Discrete Math. Appl., Vol. 21, No. 5–6, pp. 575–585 (2011) DOI 10.1515/DMA.2011.035

On the number of n-ary quasigroups of finite order

V. N. POTAPOV and D. S. KROTOV

Abstract — Let $Q(n,k)$ be the number of n-ary quasigroups of order k. We derive a recurrent formula for $Q(n,4)$. We prove that for all $n \geq 2$ and $k \geq 5$ the following inequalities hold:

$$\left(\frac{k-3}{2}\right)^{n/2}\left(\frac{k-1}{2}\right)^{n/2} < \log_2 Q(n,k) \leq c_k(k-2)^n,$$

where c_k does not depend on n. So, the upper asymptotic bound for $Q(n,k)$ is improved for any $k \geq 5$ and the lower bound is improved for odd $k \geq 7$.

This research was partially supported by the Federal Target Program 'Scientific and Pedagogical Personnel of Innovative Russia' for 2009–2013, Contract 02.740.11.0429, and the Russian Foundation for Basic Research, grants 08–01–00671, 08–01–00673, 10–01–00616.

1. INTRODUCTION

An algebraic system in a set Σ of cardinality $|\Sigma| = k$ and an n-ary operation $f\colon \Sigma^n \to \Sigma$ is called an n-ary quasigroup of order k if the unary operation obtained by fixing any $n-1$ arguments of f by any values from Σ is always bijective. The corresponding function f is often also called an n-ary quasigroup (the value table of such function is known as a Latin hypercube and as a Latin square for $n=2$).

Let us fix the set $\Sigma = \{0,1,\ldots,k-1\}$. Denote by $Q(n,k)$ the number of different n-ary quasigroups of order k (for fixed Σ). Sometimes, by the number of quasigroups we mean the number of mutually nonisomorphic quasigroups. It is known that for every n there exist only two n-ary quasigroups of order 2. There are exactly $Q(n,3) = 3\cdot 2^n$ different n-ary quasigroups of order 3, which form one equivalence class. In [9] it is proved that

$$Q(n,4) = 3^{n+1}2^{2^n+1}(1+o(1))$$

Originally published in *Diskretnaya Matematika* (2011) **23**, No. 4 (in Russian).
Received December 2, 2009.

as $n \to \infty$. In Section 4 we suggest a recurrent way to calculate the numbers $Q(n,4)$ and give the first 8 values. Before, only five values of $Q(n,4)$ were known; furthermore, the numbers $Q(n,5)$ and $Q(n,6)$ are known for $n \le 5$ and $n \le 3$ respectively (see [7]), and the number $Q(2,k)$ for $k \le 11$ (see [6] and the references there).

The asymptotics of the number and even of the logarithm of the number (and even of the logarithm of the logarithm of the number) of n-ary quasigroups of orders more than 4 is unknown. In [5], the following lower bounds are derived:

$$\begin{aligned} Q(n,5) &\ge 2^{3^{n/3-c}}, && c < 0.072;\\ Q(n,k) &\ge 2^{(k/2)^n}, && k \text{ is even};\\ Q(n,k) &\ge 2^{n(k/3)^n}, && k \equiv 0 \bmod 3;\\ Q(n,k) &\ge 2^{1.5\lfloor k/3\rfloor^n}, && k \text{ is arbitrary}. \end{aligned}$$

The following upper bound was found in [8]:

$$Q(n,k) \le 3^{(k-2)^n} 2^{n(k-2)^{n-1}}.$$

In this paper we improve the upper bound (Section 2) for the number of n-ary quasigroups of finite order and the lower bound (Section 3) for the number of n-ary quasigroups of odd order:

$$\left(\frac{k-3}{2}\right)^{n/2} \left(\frac{k-1}{2}\right)^{n/2} < \log_2 Q(n,k) \le c_k (k-2)^n,$$

where c_k does not depend on n, and give an explicit expression for it:

$$c_k = \frac{\log_2 k!}{k-2} + \frac{k}{k-4}.$$

2. AN UPPER BOUND

We will say that a set $M \subseteq \Sigma^n$ satisfies Property (A) if and only if for every element $\bar{x} \in M$ and every position $i = 1,\dots,n$ there is another element $\bar{y} \in M$ differing from $\bar{x}$ only in the ith position. By induction, it is easy to get the following assertion.

Proposition 1. *Any nonempty subset $C \subseteq \Sigma^n$ that satisfies Property* (A) *has the cardinality at least 2^n.*

A function $g\colon \Omega \to \Sigma$, where $\Omega \subset \Sigma^n$, is called a partial n-ary quasigroup of order $|\Sigma|$ if $g(\bar{x}) \ne g(\bar{y})$ for any two tuples $\bar{x}, \bar{y} \in \Omega$ differing in exactly one position. We will say that an n-ary quasigroup $f\colon \Sigma^n \to \Sigma$ is an extension of a partial n-ary quasigroup $g\colon \Omega \to \Sigma$ where $\Omega \subset \Sigma^n$ if $f|_\Omega \equiv g$.

Lemma 1. *Let $|\Sigma| = k$, $B = \Sigma \setminus \{a,b\}$, $k \ge 3$, $a,b \in \Sigma$. Then a partial n-ary quasigroup $g\colon \Sigma^{n-1} \times B \to \Sigma$ has at most $2^{(k/2)^{n-1}}$ different extensions.*

Proof. Denote by P the set of unordered pairs of elements of Σ. Consider a partial n-ary quasigroup $g\colon \Sigma^{n-1} \times B \to \Sigma$. Define the function $G\colon \Sigma^{n-1} \to P$ by the equality

$$G(\bar{x}) = \Sigma \setminus \{g(\bar{x}c)\colon c \in \Sigma \setminus \{a,b\}\}.$$

Define the graph $\Gamma = \langle \Sigma^{n-1}, E\rangle$, where two vertices $\bar{x}$ and $\bar{y}$ are adjacent if and only if the tuples $\bar{x}$ and $\bar{y}$ differ in exactly one position and $G(\bar{x}) \cap G(\bar{y}) \neq \varnothing$. It is easy to see that the connected components of Γ satisfy Property (A).

Let n-ary quasigroups f_1 and f_2 be extensions of g. It is not difficult to see that $\{f_1(\bar{x}a), f_1(\bar{x}b)\} = G(\bar{x})$ for every $\bar{x} \in \Sigma^{n-1}$; moreover, if $f_1(\bar{x}a) = f_2(\bar{x}a)$, then f_1 and f_2 coincide on the whole connected component of Γ containing $\bar{x} \in \Sigma^{n-1}$. So, to define an extension of g uniquely, it is sufficient to choose one of the two possible values for every connected component of Γ. It follows from Proposition 1 that every connected component has cardinality at least 2^{n-1}. Then the number of connected components of Γ does not exceed $(k/2)^{n-1}$. Hence g has at most $2^{(k/2)^{n-1}}$ extensions.

Theorem 1. *If $k \geq 5$ and $n \geq 2$, then*

$$Q(n,k) \leq 2^{c_k (k-2)^n},$$

where

$$c_k = \frac{\log_2 k!}{k-2} + \frac{k}{k-4}.$$

Proof. The number of partial n-ary quasigroups $g\colon \Sigma^{n-1} \times B \to \Sigma$, where $|\Sigma| = k$, $B = \Sigma \setminus \{a,b\}$, does not exceed $Q(n,k)^{k-2}$. From Lemma 1 we obtain

$$Q(n+1,k) \leq Q(n,k)^{k-2} 2^{(k/2)^n}. \tag{1}$$

Denote

$$\alpha_n = \frac{\log_2 Q(n,k)}{(k-2)^n}.$$

Then (1) implies

$$\alpha_{n+1} \leq \alpha_n + \left(\frac{k}{2(k-2)}\right)^n.$$

Since

$$\alpha_1 = \frac{\log_2 k!}{k-2}, \qquad \sum_{n=1}^{\infty} \left(\frac{k}{2(k-2)}\right)^n = \frac{k}{k-4},$$

we obtain

$$\alpha_n \leq \frac{\log_2 k!}{k-2} + \frac{k}{k-4}.$$

3. A LOWER BOUND

Let a and b be two different elements of Σ. By the $\{a, b\}$-component of an n-ary quasigroup f we will mean the set $S \subset \Sigma^n$ such that

(1) $f(S) = \{a, b\}$ and

(2) the function

$$g(\bar{x}) = \begin{cases} f(\bar{x}) & \text{whenever } \bar{x} \notin S, \\ b & \text{whenever } \bar{x} \in S \text{ and } f(\bar{x}) = a, \\ a & \text{whenever } \bar{x} \in S \text{ and } f(\bar{x}) = b \end{cases}$$

is also an n-ary quasigroup.

In this case we will say that g is obtained from f by switching the component S. We note that in the definition of the $\{a, b\}$-component condition 2 can be replaced by Property (A) from the previous section. It is obvious that switching disjoint components can be performed independently.

Proposition 2. *Let S and S' be disjoint $\{a, b\}$- and $\{c, d\}$- (respectively) components of an n-ary quasigroup f. Let an n-ary quasigroup g be obtained from f by switching S. Then S' is a $\{c, d\}$-component of g, too.*

The following proposition can be easily derived from the definition of an $\{a, b\}$-component; a similar assertion can be found in [5].

Proposition 3. *Let $C = \{c_1, d_1\} \times \{c_2, d_2\}$ be an $\{a, b\}$-component of a 2-ary quasigroup g. Let C_i be a $\{c_i, d_i\}$-component of an n_i-ary quasigroup q_i, $i = 1, 2$. Then the set $C_1 \times C_2$ is an $\{a, b\}$-component of the $(n_1 + n_2)$-ary quasigroup f, where $f(\bar{x}_1, \bar{x}_2) \equiv g(q_1(\bar{x}_1), q_2(\bar{x}_2))$.*

A 2-ary quasigroup $\varphi: \Sigma \to \Sigma$ is called idempotent if $\varphi(x, x) = x$ for every $x \in \Sigma$. The following assertion is known (see, e.g., [1]).

Proposition 4. *For every $m \geq 3$ there exists an idempotent 2-ary quasigroup of order m.*

The following assertion presents a construction of 2-ary quasigroups which will be used to find a lower bound for the number of n-ary quasigroups of odd order.

Proposition 5. *For any $m \geq 3$ there exists a 2-ary quasigroup ψ of order $2m + 1$ that has m $\{2i, 2i + 1\}$-components for every $i \in \{0, \dots, m - 1\}$; moreover, all except one $\{2i, 2i + 1\}$-components are of the form $\{2j, 2j + 1\} \times \{2l, 2l + 1\}$.*

Proof. By Proposition 4, there exists an idempotent 2-ary quasigroup φ_m of order m. For each $a, b \in \{0, \dots, m-1\}$, $a \neq b$, and $\delta, \sigma \in \{0, 1\}$ we define

$$\begin{aligned} \psi(2a+\delta, 2b+\sigma) &= 2\varphi_m(a,b) + (\delta + \sigma \bmod 2); \\ \psi(2a+\delta, 2a+\delta) &= 2a+1-\delta; \\ \psi(2a+\delta, 2a+1-\delta) &= k-1; \\ \psi(k-1, 2a+\delta) &= \psi(2a+\delta, k-1) = 2a+\delta; \\ \psi(k-1, k-1) &= k-1. \end{aligned}$$

It is obvious that ψ is a 2-ary quasigroup which satisfies the desired properties.

The following is an example of the value tables of a 2-ary quasigroup φ_4 and the corresponding ψ:

φ_4:

0	2	3	1
3	1	0	2
1	3	2	0
2	0	1	3

ψ:

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

From Proposition 1 it is easy to conclude that the odd-order 2-ary quasigroup constructed in Proposition 5 has the maximum number of mutually disjoint components among all 2-ary quasigroups of the same order.

Theorem 2. *If k is an odd integer, $k \geq 5$, and $n \geq 2$, then*

$$Q(n,k) \geq 2^{((k-3)/2)^{\lfloor (n-1)/2 \rfloor}((k-1)/2)^{\lceil (n+1)/2 \rceil}} > 2^{((k-3)/2)^{n/2}((k-1)/2)^{n/2}}.$$

Proof. Let ψ be the 2-ary quasigroup of order k constructed in Proposition 5. Define the n-ary quasigroup Ψ^n by the following recurrent equalities:

$$\begin{aligned} \Psi^2 &\equiv \psi; \\ \Psi^{2m+1}(\bar{x}, y) &= \psi(\Psi^{2m}(\bar{x}), y); \\ \Psi^{2m+2}(\bar{x}, y, z) &= \psi(\Psi^{2m}(\bar{x}), \psi(y, z)). \end{aligned}$$

We denote by α_n the number of $\{2i, 2i+1\}$-components of Ψ^n, where $i \in \{0, \dots, (k-3)/2\}$. From Propositions 3 and 5 we obtain the relations

$$\begin{aligned} \alpha_2 &= \frac{k-1}{2}, \\ \alpha_{2m+1} &\geq \alpha_{2m} \frac{k-3}{2}, \\ \alpha_{2m+2} &\geq \alpha_{2m} \frac{k-3}{2} \frac{k-1}{2}. \end{aligned}$$

Then

$$\alpha_{2m} \geq \left(\frac{k-3}{2}\right)^{m-1} \left(\frac{k-1}{2}\right)^{m}$$

and

$$\alpha_{2m+1} \geq \left(\frac{k-3}{2}\right)^{m} \left(\frac{k-1}{2}\right)^{m}.$$

Since $\{2i, 2i+1\}$-components with different i are disjoint, the number of disjoint components is at least $\alpha_n(k-1)/2$. From Proposition 2 we deduce that we can get the desired number of different n-ary quasigroups of order k by switching disjoint components in Ψ^n.

4. THE NUMBER OF DIFFERENT *n*-ARY QUASIGROUPS OF ORDER 4

Let $[n] = \{1, \ldots, n\}$. An n-ary quasigroup f is called an n-ary loop if there exists an element $e \in \Sigma$, which is called an identity, such that for all $i \in [n]$ and $a \in \Sigma$ it is true that $f(e \cdots e\underset{i}{a}e \cdots e) = a$. In what follows we always assume that 0 is an identity of an n-ary loop (in general, an n-ary loop can have more than one identities provided $n \geq 3$). We emphasise that this agreement is essential in the treatment of the concept of the number of n-ary loops. In particular, the following simple and well-known fact is true.

Proposition 6. *Let $Q'(n,k)$ be the number of n-ary loops of order k. Then*

$$Q(n,k) = k((k-1)!)^n Q'(n,k).$$

An n-ary quasigroup f is called permutably reducible (we will omit the word 'permutably') if there exist an integer m, $2 \leq m < n$, an $(n-m+1)$-ary quasigroup h, an m-ary quasigroup g, and a permutation $\sigma\colon [n] \to [n]$ such that

$$f(x_1, \ldots, x_n) \equiv h(g(x_{\sigma(1)}, \ldots, x_{\sigma(m)}), x_{\sigma(m+1)}, \ldots, x_{\sigma(n)}).$$

In this section, we will assume that $\Sigma = \{0, 1, 2, 3\}$, i.e., we will consider only the n-ary quasigroups of order 4. It is known (see, e.g., [1]) that there are exactly four binary loops of order 4 (one is isomorphic to the group $Z_2 \times Z_2$ and three, to the group Z_4).

The assertion below immediately follows from the theorem in [3].

Lemma 2. *Every reducible n-ary loop f of order* 4 *admits exactly one of the following two representations:*

$$f(\bar{x}) = q_0(q_1(\tilde{x}_1), \ldots, q_m(\tilde{x}_m)), \tag{2}$$

where q_j are n_j-ary loops, $\tilde{x}_j$ are tuples of variables x_i, $i \in I_j$, where $\{I_j\}$ is a partition of $[n]$, $j = 1, \dots, m$, q_0 is an irreducible m-ary loop, $m \geq 3$; moreover, the partition $\{I_j\}$ in this representation is unique for every f; and

$$f(\bar{x}) = q_1(\tilde{x}_1) * \cdots * q_k(\tilde{x}_k), \tag{3}$$

where $*$ is a binary operation in one of the 4 loops, q_j, $j = 1, \dots, k$, are n_j-ary loops which are not representable in the form $q_j(\tilde{x}_j) = q'(\tilde{x}'_j) * q''(\tilde{x}''_j)$, $\tilde{x}_j$ are tuples of variables x_i, $i \in I_j$, where $\{I_j\}$ is a partition of $[n]$; Moreover, the partition $\{I_j\}$ in this representation is unique for every f.

By the root operation of an n-ary quasigroup f we will mean the m-ary quasigroup q_0 if (2) holds, and the binary operation $*$ if (3) holds.

Simple combinatorial calculation yields the following formula for the number $F_{\bar{j},\bar{k}}$ of different partitions of $[n]$ into k subsets from which exactly k_i subsets have cardinality j_i, $1 \leq i \leq t$, $0 < j_1 < \cdots < j_t$:

$$F_{\bar{j},\bar{k}} = \frac{n!}{(j_1!)^{k_1} \cdots (j_t!)^{k_t}} \frac{1}{k_1! \cdots k_t!}, \tag{4}$$

where $k_1 + k_2 + \cdots + k_t = k$, $k_1 j_1 + k_2 j_2 + \cdots + k_t j_t = n$.

Let $f \colon \Sigma^n \to \Sigma$ be an n-ary quasigroup; define the set

$$S_{a,b}(f) \triangleq \cup\{\bar{x} \in \Sigma^n \colon f(\bar{x}) \in \{a, b\}\}.$$

An n-ary loop f will be called a-semilinear, where $a \in \{1, 2, 3\}$, if the characteristic function $\chi_{S_{0,a}(f)}$ of the set $S = S_{0,a}(f)$ is of the form

$$\chi_{S_{0,a}(f)}(x_1, \dots, x_n) \equiv \sum_{i=1}^{n} \chi_{\{0,a\}}(x_i) \bmod 2. \tag{5}$$

An n-ary loop f is called linear if it is a-semilinear and b-semilinear for some different a and b from $\{1, 2, 3\}$. It is not difficult to see that the assertion below is true.

Proposition 7. *One of the four binary loops of order 4 is linear (the one that is isomorphic to $Z_2 \times Z_2$); the other three are 1-, 2-, and 3- semilinear respectively.*

The assertion below is well known (see [9]).

Proposition 8. *A linear n-ary loop is unique and is 1-, 2-, and 3-semilinear.*

It is not difficult to see (see also [9]) that the following assertion is true.

Proposition 9. *Let f be a reducible a-semilinear n-ary loop; then f can be represented either as composition (2) or (3) of a-semilinear loops.*

Let us denote by l_n^a the number of the a-semilinear n-ary loops and by l_n the number of the semilinear n-ary loops.

As proved in [9], the number of the n-ary loops asymptotically coincides with l_n, which can be easily calculated.

Lemma 3 ([9])**.** *The relations* $l_n = 3 \cdot 2^{2^n-n-1} - 2$*,* $l_n^a = 2^{2^n-n-1}$*,* $a \in \{1,2,3\}$*, are true.*

In [4], the set of n-ary quasigroups of order 4 was characterised in the terms defined above; namely, the following was proved.

Theorem 3. *Every n-ary loop of order* 4 *is reducible or semilinear.*

This fact gives a base for deriving a recurrent formula for the number of n-ary loops (and quasigroups) of order 4.

We will use the following notation:

v_n is the number of n-ary loops (of order 4);

r_n^* is the number of reducible n-ary loops with the binary root operation $*$;

r_n^0 is the number of reducible n-ary loops with the root operation of arity at least 3;

r_n^{a*} is the number of reducible a-semilinear n-ary loops with the a-semilinear binary root operation $*$;

r_n^{a0} is the number of reducible a-semilinear n-ary loops with the root operation of arity at least 3;

p_n^a is the number of irreducible a-semilinear n-ary loops;

p_n is the number of irreducible n-ary loops.

From Lemma 2 and Proposition 9, the relations follow:

$$r_n^{a*} = \sum_{i=2}^{n} \sum_{\bar{j},\bar{k}} F_{\bar{j},\bar{k}} (l_{j_1}^a - r_{j_1}^{a*})^{k_1} \cdots (l_{j_t}^a - r_{j_t}^{a*})^{k_t},$$

$$r_n^{*} = \sum_{i=2}^{n} \sum_{\bar{j},\bar{k}} F_{\bar{j},\bar{k}} (v_{j_1} - r_{j_1}^{*})^{k_1} \cdots (v_{j_t} - r_{j_t}^{*})^{k_t},$$

$$r_n^{a0} = \sum_{i=3}^{n-1} p_i^a \sum_{\bar{j},\bar{k}} F_{\bar{j},\bar{k}} (l_{j_1}^a)^{k_1} \cdots (l_{j_t}^a)^{k_t},$$

$$r_n^{0} = \sum_{i=3}^{n-1} p_i \sum_{\bar{j},\bar{k}} F_{\bar{j},\bar{k}} (v_{j_1})^{k_1} \cdots (v_{j_t})^{k_t},$$

where the second sum is over the tuples $\bar{k} = (k_1, \dots, k_t)$ and $\bar{j} = (j_1, \dots, j_t)$ of positive integers such that $k_1 + \dots + k_t = i$, $k_1 j_1 + k_2 j_2 + \dots + k_t j_t = n$ and $j_1 < \dots < j_t$. From Theorem 3 and Proposition 8 we obtain

$$v_n = p_n + r_n^0 + 4r_n^*, \quad p_n^a = l_n^a - r_n^{a0} - 2r_n^{a*}, \quad p_n = 3p_n^a.$$

From Lemma 3, we see that

$$l_n^a = 2^{2^n - n - 1}, \qquad a \in \{1, 2, 3\}.$$

Proposition 7 yields the initial values

$$r_2^{a*} = 2, \quad r_2^* = 4, \quad r_2^{a0} = r_2^0 = 0.$$

We see that the equalities above and Proposition 6 provide us with a recurrent way of calculation of the number of the n-ary quasigroups of order 4.

Finally, we present the first eight values of $Q'(n, 4)$:

1,
4,
64,
7132,
201538000,
432345572694417712,
398768398735474764292277335396327796 8,
6784692728748995825599862402852807103648670634897795104270387222297502768 32,

and of $Q(n, 4)$:

24,
576,
55296,
36972288,
6268637952000,
8068606015852301108428 8,
446518521873655454467691792646025672500019 2,
4558271384916189349044295395852008182480786230841798008741684281906576963885826048.

5. CONCLUSION

We will briefly discuss a connection of our topic with the known concept of latin trade. A partial n-ary quasigroup $t\colon \Omega \to \Sigma$, $\Omega \subset \Sigma^n$ is called a multidimensional latin trade, here for brevity simply trade, if there exists another partial n-ary quasigroup $t'\colon \Omega \to \Sigma$ such that

(1) $t(\bar{x}) \neq t'(\bar{x})$ for all $\bar{x} \in \Omega$;

(2) for any i from 1 to n, the sets $\{t(x_1, \dots, x_{i-1}, y, x_{i-1}, \dots, x_n) \mid y \in \Sigma\}$ and $\{t'(x_1, \dots, x_{i-1}, y, x_{i-1}, \dots, x_n) \mid y \in \Sigma\}$ coincide for any admissible values $x_1, \dots, x_{i-1}, x_{i-1}, \dots, x_n$.

In this case, the pair (t, t') is called a bitrade (depending on the context, bitrades are considered either as ordered or as unordered pairs); the trade t' is called a mate of t. In the case $n = 2$, bitrades (latin bitrades) are widely studied, see the survey [2].

We will say that an n-ary quasigroup f has a trade t if $t = f|_\Omega$ for some Ω. As follows from the definitions, replacing the values of f in Ω by the values of a mate t' of t results in another n-ary quasigroup. We will say that trades $t = f|_\Omega$ and $s = f|_\Theta$ are independent if their supports Ω and Θ are disjoint. The maximum number of mutually independent trades of an n-ary quasigroup f will be called its trade number $\mathrm{Trd}(f)$. Denote by $\mathrm{Trd}(n, k)$ the maximum of $\mathrm{Trd}(f)$ over all n-ary quasigroups f of order k. Since independent trades of an n-ary quasigroup can be independently replaced by mates, the number $Q(n, k)$ of different n-ary quasigroups of order k satisfies the inequality

$$Q(n, k) \geq 2^{\mathrm{Trd}(n,k)}. \tag{6}$$

It is easy to understand that the lower bound in Section 3 (as well as all bounds in [5]) is derived in this way: an $\{a, b\}$-component is the support of some trade by the definition. Since the support of a trade satisfies Property (A), Proposition 1 implies that

$$\mathrm{Trd}(n, k) \leq k^n / 2^n = 2^{(\log_2 k - 1)n};$$

moreover, for even k the equality is easily proved. For odd k, as follows from the results of Section 3, we have

$$\mathrm{Trd}(n, k) \geq 2^{c(k)n},$$

where $c(k) \to \log_2 k - 1$ as $k \to \infty$. But for fixed k, in particular, for the small values $5, 7, \dots$, the question about the asymptotics of $\mathrm{Trd}(n, k)$ remains open.

Problem 1. Find the asymptotics of the logarithm and the asymptotics of $\mathrm{Trd}(n, k)$ as $n \to \infty$ for odd $k \geq 5$.

Another question concerning the closeness of bound (6) to the real value. For the order 4, it is asymptotically sharp in logarithms. For any larger fixed order, the asymptotics of $\log \log Q(n, k)$ is unknown. It is natural to hypothesise that the asymptotics of $\log \log Q(n, k)$ and $\log \mathrm{Trd}(n, k)$ coincide.

Problem 2. Is it true that

$$\lim_{n \to \infty} \left(\frac{\log_2 \log_2 Q(n, k)}{n} \right) = \lim_{n \to \infty} \left(\frac{\log_2 \mathrm{Trd}(n, k)}{n} \right)?$$

In particular, is it true that

$$\lim_{n\to\infty}\left(\frac{\log_2\log_2 Q(n,k)}{n}\right) \le \log_2 k - 1?$$

Even the existence of these limits is not proved yet.

REFERENCES

1. V. D. Belousov, *Foundations of Quasigroup and Loop Theory*. Nauka, Moscow, 1967 (in Russian).
2. N. J. Cavenagh, The theory and application of latin bitrades: A survey. *Mathematica Slovaca* (2008) **58**, 691–718.
3. A. V. Cheremushkin, Canonical decomposition of n-ary quasigroups. *Mat. Issled.* (1988) **102**, 97–105 (in Russian).
4. D. S. Krotov and V. N. Potapov, n-ary quasigroups of order 4. *SIAM J. Discrete Math.* (2009) **23**, 561–570.
5. D. S. Krotov, V. N. Potapov, and P. V. Sokolova, On reconstructing reducible n-ary quasigroups and switching subquasigroups. *Quasigroups Relat. Syst.* (2008) **16**, 55–67.
6. B. D. McKay and I. M. Wanless, On the number of Latin squares. *Ann. Comb.* (2005) **9**, 335–344.
7. B. D. McKay and I. M. Wanless, A census of small Latin hypercubes. *SIAM J. Discrete Math.* (2008) **22**, 719–736.
8. V. N. Potapov, An upper estimation of the number of n-quasigroups of finite order. In: *Proc. XVII Intern. School-Seminar 'Synthesis and Complexity of Control Systems'*. Novosibirsk, 2008, pp. 136–137 (in Russian).
9. V. N. Potapov and D. S. Krotov, Asymptotics for the number of n-quasigroups of order 4. *Sib. Math. J.* (2006) **47**, 720–731.