q(n, 2\lfloor k/4 \rfloor)| \geqslant |Q(n,2)|^{\lfloor k/4 \rfloor^n} = 2^{\lfloor k/4 \rfloor^n}.$$

Clearly, these calculations have sense only if $\lfloor k/4 \rfloor > 1$, i. e., $k \geqslant 8$. □

6. On the number of n-quasigroups, II

In this section we continue using the same general switching principle as in previous ones: independent changing the values of n-quasigroups on disjoint subsets of Σ^n. We improve the lower bound in the cases when the order is not divided by 2 or 3; in particular, we establish a double-exponential lower bound on the number of n-quasigroups of orders 5 and 7.

We say that a nonempty set $\Theta \subset \Sigma^n$ is an *ab-component* or a *switching component* of an n-quasigroup q iff

(**a**) $q(\Theta) = \{a, b\}$ and

(**b**) the function $q\Theta : \Sigma^n \to \Sigma$ defined as follows is an n-quasigroup too:

$$q\Theta(\bar{x}) \stackrel{\mathrm{def}}{=} \begin{cases} q(\bar{x}) & \text{if } \bar{x} \notin \Theta \\ b & \text{if } \bar{x} \in \Theta \text{ and } q(\bar{x}) = a \\ a & \text{if } \bar{x} \in \Theta \text{ and } q(\bar{x}) = b. \end{cases}$$

For example, $\{(0,0),(0,1),(1,0),(1,1)\}$ and $\{(2,2),(2,3),(3,3),(3,4),(4,2),(4,4)\}$ are 01-components in (4.5).

Remark 3. From some point of view, it is naturally to require also Θ to be inclusion-minimal, i.e., (**c**) Θ does not have a nonempty proper subset that satisfies (a) and (b). Although in what follows all ab-components satisfy (c), formally we do not use it.

Lemma 5. *Let an n-quasigroup q have s pairwise disjoint switching components $\Theta_1, \ldots, \Theta_s$ (note that we do not require them to be ab-components for common a, b). Then $|Q(n,|\Sigma|)| \geqslant 2^s$.*

Proof. Indeed, denoting $q\Theta^0 \stackrel{\mathrm{def}}{=} q$ and $q\Theta^1 \stackrel{\mathrm{def}}{=} q\Theta$, we have 2^s distinct n-quasigroups $q\Theta_1^{t_1}...\Theta_s^{t_s}$, $(t_1,\ldots,t_s)\in\{0,1\}^s$. □

6.1. The order 5

In this section, we consider the n-quasigroups of order 5, the only case, when the other our bounds do not guarantee the double-exponential growth of the number of n-quasigroups as $n\to\infty$. Of course, the way that we use for the order 5 works for any other order $k>3$, but the bound obtained is worse than (6) provided k is composite, worse than (7) provided $k\geqslant 8$, and worse than (8) provided $k\geqslant 6$. The bound is based on the following straightforward fact:

Lemma 6. *Let $\{0,1\}^n$ be a 01-component of an n-quasigroup q. For every $i\in\{1,\ldots,n\}$ let q_i be an n_i-quasigroup and let Θ_i be its 01-component. Then $\Theta_1\times\ldots\times\Theta_n$ is a 01-component of the $(n_1+\ldots+n_n)$-quasigroup*

$$f(x_{1,1},...,x_{1,n_1},x_{2,1},\ldots,x_{n,n_n}) \stackrel{\mathrm{def}}{=} q(q_1(x_{1,1},...,x_{1,n_1}),\ldots,q_n(x_{n,1},...,x_{n,n_n})).$$

For a quasigroup $q:\Sigma^2\to\Sigma$ denote $q^1 \stackrel{\mathrm{def}}{=} q$, $q^2(x_1,x_2,x_3) \stackrel{\mathrm{def}}{=} q(x_1,q^1(x_2,x_3))$, $\ldots$, $q^i(x_1,x_2,\ldots,x_{i+1}) \stackrel{\mathrm{def}}{=} q(x_1,q^{i-1}(x_2,\ldots,x_{i+1}))$.

Proposition 3. *If $n=3m$ then $|Q(n,5)|\geqslant 2^{3^m}$; if $n=3m+1$ then $|Q(n,5)|\geqslant 2^{4\cdot 3^{m-1}}$; if $n=3m+2$ then $|Q(n,5)|\geqslant 2^{2\cdot 3^m}$. Roughly, for any n we have*

$$|Q(n,5)| > 2^{3^{n/3-0.072}} > e^{e^{\frac{\ln 3}{3}n-0.44}}.$$

Proof. Let q be the quasigroup of order 5 with value table (4.5). Then

(*) q has two disjoint 01-components $D_0 \stackrel{\mathrm{def}}{=} \{(0,0),(0,1),(1,0),(1,1)\}$ and $D_1 \stackrel{\mathrm{def}}{=} \{(2,2),(2,3),(3,3),(3,4),(4,2),(4,4)\}$;

(**) q^2 has three mutually disjoint 01-components $T_0 \stackrel{\text{def}}{=} \{0,1\} \times D_0$, $T_1 \stackrel{\text{def}}{=} \{0,1\} \times D_1$, and $T_2 \stackrel{\text{def}}{=} \{(x_1,x_2,x_3) | q^2(x_1,x_2,x_3) \in \{0,1\}\} \setminus (T_0 \cup T_1)$;

(***) $\{0,1\}^{m+1}$ is a 01-component of q^m.

By Lemma 6,

i. the $3m$-quasigroup defined as the superposition

$$q^{m-1}(q^2(\cdot,\cdot,\cdot),\ldots,q^2(\cdot,\cdot,\cdot))$$

has 3^m components $T_{t_1} \times \ldots \times T_{t_m}$, $(t_1,\ldots,t_m) \in \{0,1,2\}^m$;

ii. the $3m+1$-quasigroup defined as the superposition

$$q^m(q^2(\cdot,\cdot,\cdot),\ldots,q^2(\cdot,\cdot,\cdot),q(\cdot,\cdot),q(\cdot,\cdot))$$

has $3^{m-1}4$ components $T_{t_1} \times \ldots \times T_{t_{m-1}} \times D_{t_m} \times D_{t_{m+1}}$, $(t_1,\ldots,t_{m+1}) \in \{0,1,2\}^{m-1} \times \{0,1\}^2$;

iii. the $3m+2$-quasigroup defined as the superposition

$$q^m(q^2(\cdot,\cdot,\cdot),\ldots,q^2(\cdot,\cdot,\cdot),q(\cdot,\cdot))$$

has $3^m 2$ components $T_{t_1} \times \ldots \times T_{t_m} \times D_{t_{m+1}}$, $(t_1,\ldots,t_{m+1}) \in \{0,1,2\}^m \times \{0,1\}$.

By Lemma 5, the theorem follows. □

Remark 4. If, in the proof, we consider the superposition $q^{n/2}(q(\cdot,\cdot),\ldots, q^2(\cdot,\cdot))$, then we obtain the bound $|Q(n,5)| \geqslant 2^{2^{n/2}}$ for even n, which is worse because $\frac{\ln 2}{2} < \frac{\ln 3}{3}$.

6.2. The case of order $\geqslant 7$

In this section, we will prove the following:

Proposition 4. *The number $|Q(n,k)|$ of n-quasigroups $\{0,1,\ldots,k-1\}^n \to \{0,1,\ldots,k-1\}$ satisfies*

$$|Q(n,k)| \geqslant 2^{\lfloor k/2 \rfloor \lfloor k/3 \rfloor^{n-1}} > e^{e^{\ln\lfloor k/3\rfloor n + \ln\lfloor k/2 \rfloor - \ln \lfloor k/3 \rfloor - 0.37}} > e^{e^{\ln\lfloor k/3 \rfloor n + 0.038}}. \quad (8)$$

Note that this bound has no sense if $k < 6$; and it is weaker than (6) if $k \vdots 2$ or $k \vdots 3$. The proof is based on the following straightforward fact:

Lemma 7. *Let $\{c,d\} \times \{e,f\}$ be an ab-component of a quasigroup g. Then*

(a) $\{a,b\}\times\{e,f\}$ *is a* cd*-component of the quasigroup* g^- *defined by* $g(x,y)=z \Leftrightarrow g^-(z,y)=x$;

(b) *if* $\{a_1,b_1\}\times\ldots\times\{a_n,b_n\}$ *is a* ef*-component of an* n*-quasigroup* q*, then* $\{c,d\}\times\{a_1,b_1\}\times\ldots\times\{a_n,b_n\}$ *is an* ab*-component of the* $(n+1)$*-quasigroup defined as the superposition* $g(\cdot,q(\cdot,\ldots,\cdot))$.

Proof of Proposition 4. Taking into account Corollary 2, it is enough to consider only the cases of odd $k\not\equiv 0 \bmod 3$. Moreover, we can assume that $k>6$ (otherwise the statement is trivial).

Define the 2-quasigroup q as

$$\begin{aligned} q(2j,i) &\stackrel{\text{def}}{=} i+3j \bmod k;\\ q(2j+1,i) &\stackrel{\text{def}}{=} \pi(i)+3j \bmod k;\\ q(2\lfloor k/3\rfloor+j,i) &\stackrel{\text{def}}{=} \tau(i)+3j \bmod k;\ \ j=0,\ldots,\lfloor k/3\rfloor-1,\ \ i=0,\ldots,k-1 \end{aligned}$$

where π, τ, and the remaining values of q are defined by the following value table (the fourth row is used only for the case $k\equiv 2 \bmod 3$):

i	0	1	2	3	4	…	$k{-}5$	$k{-}4$	$k{-}3$	$k{-}2$	$k{-}1$
$\pi(i)$	1	0	3	2	5	…	$k{-}4$	$k{-}5$	$k{-}2$	$k{-}1$	$k{-}3$
$\tau(i)$	$k{-}1$	2	1	4	3	…		$k{-}3$	$k{-}4$	0	$k{-}2$
$q(k{-}2,i)$	$k{-}3$	$k{-}2$	$k{-}1$	0	1	…		$k{-}7$	$k{-}6$	$k{-}4$	$k{-}5$
$q(k{-}1,i)$	$k{-}2$	$k{-}1$	0	1	2	…		$k{-}6$	$k{-}5$	$k{-}3$	$k{-}4$

In what follows, the tables illustrate the cases $k=7$ and $k=11$.

$k=7$:

0	1	2	3	4	5	6
1	0	3	2	5	6	4
3	4	5	6	0	1	2
4	3	6	5	1	2	0
6	2	1	4	3	0	5
2	5	4	0	6	3	1
5	6	0	1	2	4	3

$k=11$:

0	1	2	3	4	5	6	7	8	9	10
1	0	3	2	5	4	7	6	9	10	8
3	4	5	6	7	8	9	10	0	1	2
4	3	6	5	8	7	10	9	1	2	0
6	7	8	9	10	0	1	2	3	4	5
7	6	9	8	0	10	2	1	4	5	3

For each $j=0,\ldots,\lfloor k/3\rfloor-1$ and $i=0,\ldots,\lfloor k/2\rfloor-2$ the set $\{2j,2j+1\}\times\{2i,2i+1\}$ is a $(2i+3j \bmod k)(2i+3j+1 \bmod k)$-component of such q. By Lemma 7(a), for the same pairs i,j the set $\{2i+3j \bmod k, 2i+3j+1 \bmod k\}\times\{2i,2i+1\}$ is a $(2j)(2j+1)$-component of $g\stackrel{\text{def}}{=}q^-$; moreover, we can observe that for each j there is one more "non-square" $(2j)(2j+1)$-component of g which is disjoint with all considered "square" components, see the following examples (we omit the analytic description; indeed, we can ignore this component if we do not care about the constant in the bound $e^{e^{\ln\lfloor k/3\rfloor n+const}}$).

$k=7$:

0	1	6	5	2	4	3
1	0	4	6	3	2	5
5	4	0	1	6	3	2
2	3	1	0	4	5	6
3	2	5	4	0	6	1
6	5	2	3	1	0	4
4	6	3	2	5	1	0

$k=11$:

0	1	10	9	5	4	8	7	2	6	3
1	0	6	10	9	8	4	5	3	2	7
7	6	0	1	10	9	5	4	8	3	2
2	3	1	0	6	10	9	8	4	7	5
3	2	7	6	0	1	10	9	5	4	8
8	7	2	3	1	0	6	10	9	5	4
4	5	3	2	7	6	0	1	10	8	9
5	4	8	7	2	3	1	0	6	9	10
9	8	4	5	3	2	7	6	0	10	1
10	9	5	4	8	7	2	3	1	0	6
6	10	9	8	4	5	3	2	7	1	0

By induction, using Lemma 7(b), we derive that for every $j_1,\ldots,j_{n-1}\in\{0,\ldots,\lfloor k/3\rfloor-1\}$ and $i\in\{0,\ldots,\lfloor k/2\rfloor-2\}$ the set

$$\begin{array}{l}\{\quad 2j_2+3j_1 \bmod k, \qquad 2j_2+3j_1+1 \bmod k\}\times \\ \qquad\qquad\qquad \ldots \\ \{2j_{n-1}+3j_{n-2} \bmod k,\ 2j_{n-1}+3j_{n-2}+1 \bmod k\}\times \\ \{\quad 2i+3j_{n-1} \bmod k, \qquad 2i+3j_{n-1}+1 \bmod k\}\times\{2i,2i+1\}\end{array}$$

is a $(2j_1)(2j_1+1)$-component of the n-quasigroup g^{n-1}. Also, for every such $j_1,\ldots,j_{n-1}$ there is one more $(2j_1)(2j_1+1)$-component of g^{n-1}, which is generated by the "non-square" $(2j_{n-1})(2j_{n-1}+1)$-component of g. In summary, g^{n-1} has at least $\lfloor k/3\rfloor^{n-1}\lfloor k/2\rfloor$ pairwise disjoint switching components. By Lemma 5, the theorem is proved. □

Summarizing Corollary 2, Propositions 3 and 4, we get the following theorem.

Theorem 3. *Let a finite set Σ of size $k>3$ be fixed. The number $|Q(n,k)|$ of n-quasigroups $\Sigma^n\to\Sigma$ satisfies the following*:

(a) *If k is even, then $|Q(n,k)|\geqslant 2^{(k/2)^n}$.*

(b) *If k is divided by 3, then $|Q(n,k)|\geqslant 2^{n(k/3)^n}$.*

(c) *If $k=5$, then $|Q(n,k)|\geqslant 2^{3^{n/3-c}}$ where $c<0.072$ depends on* $n \bmod 3$.

(d) *In all other cases, $|Q(n,k)|\geqslant 2^{1.5\lfloor k/3\rfloor^n}$.*

References

[1] **M. A. Akivis, V. V. Goldberg**: *Solution of Belousov's problem*, Discuss. Math., Gen. Algebra Appl. **21** (2001), no. 1, 93 – 103.

[2] **V. D. Belousov**: *n-Ary Quasigroups*, (Russian), Shtiintsa, Kishinev, 1972.

[3] **V. D. Belousov, M. D. Sandik**: *n-Ary quasi-groups and loops*, Sib. Math. J. **7** (1966), 24 – 42 (translated from Sib. Mat. Zh. **7** (1966), 31 – 54).

[4] **V. V. Borisenko**: *Irreducible* n*-quasigroups on finite sets of composite order*, (Russian), Mat. Issled. **51** (1979), 38 – 42.

[5] **B. R. Frenkin**: *Reducibility and uniform reducibility in certain classes of* n*-groupoids, II*, (Russian), Mat. Issled., **7:1(23)** (1972), 150 – 162.

[6] **M. M. Glukhov**: *Varieties of* (i, j)*-reducible* n*-quasigroups*, (Russian), Mat. Issled., **39**, Shtiintsa, Kishinev, 1976, 67 – 72.

[7] **V. V. Goldberg**: *The invariant characterization of certain closure conditions in ternary quasigroups*, Sib. Math. J. **16** (1975), 23 – 34 (translated from Sib. Mat. Zh. **16** (1975), 29 – 43).

[8] **V. V. Goldberg**: *Reducible* $(n+1)$*-webs, group* $(n+1)$*-webs and* $(2n+2)$*-hedral* $(n+1)$*-webs of multidimensional surfaces*, Sib. Math. J. **17** (1976), 34 – 44 (translated from Sib. Mat. Zh. **17** (1976), 44 – 57).

[9] **D. S. Krotov**: *On reducibility of* n*-ary quasigroups*, Discrete Math., in press., 2007. DOI: 10.1016/j.disc.2007.08.099

[10] **D. S. Krotov**: *On irreducible* n*-ary quasigroups with reducible retracts*, Eur. J. Comb. **29** (2008), 507 – 513.

[11] **D. S. Krotov, V. N. Potapov**: *On the reconstruction of* n*-quasigroups of order* 4 *and the upper bounds on their number*, Proc. the Conference Devoted to the 90th Anniversary of Alexei A. Lyapunov, Novosibirsk, Russia, Oct. 2001, 323 – 327. Available at http://www.sbras.ru/ws/Lyap2001/2363

[12] **D. S. Krotov, V. N. Potapov**: *On reducibility of* n*-ary quasigroups, II*, Available at http://arxiv.org/abs/0801.0055

[13] **C. F. Laywine, G. L. Mullen**: *Discrete Mathematics Using Latin Squares*, Wiley, New York, 1998.

[14] **B. D. McKay, I. M. Wanless**: *A census of small Latin hypercubes*, SIAM J. Discrete Math., **22** (2008), 719 – 736.

[15] **V. N. Potapov, D. S. Krotov**: *Asymptotics for the number of* n*-quasigroups of order* 4, Sib. Math. J. **47** (2006), 720 – 731 (translated from Sib. Mat. Zh. 47 (2006), 873 – 887).

[16] **H. J. Ryser**: *A combinatorial theorem with an application to latin rectangles*, Proc. Am. Math. Soc. **2** (1951), 550 – 552.

Received September 23, 2007

Sobolev Institute of Mathematics
pr-t Ak. Koptyuga 4
Novosibirsk 630090
Russia
e-mail: {krotov;vpotapov}@math.nsc.ru; superpos@gorodok.net