Siberian Mathematical Journal, Vol. 47, *No.* 4, *pp.* 720–731, 2006
Original Russian Text Copyright © 2006 *Potapov V. N. and Krotov D. S.*

ASYMPTOTICS FOR THE NUMBER OF n-QUASIGROUPS OF ORDER 4

V. N. Potapov and D. S. Krotov UDC 519.143

Abstract: The asymptotic form of the number of n-quasigroups of order 4 is $3^{n+1}2^{2^n+1}(1+o(1))$.

Keywords: n-quasigroup, MDS codes, decomposability, reducibility

An algebraic system consisting of a set Σ of cardinality $|\Sigma| = k$ and an n-ary operation $f : \Sigma^n \to \Sigma$ uniquely invertible in each of its arguments is called an *n-quasigroup of order k*. The function f can also be referred to as an *n-quasigroup of order k* (see [1]). The value table of an n-quasigroup of order k is called a *Latin n-cube of dimension k* (in case $n = 2$, a *Latin square*). Furthermore, there is a one-to-one correspondence between the n-quasigroups and the distance 2 MDS codes of length $n + 1$.

It is not difficult to show that for each n there exist only two n-quasigroups of order 2 and $3 \cdot 2^n$ different n-quasigroups of order 3 which constitute one equivalence class. In this work we study the properties of n-quasigroups of order 4 and derive the asymptotic representation $3^{n+1}2^{2^n+1}(1 + o(1))$ for their number. The results of this research were announced in [2]. For $k > 4$, the asymptotic form of the number of n-quasigroups and even the asymptotic form of its logarithm remain unknown.

In § 1–§ 4 we give the necessary definitions and propositions concerning the quaternary distance 2 MDS codes and double-codes (§ 1), linear double-codes (§ 2), n-quasigroups of order 4 (§ 3), semilinear n-quasigroups of order 4 (§ 4). In § 5 we prove that almost all (as $n \to \infty$) n-quasigroups of order 4 are semilinear and establish asymptotically tight bounds on their number.

In addition to the main result, of special interest are Lemma 1 on a linear antilayer in a double-MDS-code and Lemma 4 on a semilinear layer in an n-quasigroup as well as Lemmas 2 and 3 on the decomposability of double-MDS-codes and n-quasigroups which were proved in [3, 4], and their Corollary 3.

§ 1. MDS Codes and Double-Codes

Let $\Sigma = \{0, 1, 2, 3\}$ and let n be a natural number. In this paper we study the subsets of Σ^n and the functions on Σ^n with some properties to be specified below. The elements of Σ^n will be called *vertices.* Denote by $[n]$ the set of natural numbers from 1 to n. Given $\bar{y} = (y_1, \dots, y_n)$, we put $\bar{y}^{(i)}\#x = (y_1, \dots, y_{i-1}, x, y_{i+1}, \dots, y_n)$.

Assume that $\bar{x} \in \Sigma^n$ and $k \in [n]$. The set $\mathscr{E}_k(\bar{x}) \triangleq \{\bar{x}^{(k)}\#a : a \in \Sigma\}$ is called a *k-edge.* Two different vertices in Σ^n are called *neighbor vertices* provided that they both belong to some k-edge, i.e., differ in only one coordinate.

Definition. A set $C \subset \Sigma^n$ is called a *distance* 2 MDS *code* (*of length* n) (henceforth simply an MDS *code*) whenever $|\mathscr{E}_k(\bar{x}) \cap C| = 1$ for all $\bar{x} \in \Sigma^n$ and $k \in [n]$. Note that $|C| = |\Sigma^n|/4 = 2^{2n-2}$.

Definition. A set $S \subset \Sigma^n$ is called a *double-code* whenever $|\mathscr{E}_k(\bar{x}) \cap S| = 2$ for all $\bar{x} \in S$ and $k \in [n]$.

Definition. A double-code $S \subset \Sigma^n$ is called a *double*-MDS-*code* whenever $|S| = |\Sigma^n|/2 = 2^{2n-1}$. In other words, a set $S \subset \Sigma^n$ is a double-MDS-code provided that $|\mathscr{E}_k(\bar{x}) \cap S| = 2$ for all $\bar{x} \in \Sigma^n$ and $k \in [n]$. Obviously, $\Sigma^n \backslash S$ also is a double-MDS-code in this case.

The first author was supported by the Russian Foundation for Basic Research (Grant 05–01–00364).

Novosibirsk. Translated from *Sibirskiĭ Matematicheskiĭ Zhurnal*, Vol. 47, No. 4, pp. 873–887, July–August, 2006. Original article submitted May 14, 2005. Revision submitted January 31, 2006.

 0037-4466/06/4704–0720

Denote by $\Gamma(S)$ the *adjacency graph* of a double-code $S \subset \Sigma^n$ with vertex set S and edge set $\{(\bar{x}, \bar{y}) : \bar{x},\, \bar{y}$ are neighbor vertices in $\Sigma^n\}$.

Definition. A nonempty double-code $S \subset \Sigma^n$ is called *prime* provided that S is a subset of a double-MDS-code $S' \subset \Sigma^n$ and the graph $\Gamma(S)$ is connected. By way of illustration, we list all up to equivalence nonempty double-codes in Σ^2 (Fig. 1).

(a) (b) (c) (d)

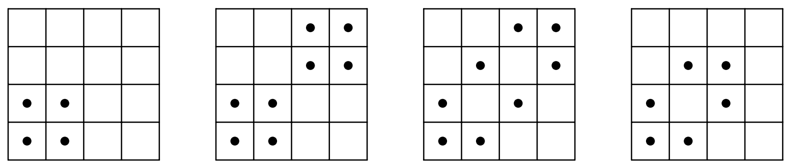

Fig. 1

The double-codes (a) and (c) are prime; (b) and (c) are double-MDS-codes.

Definition. A double-MDS-code S is *splittable* provided that $S = C_1 \cup C_2$, where C_1 and C_2 are disjoint MDS codes. Unsplittable double-MDS-codes exist in Σ^n starting from $n = 3$. A double-MDS-code S is splittable if and only if $\Gamma(S)$ is a bipartite graph.

Definition. An *isotopy* or *n-isotopy* we call an ordered collection of n permutations $\theta_i : \Sigma \to \Sigma$, $i \in [n]$. Let $\bar{\theta} = (\theta_1, \dots, \theta_n)$ be an isotopy and $S \subseteq \Sigma^n$. Put $\bar{\theta} S \triangleq \{(\theta_1 x_1, \dots, \theta_n x_n) : (x_1, \dots, x_n) \in S\}$.

Definition. Some sets $S_1 \subseteq \Sigma^n$ and $S_2 \subseteq \Sigma^n$ are called *equivalent* provided that there exist a coordinate permutation $\tau : [n] \to [n]$ and an n-isotopy $\bar{\theta}$ such that

$$\chi_{S_1}(x_1, \dots, x_n) \equiv \chi_{\bar{\theta} S_2}(x_{\tau(1)}, \dots, x_{\tau(n)}).$$

Here and in what follows χ_B denotes the characteristic function of a set B.

Obviously, if two double-codes are equivalent then they have equivalent adjacency graphs; they are both double-MDS-codes or neither is a double-MDS-code; they are both splittable or neither is splittable; and both are prime or neither is prime.

Proposition 1. *Let S be a splittable double-*MDS*-code and let γ be the number of the prime double-codes that S includes. Then the double-code S includes exactly 2^γ different* MDS *codes.*

Proof. The number of the MDS codes that S includes equals the number of the ways of choosing part of the bipartite graph $\Gamma(S)$. Since in each of the γ connected components of $\Gamma(S)$ such a part can be chosen independently, the number of the ways is 2^γ. $\square$

Definition. Let $S \subseteq \Sigma^n$, $k \in [n]$, and $y \in \Sigma$. The set

$$\mathscr{L}_{k;y} S \triangleq \{(x_1, \dots, x_{k-1}, x_k, \dots, x_{n-1}) : (x_1, \dots, x_{k-1}, y, x_k, \dots, x_{n-1}) \in S\}$$

is called the yth *layer* of S in direction k.

Proposition 2. *Let $S, S' \subseteq \Sigma^n$ be some sets, $k \in [n]$, and $\{a, b, c, d\} = \Sigma$.*

(a) *If S is a double-code (splittable double-code, double-*MDS*-code) then $\mathscr{L}_{k;a} S$ also is a double-code (splittable double-code, double-*MDS*-code) in Σ^{n-1}.*

(b) *If $k < k' \in [n]$ then $\mathscr{L}_{k;b}(\mathscr{L}_{k';a} S) = \mathscr{L}_{k'-1;a}(\mathscr{L}_{k;b} S)$.*

(c) *$\mathscr{L}_{k;a}(S \cap S') = \mathscr{L}_{k;a} S \cap \mathscr{L}_{k;a} S'$.*

(d) *If S and S' are double-codes and $\mathscr{L}_{k;a} S = \mathscr{L}_{k;a} S'$, $\mathscr{L}_{k;b} S = \mathscr{L}_{k;b} S'$, $\mathscr{L}_{k;c} S = \mathscr{L}_{k;c} S'$ then $\mathscr{L}_{k;d} S = \mathscr{L}_{k;d} S'$.*

(e) *If S is a double-*MDS*-code and $\mathscr{L}_{k;a} S = \mathscr{L}_{k;b} S$ then $\mathscr{L}_{k;c} S = \mathscr{L}_{k;d} S = \Sigma^{n-1} \backslash \mathscr{L}_{k;a} S$.*

Let us show that a double-MDS-code is completely defined by any of its nonempty subsets that are double-codes.

Proposition 3 (on unique extension of a double-code). *Let $S_1, S_2 \subset \Sigma^n$ be double-*MDS*-codes. Then*

(a) *if $S_0 \subseteq S_1 \cap S_2$ is a nonempty double-code then $S_1 = S_2$;*

(b) *if $S_0 \subseteq S_1 \backslash S_2$ is a nonempty double-code then $S_1 = \Sigma^n \backslash S_2$.*

PROOF. We will prove (a) by induction on n. For $n = 1$ the claim is trivial. Assume that (a) holds for $n = m-1$; let us show that it holds for $n = m$. By Proposition 2(a), we have: $\mathscr{L}_{1;a}S_0$ is a double-code, $\mathscr{L}_{1;a}S_1$ and $\mathscr{L}_{1;a}S_2$ are double-MDS-codes for each $a \in \Sigma$. By Proposition 2(c), $\mathscr{L}_{1;a}S_0 \subseteq \mathscr{L}_{1;a}S_1 \cap \mathscr{L}_{1;a}S_2$. Then, by the inductive assumption, $\mathscr{L}_{1;a}S_1 = \mathscr{L}_{1;a}S_2$ for all $a \in \Sigma$ such that $\mathscr{L}_{1;a}S_0$ is not empty. By the definition of a double-code, at least two of the four sets $\mathscr{L}_{1;a}S_0$, $a \in \Sigma$, are nonempty. If there are three nonempty sets then the equality $S_1 = S_2$ follows from Proposition 2(d). Assume that two sets, say $\mathscr{L}_{1;2}S_0$ and $\mathscr{L}_{1;3}S_0$, are empty. Then $\mathscr{L}_{1;0}S_0 = \mathscr{L}_{1;1}S_0$, because $|\mathscr{E}_1(\bar{x}) \cap S_0| = 2$ for all $\bar{x} \in S_0$. Hence $\mathscr{L}_{1;0}S_1 = \mathscr{L}_{1;1}S_1 = \mathscr{L}_{1;0}S_2 = \mathscr{L}_{1;1}S_2$, by the inductive assumption. Then, by Proposition 2(e), we obtain $S_1 = S_2$.

(b) Consider $S_2' \triangleq \Sigma^n \backslash S_2$. Since S_2' is a double-MDS-code and $S_0 \subseteq S_1 \cap S_2'$, it follows from (a) that $S_2' = S_1$. $\square$

§ 2. Linear Double-Codes

DEFINITION. A nonempty double-code $S \subset \Sigma^n$ is called *linear* whenever

$$\chi_S(x_1, \dots, x_n) \equiv \chi_{S_1}(x_1) \oplus \chi_{S_2}(x_2) \oplus \dots \oplus \chi_{S_n}(x_n) \tag{1}$$

where S_i ($1 \le i \le n$) are subsets of Σ and $\oplus$ is the modulo 2 addition. Obviously, S_i are double-MDS-codes in Σ. A linear double-code in Σ^2 is illustrated in Fig. 1(b).

In the following two propositions, some elementary properties of linear 2-codes are proved.

Proposition 4 (properties of the class of linear double-codes). (a) *The linear double-codes constitute an equivalence class.*

(b) *A linear double-code is a splittable double-*MDS*-code.*

(c) *The complement of a linear double-code is a linear double-code.*

(d) *A double-code S is linear if and only if there exists a prime double-code $S_0 \subset S$ equivalent to $\{0,1\}^n$.*

(e) *A linear double-code is uniquely defined by the subset of all its vertices of type $\bar{0}^{(i)}\#y$, $i \in [n]$, $y \in \Sigma$.*

(f) *The number of linear double-codes in Σ^n is $2 \cdot 3^n$.*

PROOF. The properties (a)–(c) follow from definitions.

(d) *Necessity.* By (a), we may assume without loss of generality that $\chi_S(x_1, \dots, x_n) \equiv \bigoplus_{i=1}^n \chi_{\{2,3\}}(x_i)$. In this case $S_0 \triangleq \{2,3\} \times \{0,1\}^{n-1}$ is a subset of S.

Sufficiency. Suppose that a double-code $S_0 \subset S$ is equivalent to $\{0,1\}^n$. Without loss of generality assume that $S_0 = \{2,3\} \times \{0,1\}^{n-1}$. Then S_0 is a subset of the linear double-code S' where $\chi_{S'}(x_1, \dots, x_n) \equiv \bigoplus_{i=1}^n \chi_{\{2,3\}}(x_i)$. By Proposition 3(a), we have $S = S'$.

(e) Indeed, let a double-code S be represented as in (1). Put $\chi^0 \triangleq \chi_S(\bar{0})$ and $\chi^i(y) \triangleq \chi_S(\bar{0}^{(i)}\#y)$, $i \in [n]$. We have

$$\chi_S(x_1, \dots, x_n) \equiv \chi^0 \oplus \bigoplus_{i=1}^{n} (\chi^i(x_i) \oplus \chi^0), \tag{2}$$

which can be easily checked on using (1) for χ_S.

(f) follows from (2). Indeed, we can choose χ^0 in two ways. Then each of the functions χ^i, $i \in [n]$, can be chosen in three ways, taking into account that χ^i is the characteristic function of a double-MDS-code in Σ and $\chi^i(\bar{0}) = \chi^0$. $\square$

The set $\{0,1\}^n$, as well as the graph $\Gamma(\{0,1\}^n)$, is called the *Boolean n-cube*. The next proposition follows from definitions and Proposition 2.

Proposition 5 (on heritable properties of linear double-codes). (a) *If $S \subset \Sigma^n$ is a linear double-code then $\mathscr{L}_{k;y}S$ is a linear double-code.*

(b) *Let $S \subset \Sigma^n$ be a double-code. If two layers of S by some direction are linear and coincide then S is a linear double-code.*

The main result of this section is the following lemma, presenting a partial conversion of Item (a) and a partial strengthening of Item (b) of Proposition 5. The lemma claims that the existence of a linear layer in a splittable double-MDS-code implies the existence of a layer ("antilayer") in the same direction that complements the former.

Lemma 1 (on a linear antilayer). *Let $S \subset \Sigma^n$ be a splittable double-*MDS*-code and let $L \triangleq \mathscr{L}_{k;a}S$ be a linear double-code for some $k \in [n]$ and $a \in \Sigma$. Then*

(a) *there is $b \in \Sigma$ such that $\mathscr{L}_{k;b}S = \Sigma^{n-1}\backslash L$;*

(b) *$\Sigma^n\backslash S$ is a splittable double-*MDS*-code.*

Before proving Lemma 1 we introduce the notation $\neg(\alpha_1, \alpha_2, \dots, \alpha_n) \triangleq (\alpha_1 \oplus 1, \alpha_2 \oplus 1, \dots, \alpha_n \oplus 1)$ where $\alpha_i \in \{0,1\}$ and prove two auxiliary propositions.

Proposition 6. *Let $\{P_1, P_2, P_3\}$ be a partition of the Boolean n-cube with $n \geq 4$ into three nonempty sets: $P_1 \cup P_2 \cup P_3 = \{0,1\}^n$. Moreover, the following holds:*

($*$) *for every $k \in [n]$ and every $b \in \{0,1\}$ at least one set (layer) of $\mathscr{L}_{k;b}P_1$, $\mathscr{L}_{k;b}P_2$, $\mathscr{L}_{k;b}P_3$ is empty.*

Then $\{P_1, P_2, P_3\} = \{\{\bar\alpha\}, \{\neg\bar\alpha\}, \{0,1\}^n\backslash\{\bar\alpha, \neg\bar\alpha\}\}$ where $\bar\alpha \in \{0,1\}^n$.

Proof. Denote by $N_i \subseteq [n]$ the set of coordinates k whose values are not fixed in P_i, i.e., $\mathscr{L}_{k;0}P_i \neq \varnothing$ and $\mathscr{L}_{k;1}P_i \neq \varnothing$. It is easy to see that N_1, N_2, and N_3 are pairwise disjoint (if, for example, $k \in N_1 \cap N_2$ then ($*$) implies $\mathscr{L}_{k;0}P_3 = \varnothing$ and $\mathscr{L}_{k;1}P_3 = \varnothing$, which contradicts the nonemptiness of P_3). So, the obvious relation $2^n = |P_1| + |P_2| + |P_3| \leq 2^{|N_1|} + 2^{|N_2|} + 2^{|N_3|}$ yields $\{N_1, N_2, N_3\} = \{\varnothing, \varnothing, [n]\}$ and $\{P_1, P_2, P_3\} = \{\{\bar\alpha\}, \{\bar\beta\}, \{0,1\}^n\backslash\{\bar\alpha, \bar\beta\}\}$. The hypothesis ($*$) implies that $\bar\beta = \neg\bar\alpha$. $\square$

Proposition 7. *Let S be a double-*MDS*-code in Σ^n, $n \geq 3$, and $k \in [n]$. Let P_0, P_1, P_2, and P_3 be the intersections of the four layers of S in direction k with the Boolean $(n-1)$-cube, i.e., $P_i \triangleq \mathscr{L}_{k;i}S \cap \{0,1\}^{n-1}$. Assume that at least one of the following holds:*

(a) *$n = 3$, $P_i = \{0,1\}^2$ for some i, and $P_i \neq \varnothing$ for all $i \in \{0,1,2,3\}$;*

(b) *$\{P_0, P_1, P_2, P_3\} = \{\{0,1\}^{n-1}, \{\bar\alpha\}, \{\bar\beta\}, \{0,1\}^{n-1}\backslash\{\bar\alpha, \bar\beta\}\}$ where $\bar\alpha \in \{0,1\}^{n-1}$ and $\bar\beta = \neg\bar\alpha$.*

Then the double-codes S and $\Sigma^n\backslash S$ are unsplittable.

Proof. (a) There are two nonequivalent cases for the choice of P_i. It is not difficult to check (we leave this to the reader) that in each case an attempt to recover the double-MDS-code S leads to an unsplittable double-MDS-code with the unsplittable complement.

(b) Without loss of generality we may assume that $k = n$, $\bar\alpha = 0^{n-1}$, $\bar\beta = 1^{n-1}$,

$$P_0 = \{0,1\}^{n-1}, \quad P_1 = \{\bar\alpha\}, \quad P_2 = \{\bar\beta\}, \quad P_3 = \{0,1\}^{n-1}\backslash\{\bar\alpha, \bar\beta\}$$

(otherwise we can select a suitable coordinate permutation and isotopy and consider an equivalent double-code that satisfies this assumption). We will argue by induction on n. The base of induction, the case of $n = 3$, is considered in Item (a). Assume that the statement holds for $n = m - 1$. Let us show that it holds for $n = m$ as well. Consider the intersections of the layers $\mathscr{L}_{k;0}S$, $\mathscr{L}_{k;1}S$, $\mathscr{L}_{k;2}S$, $\mathscr{L}_{k;3}S$ with the set $E \triangleq \{2,3\} \times \{0,1\}^{n-2}$, which is equivalent to the Boolean $(n-1)$-cube $\{0,1\}^{n-1}$ and is a "neighbor cube" to it:

$$Q_i \triangleq \{2,3\} \times \{0,1\}^{n-2} \cap \mathscr{L}_{1;i}S.$$

Fig. 2 illustrates the situation.

($*$) We claim that the sets Q_0, Q_1, Q_2, and Q_3 are defined up to four elements. More exactly,

$$Q_0 = \varnothing, \quad Q_1 = E\backslash\{\bar\alpha'\}, \quad Q_2 = E\backslash\{\bar\beta'\}, \quad Q_3 = \{\bar\alpha'', \bar\beta''\}, \tag{3}$$

where $\bar\alpha', \bar\alpha'' \in \{(2,0,\dots,0),(3,0,\dots,0)\}$ and $\bar\beta', \bar\beta'' \in \{(2,1,\dots,1),(3,1,\dots,1)\}$. Indeed, the set $\{0,1\}^{n-1} \cup E$ can be split into the 1-edges of type $\mathscr{E}_1(\bar x)$, $\bar x \in \{0\} \times \{0,1\}^{n-2}$. Since S is a double-MDS-code; therefore, every such 1-edge contains two vertices from $P_i \cup Q_i$ for each $i \in \{0,1,2,3\}$. In particular,

- if such 1-edge contains two vertices from P_i then it does not contain vertices from Q_i;
- if it does not contain vertices from P_i then it contains two vertices from Q_i.

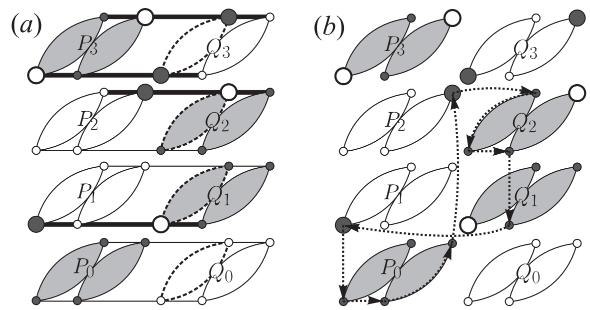

Fig. 2. An Illustration of Proposition 7.

According to (3) these two rules define all vertices of Q_i, $i = 0,1,2,3$, except for the four cases (Fig. 2(a), the bold horizontal lines):

- the 1-edge $\mathscr{E}_1(0,0,\dots,0)$ contains exactly one vertex $(0,0,\dots,0)$ from P_1,
- the 1-edge $\mathscr{E}_1(0,0,\dots,0)$ contains exactly one vertex $(1,0,\dots,0)$ from P_3,
- the 1-edge $\mathscr{E}_1(0,1,\dots,1)$ contains exactly one vertex $(1,1,\dots,1)$ from P_2,
- the 1-edge $\mathscr{E}_1(0,1,\dots,1)$ contains exactly one vertex $(0,1,\dots,1)$ from P_3.

In each of the cases we have a choice of a vertex of Q_i for the respective i. This choice corresponds to the choice of $\alpha', \alpha'', \beta', \beta''$. The claim $(*)$ is proved.

Since S is a double-MDS-code, every vertex from E belongs to exactly two sets Q_i. So, it follows directly from (3) that $\bar\alpha' = \bar\alpha''$ and $\bar\beta' = \bar\beta''$. Without loss of generality we may assume that $\bar\alpha' = \bar\alpha'' = (2,0,\dots,0)$. Thus, it suffices to consider the two cases: $\bar\beta' = \bar\beta'' = (2,1,\dots,1)$ (Fig. 2(a)) and $\bar\beta' = \bar\beta'' = (3,1,\dots,1)$ (Fig. 2(b)).

1. Case $\bar\beta' = \bar\beta'' = (2,1,\dots,1)$ (Fig. 2(a)). In this case we can use the inductive assumption. Indeed, consider the set $\Sigma^{n-1} \backslash \mathscr{L}_{1;2}S$. Its layers in the last direction intersected with the Boolean $(n-2)$-cube coincide with $\{0,1\}^{n-2}$, $\{(0,\dots,0)\}$, $\{(1,\dots,1)\}$, and $\{0,1\}^{n-1} \backslash \{(0,\dots,0),(1,\dots,1)\}$ (see Fig. 2(a), the dotted lines). By the inductive assumption, the double-codes $\Sigma^{n-1} \backslash \mathscr{L}_{1;2}S$ and $\mathscr{L}_{1;2}S$ are unsplittable. Hence, $\Sigma^n \backslash S$ and S are unsplittable.

2. Case $\bar\beta' = \bar\beta'' = (3,1,\dots,1)$ (Fig. 2(b)). In this case we can find a cyclic path of odd length $2n+3$ in $\Gamma(S)$:

$$(0000\dots00,\ \underbrace{1000\dots00,\ 1100\dots00,\ 1110\dots00,\ \cdots,\ 1111\dots10}_{n-1},\ 1111\dots12,$$
$$\underbrace{2111\dots12,\ 2011\dots12,\ 2001\dots12,\ \cdots,\ 2000\dots02}_{n-1},\ 3000\dots02,\ 3000\dots01,\ 0000\dots01)$$

(Fig. 2(b), the dotted lines); this implies that the graph is not bipartite and the double-code S is unsplittable by definition. Similarly, the odd cyclic path

$$(2000\dots00,\ \underbrace{3000\dots00,\ 3100\dots00,\ 3110\dots00,\ \cdots,\ 3111\dots10}_{n-1},\ 3111\dots12,$$
$$\underbrace{0111\dots12,\ 0011\dots12,\ 0001\dots12,\ \cdots,\ 0000\dots02}_{n-1},\ 1000\dots02,\ 1000\dots01,\ 2000\dots01)$$

in $\Gamma(\Sigma^n \backslash S)$ shows that the double-code $\Sigma^n \backslash S$ is unsplittable. $\square$

Proof of Lemma 1. (a) We prove the claim by induction. The base of induction, the case of $n = 2$, is trivial. Assume that the lemma holds for $n = m - 1$. Let us show that the claim is true for $n = m \geq 3$.

By Proposition 4(d) the splittability and linearity of a double-code are preserved under isotopy and coordinate permutation, without loss of generality we may assume that $k = n$, $a = 0$, and the linear double-code L includes $\{0,1\}^{n-1}$. Let P_0, P_1, P_2, and P_3 be defined as in Proposition 7; i.e., $P_i \triangleq \{0,1\}^{n-1} \cap \mathscr{L}_{n;i}S$.

It is enough to show that at least one of the sets P_1, P_2, and P_3 is empty. Then by Proposition 3(b) the corresponding layer of S will be the complement of L.

$(*)$ Assume the contrary, i.e., that each of the sets P_1, P_2, and P_3 is nonempty.

$(**)$ Then we claim that P_1, P_2, and P_3 satisfy the hypothesis of Proposition 6. Since S is a double-MDS-code, its layers in the given direction constitute a twofold covering of Σ^{n-1}; and the sets P_0, P_1, P_2, and P_3 constitute a twofold covering of $\{0,1\}^{n-1}$. Since $P_0 = \{0,1\}^{n-1}$, we see that P_1, P_2, and P_3 are pairwise disjoint and $P_1 \cup P_2 \cup P_3 = \{0,1\}^{n-1}$. It remains to show that for all $r \in [n-1]$ and $b \in \{0,1\}$ at least one of the sets $\mathscr{L}_{r;b}P_1$, $\mathscr{L}_{r;b}P_2$, $\mathscr{L}_{r;b}P_3$ is empty. This fact follows from the inductive assumption. Indeed, the double-code $\mathscr{L}_{r;b}S$ fully satisfies the hypothesis of the lemma, and, by the inductive assumption, it has a layer $\mathscr{L}_{n-1;i}\mathscr{L}_{r;b}S$, $i \in \{1,2,3\}$, complementary to the "linear" layer $\mathscr{L}_{n-1;0}\mathscr{L}_{r;b}S$. Using Proposition 2(b),(d) and the inclusion $\mathscr{L}_{n-1;0}\mathscr{L}_{r;b}S \supset \{0,1\}^{n-2}$, we infer

$$\mathscr{L}_{r;b}P_i = \mathscr{L}_{r;b}\big(\{0,1\}^{n-1} \cap \mathscr{L}_{n;i}S\big) = \{0,1\}^{n-2} \cap \mathscr{L}_{r;b}\mathscr{L}_{n;i}S = \{0,1\}^{n-2} \cap \mathscr{L}_{n-1;i}\mathscr{L}_{r;b}S = \varnothing.$$

The claim $(**)$ is proved.

By Proposition 6, S satisfies the hypothesis of Proposition 7. This means that the double-code S is unsplittable, which contradicts the hypothesis of the lemma. Thus, the assumption $(*)$ is not true, and one of the sets P_1, P_2, and P_3 is empty.

Suppose $P_j = \varnothing$. Then $b = j$, $\{0,1\}^{n-1} \subset L \backslash \mathscr{L}_{n;b}S$; therefore $\mathscr{L}_{n;b}S = \Sigma^{n-1} \backslash L$ by Proposition 3(b). Item (a) of the lemma is proved.

(b) As shown in Item (a), two layers of the double-MDS-code S in direction k are complements to each other (with respect to Σ^{n-1}). The definition of a double-code implies that the other two layers also are complements to each other. Hence an appropriate permutation of layers converts S to its complement $\Sigma^n \backslash S$ and the splittability of the former means the splittability of the later. $\square$

Examples show that the layer linearity hypothesis in Lemma 1 is essential for the existence of a layer complementary to a given one in a splittable double-MDS-code.

§ 3. MDS Codes and n-Quasigroups

Definition. Let $G \subseteq \Sigma^n = \{0,1,2,3\}^n$; a function $f : G \to \Sigma$ is called a *partial n-quasigroup of order* 4 provided that the equation

$$f(\bar{a}^{(i)}\#x) = f(a_1, \dots a_{i-1}, x, a_{i+1}, \dots a_n) = b \tag{4}$$

has at most one solution $x \in \Sigma$ for all $\bar{a} \in \Sigma^n$ and $b \in \Sigma$. If, in addition, $G = \Sigma^n$ then the function f is called an *n-quasigroup* of order 4 (in what follows we omit the words "of order 4"). In this case (4) has exactly one solution for all $\bar{a} \in \Sigma^n$ and $b \in \Sigma$. By $f^{\langle i \rangle}$ we denote the *inversion* of the n-quasigroup f in the ith argument, which is defined by the relation

$$f^{\langle i \rangle}(\bar{x}) = b \quad\Longleftrightarrow\quad f(\bar{x}^{(i)}\#b) = x_i.$$

Obviously, the inversion of an n-quasigroup f in each argument also is an n-quasigroup.

Definition. An n-quasigroup $g : \Sigma^n \to \Sigma$ is called an *extension* of a partial n-quasigroup $f : G \to \Sigma$ provided that $f = g|_G$. A partial n-quasigroup that have at least one extension is called *extendable.*

Definition. An n-quasigroup f is called *reduced* provided that $f(\bar{0}^{(i)}\#a) = a$ for all $i \in [n]$ and $a \in \Sigma$. A permutation $\tau : \Sigma \to \Sigma$ is called *reduced* provided that $\tau(0) = 0$.

Definition. An n-quasigroup f is called *decomposable* if there exist an integer m, $2 \le m < n$, an $(n-m+1)$-quasigroup h, an m-quasigroup g, and a permutation $\sigma : [n] \to [n]$ such that

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

Take $f : \Sigma^n \to \Sigma$ and define the sets

$$C(f) \triangleq \{(\bar{x}, f(\bar{x})) : \bar{x} \in \Sigma^n\},\ C_a(f) \triangleq \{\bar{x} \in \Sigma^n : f(\bar{x}) = a\},\ S_{a,b}(f) \triangleq C_a(f) \cup C_b(f).$$

The following is straightforward from definitions:

Proposition 8. (a) *The mapping $C(\cdot)$ is a one-to-one correspondence between the set of all n-quasigroups and the set of all* MDS *codes of length $n+1$.*

(b) *A function $f : \Sigma^n \to \Sigma$ is an n-quasigroup if and only if the sets $C_a(f)$ are pairwise disjoint* MDS-*codes for all $a \in \Sigma$.*

(c) *A function $f : \Sigma^n \to \Sigma$ is an n-quasigroup if and only if for all different a and b in Σ the set $S_{a,b}(f)$ is a splittable double-*MDS-*code.*

Definition. n-Quasigroups f and g are called *equivalent* provided that there exist a permutation $\sigma : [n] \to [n]$ and an $(n+1)$-isotopy $\bar{\tau} = (\tau_0, \tau_1, \ldots, \tau_n)$ such that

$$f(x_1, \ldots, x_n) \equiv \tau_0 g(\tau_1 x_{\sigma(1)}, \ldots, \tau_n x_{\sigma(n)}).$$

A set of n-quasigroups is called *closed under equivalence* provided that it contains n-quasigroups together with their equivalence classes.

It follows from definitions that if n-quasigroups f and g are equivalent then the MDS codes $C(f)$ and $C(g)$ are equivalent too. Moreover, an n-quasigroup f and its inversion $f^{\langle i \rangle}$, $i \in [n]$, correspond to the equivalent MDS codes $C(f)$ and $C(f^{\langle i \rangle})$. For $n \ge 3$, there are examples in which an n-quasigroup and its inversion are not equivalent. Thus the equivalence of MDS codes does not imply that the corresponding n-quasigroups are equivalent. However, we easily see

Proposition 9. (a) *Equivalent n-quasigroups are decomposable or nondecomposable simultaneously.*

(b) *If an n-quasigroup f is decomposable then so are its inversions $f^{\langle i \rangle}$, $i \in [n]$.*

Proposition 10. *Let $f : \Sigma^n \to \Sigma$ be an n-quasigroup. Then there are a unique isotopy $(\tau_0, \tau_1, \ldots, \tau_n)$ with $\tau_0 = (0, a)$, $a \in \Sigma$, and reduced permutations $\tau_1, \ldots, \tau_n : \Sigma \to \Sigma$ such that*

$$f(\bar{x}) \equiv \tau_0 g(\tau_1 x_1, \tau_2 x_2, \ldots, \tau_n x_n) \tag{5}$$

where g is a reduced n-quasigroup, $\bar{x} = (x_1, x_2, \ldots, x_n)$.

Proof. From (5) we deduce

$$\begin{aligned} \tau_0(0) = f(0, \ldots, 0), &\quad \text{i.e., } \tau_0 = (0, f(0, \ldots, 0)), \\ \tau_i(b) = \tau_0^{-1} f(\bar{0}^{(i)} \# b), &\quad i = 1, \ldots, n, \\ g(\bar{x}) = \tau_0^{-1} f\big(\tau_1^{-1} x_1, \tau_2^{-1} x_2, \ldots, \tau_n^{-1} x_n\big), & \end{aligned} \tag{6}$$

which yields the uniqueness of the representation. On the other hand, it is straightforward that if we define $\tau_0, \tau_1, \ldots, \tau_n$ and g by (6) then the conditions of the proposition will be satisfied. $\square$

Let V_n be the set of all n-quasigroups of order 4. Denote by $R_n \subseteq V_n$ the set of all decomposable n-quasigroups and by $V_n^\star \subset V_n$ the set of all reduced n-quasigroups. Given an arbitrary subset of V_n denoted by a capital letter with index, for example W_n, we introduce the following notation: $W_n^\star \triangleq W_n \cap V_n^\star$, $w_n \triangleq |W_n|$, and $w_n^\star \triangleq |W_n^\star|$.

The following is immediate from Proposition 10:

Corollary 1. *Let $W_n \subseteq V_n$ be a set of n-quasigroups of order 4 closed under equivalence. Then $w_n = 4 \cdot 6^n w_n^\star$.*

A partial n-quasigroup $g : G \to \Sigma$ is called *compatible* with an n-quasigroup f whenever $f(\bar{x}) \neq g(\bar{x})$ for every $\bar{x}$ from G. Denote by $F(g)$ the set of all n-quasigroups compatible with an n-quasigroup g.

Proposition 11. *Let g be an n-quasigroup and let $W_n \subseteq V_n$ be a set of n-quasigroups which is closed under equivalence. Then $|F(g) \cap W_n| \leq 3^{n+1} w_n^*$.*

Proof. Consider the set $T \subset \Sigma^n$ that consists of the vertices differing from $(0, \dots, 0) \in \Sigma^n$ in at most one position. Given a partial n-quasigroup $t : T \to \Sigma$, consider the set $W_n(t)$ of its extensions from the class W_n, i.e., $W_n(t) \triangleq \{f \in W_n : f|_T = t\}$. Since W_n is closed under equivalence, $|W_n(t)| = w_n^\star$.

It is easy to see that there are exactly 3^{n+1} different partial n-quasigroups $t : T \to \Sigma$ compatible with a given n-quasigroup g. Since an n-quasigroup $f \in W_n(t)$ is compatible with g only if $t = f|_T$ is compatible with g, the number of the n-quasigroups from W_n that are compatible with g does not exceed $3^{n+1} w_n^\star$. $\square$

Let $q : \Sigma^{n-1} \times A \to \Sigma$ be a partial n-quasigroup, $A \subseteq \Sigma$, and let α be an element of A. We call the subfunction

$$q_\alpha(x_1, \dots, x_{n-1}) \triangleq q(x_1, \dots, x_{n-1}, \alpha).$$

a *layer* of q. The following is straightforward from Proposition 11 and Corollary 1:

Corollary 2. *Let U_n be the set of partial n-quasigroups $g : \Sigma^{n-1} \times \{a, b\} \to \Sigma$ such that their layers g_α, $\alpha \in \{a, b\}$, belong to a set W_{n-1} closed under equivalence. Then $|U_n| \leq (3w_{n-1}^2)/2^{n+1}$.*

Proposition 12 (a representation of a decomposable n-quasigroup by the superposition of subfunctions). *Let h and g be $(n-m+1)$- and m-quasigroups and*

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

$$h_0(x, \bar{z}) \triangleq f(x, \bar{0}, \bar{z}), \quad g_0(x, \bar{y}) \triangleq f(x, \bar{y}, \bar{0}), \quad \delta(x) \triangleq f(x, \bar{0}, \bar{0}), \tag{7}$$

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

$$f(x, \bar{y}, \bar{z}) \equiv h_0(\delta^{-1}(g_0(x, \bar{y})), \bar{z}). \tag{8}$$

Proof. It follows from (7) that

$$h_0(\cdot, \bar{z}) \equiv h(g(\cdot, \bar{0}), \bar{z}), \quad g_0(x, \bar{y}) \equiv h(g(x, \bar{y}), \bar{0}), \quad \delta^{-1}(\cdot) \equiv g^{\langle 1 \rangle}(h^{\langle 1 \rangle}(\cdot, \bar{0}), \bar{0}).$$

Inserting these representations of h_0, g_0, and δ^{-1} to (8), we can readily verify its validity. $\square$

Proposition 13 (on the number of decomposable n-quasigroups). *If $r_n^\star$ is the number of reduced decomposable n-quasigroups then*

$$r_n^\star \leq \sum_{m=2}^{n-1} \binom{n}{m} v_{n-m+1}^\star v_m^\star.$$

Proof. By Proposition 12 a reduced decomposable n-quasigroup can be represented (maybe ambiguously) as a superposition of reduced $(n-m+1)$- and m-quasigroups with $m \in \{2, \dots, n-1\}$. For every such m, the number of ways of splitting the set of arguments into two groups equals $\binom{n}{m}$; and the numbers of ways of choosing $(n-m+1)$- and m-quasigroups equal respectively $v_{n-m+1}^\star$ and $v_m^\star$. The order of arguments in each of the groups is not essential, because a reduced m-quasigroup goes into a reduced m-quasigroup under a coordinate permutation. $\square$

§ 4. Semilinear n-Quasigroups

DEFINITION. An n-quasigroup f is called *semilinear* provided that there are $a, b \in \Sigma$ such that $S_{a,b}(f)$ is a linear double-code. An n-quasigroup f is called *linear* provided that for all $a, b \in \Sigma$, $a \neq b$, the double-code $S_{a,b}(f)$ is linear.

Proposition 14. *The reduced linear n-quasigroup is unique.*

PROOF. The statement follows from Proposition 4(e) and the fact that every n-quasigroup f is uniquely defined by the double-MDS-codes $S_{0,1}(f)$ and $S_{0,2}(f)$. $\square$

Denote by $K_n \subseteq V_n$ the set of all semilinear n-quasigroups and by $K_n(a, b)$ the set of semilinear n-quasigroups f such that the double-code $S_{a,b}(f)$ is linear. The following proposition is easy:

Proposition 15. *For all different a, b, c in Σ the intersection $K_n(a, b) \cap K_n(a, c)$ is the set of all linear n-quasigroups.*

Using Proposition 5(a), we easily prove by induction on m the following

Proposition 16. *Let f be a semilinear n-quasigroup. Then for all $(a_1, \dots, a_m) \in \Sigma^m$ the function*

$$g(x_1, \dots, x_{n-m}) \triangleq f(x_1, \dots, x_{n-m}, a_1, \dots, a_m)$$

is a semilinear $(n - m)$-quasigroup.

Proposition 17. (a) *Equivalent n-quasigroups are or are not semilinear simultaneously.*

(b) *If f is a semilinear n-quasigroup then its inversions $f^{\langle i \rangle}$, $i \in [n]$, also are semilinear n-quasigroups.*

PROOF. Item (a) follows from the fact that the set of linear double-codes is closed under equivalence (Proposition 4(a)).

Let us prove (b). It is straightforward that the semilinearity of f is equivalent to the existence of $a_0 = a$, $b_0 = b$, $a_1, \dots, a_n$, $b_1, \dots, b_n$ such that $a_i \neq b_i$ and

$$\bigoplus_{i=0}^{n} \chi_{\{a_i, b_i\}}(x_i) = 0 \tag{9}$$

for all $x_0, x_1, \dots, x_n$ satisfying $x_0 = f(x_1, x_2, \dots, x_n)$. Since (9) is symmetric with respect to the choice of the dependent variable, the claim is proved. $\square$

REMARK. The reduced linear n-quasigroup f can be represented as $f(x_1, \dots, x_n) = x_1 * \dots * x_n$ where $(\Sigma, *)$ is a group isomorphic to $Z_2 \times Z_2$, with the addition table

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

The following two lemmas were proved in [3, 4]. The first concerns a representation of a nonprime double-MDS-code by prime double-codes of smaller dimensions. The second lemma, an essential corollary of the former, connects the decomposability property of an n-quasigroup q with the nonprimality property of $S_{c,d}(q)$.

Lemma 2 (on decomposition of a double-MDS-code) [3, 4]. *Let S be a double-*MDS*-code. Then there exists $k = k(S) \in [n]$ such that*

(a) *the characteristic function χ_S can be represented as*

$$\chi_S(\bar{x}) \equiv \bigoplus_{j=1}^{k} \chi_{S_j}(\tilde{x}_j) \tag{10}$$

where $\tilde{x}_j = (x_{i_{j,1}}, \dots, x_{i_{j,n_j}})$ *are disjoint collections of variables from* $\bar{x}$, $S_j \subset \Sigma^{n_j}$ *are prime double*-MDS-*codes for* $j \in [k]$; *the representation is unique up to substitution of double*-MDS-*codes* $S_j \backslash \Sigma^{n_j}$ *for some double*-MDS-*codes* S_j;

(b) S *is a union of* 2^{k-1} *pairwise disjoint prime double-codes of the same cardinality*; $\Sigma^n \backslash S$ *is a union of* 2^{k-1} *pairwise disjoint prime double-codes of the same cardinality.*

Lemma 3 (on decomposability of n-quasigroups) [3, 4]. *Let* $S \subset \Sigma^n$ *be a double*-MDS-*code that satisfies* (10), $c \neq d \in \Sigma$, *and let* q *be an* n-*quasigroup such that* $S_{c,d}(q) = S$. *Then*

$$q(\bar{x}) \equiv q_0(q_1(\tilde{x}_1), \dots, q_k(\tilde{x}_k)) \tag{11}$$

where q_j, $j \in [k]$, *are* n_j-*quasigroups,* q_0 *is a semilinear* k-*quasigroup, and the collections of variables* $\tilde{x}_j = (x_{i_{j,1}}, \dots, x_{i_{j,n_j}})$, $j \in [k]$, *and the numbers* k, n_j *are defined by Lemma* 2.

Corollary 3. *Let* $\{a, b, c, d\} = \Sigma$, *let* q *be an* n-*quasigroup, and let a partial* n-*quasigroup* $g \triangleq q|_{\Sigma^{n-1} \times \{a,b\}}$ *have more than two extensions. Then* $q \in R_n \cup K_n$.

Proof. It follows from definitions that $C_a(f^{\langle n \rangle}) = C(f_a)$ for an arbitrary n-quasigroup f and its inversion in the nth argument $f^{\langle n \rangle}$. Let

$$S \triangleq \Sigma^n \backslash (C(g_a) \cup C(g_b)).$$

Then for every extension f of the partial n-quasigroup g we see that

$$S = \Sigma^n \backslash (C(f_a) \cup C(f_b)) = C(f_c) \cup C(f_d) = S_{c,d}(f^{\langle n \rangle}).$$

By hypothesis, the partial n-quasigroup g has more than two extensions f. Each of the extensions is uniquely defined by its layer f_c. Hence the double-MDS-code S includes more than two different MDS codes $C(f_c)$. By Proposition 1, the double-MDS-code $S = S_{c,d}(q^{\langle n \rangle})$ consists of more than one prime double-code. According to Lemmas 2 and 3, the number k in (11) is not less than 2. If $k < n$ then (11) implies the decomposability of $q^{\langle n \rangle}$; if $k = n$ then (10) implies the semilinearity. So, $q^{\langle n \rangle} \in K_n \cup R_n$. Then by Propositions 9(b) and 17(b) we obtain $q \in K_n \cup R_n$. $\square$

§ 5. On the Number of n-Quasigroups

In this section, we evaluate the number of n-quasigroups of order 4 by establishing that the subclass of semilinear n-quasigroups is asymptotically dominant. We first calculate the number of the semilinear n-quasigroups.

Theorem 1 (on the number of semilinear n-quasigroups). $k_n^\star = 3 \cdot 2^{2^n - n - 1} - 2$ *and* $k_n = 3^{n+1} \cdot 2^{2^n + 1} - 2^3 6^n$.

Proof. An arbitrary n-quasigroup f in $K_n^\star(0,1)$ can be defined by firstly choosing the linear double-code $S_{0,1}(f)$ and secondly, the MDS codes $C_0(f) \subset S_{0,1}(f)$ and $C_2(f) \subset \Sigma^n \backslash S_{0,1}(f)$. A linear double-code can be chosen in $2 \cdot 3^n$ ways (Proposition 4(f)); an MDS code, in $2^{2^{n-1}}$ ways (Proposition 1). So,

$$|K_n(0,1)| = 2 \cdot 3^n \cdot 2^{2^{n-1}} \cdot 2^{2^{n-1}} = 3^n \cdot 2^{2^n + 1}.$$

By Corollary 1 we find that $|K_n^\star(0,1)| = 2^{2^n - n - 1}$ and, similarly,

$$|K_n^\star(0,2)| = |K_n^\star(0,3)| = 2^{2^n - n - 1}.$$

It follows from Propositions 14 and 15 that the pairwise intersections of $K_n^\star(0,1)$, $K_n^\star(0,2)$, $K_n^\star(0,3)$ contain only one element. Then, by the inclusion and exclusion formula,

$$k_n^\star = |K_n^\star(0,1) \cup K_n^\star(0,2) \cup K_n^\star(0,3)| = 3 \cdot 2^{2^n - n - 1} - 3 + 1.$$

By Corollary 1, $k_n = 4 \cdot 6^n k_n^\star$. $\square$

Remark. The lower bound $v_n \geq 3^{n+1} \cdot 2^{2^n + 1} - 2^3 6^n$ was established in [5].

As a result of a numerical experiment, we have the values:

$$v_1^\star = 1, \quad v_2^\star = 4, \quad v_3^\star = 64 \quad [6], \quad v_4^\star = 7132, \quad v_5^\star = 201538000. \tag{12}$$

The following lemma shows that the existence of a semilinear layer in a n-quasigroup yields an arrangement of its structure.

Lemma 4 (on a semilinear layer). *Let q be an n-quasigroup and there exists $\alpha \in \Sigma$ such that $q_\alpha \in K_{n-1}$. Then $q \in K_n \cup R_n$.*

PROOF. Assume that $q_\alpha \in K_{n-1}$ for some $\alpha \in \Sigma$ and so the double-MDS-code $S_{a,b}(q_\alpha)$ is linear for some $a, b \in \Sigma$. Consider $S_{a,b}(q)$; we have $S_{a,b}(q_\alpha) = \mathscr{L}_{n;\alpha}(S_{a,b}(q))$. Then, by Lemma 1, there is $\beta \in \Sigma$, $\beta \neq \alpha$, such that

$$S_{a,b}(q_\beta) = \mathscr{L}_{n;\beta}(S_{a,b}(q)) = \Sigma^{n-1} \backslash S_{a,b}(q_\alpha),$$

i.e., the $(n-1)$-quasigroup q_β is semilinear.

$(*)$ We claim that the partial n-quasigroup $g \triangleq q|_{\Sigma^{n-1}\times\{\alpha,\beta\}}$ has two semilinear extensions. Let $\{a, b, c, d\} = \{\alpha, \gamma, \beta, \delta\} = \Sigma$ and let $\sigma \triangleq (ab)(cd)$ be a permutation of symbols of Σ. Then the function f defined by the equalities

$$f(x_1, \dots, x_{n-1}, \alpha) \triangleq q(x_1, \dots, x_{n-1}, \alpha),\ f(x_1, \dots, x_{n-1}, \beta) \triangleq q(x_1, \dots, x_{n-1}, \beta),$$

$$f(x_1, \dots, x_{n-1}, \gamma) \triangleq \sigma q(x_1, \dots, x_{n-1}, \alpha),\ f(x_1, \dots, x_{n-1}, \delta) \triangleq \sigma q(x_1, \dots, x_{n-1}, \beta)$$

is an extension of the partial n-quasigroup g. It is clear that $S_{a,b}(f_\gamma) = S_{a,b}(f_\alpha) = S_{a,b}(q_\alpha)$; therefore the double-codes $\mathscr{L}_{n;\alpha}(S_{a,b}(f)) = \mathscr{L}_{n;\gamma}(S_{a,b}(f))$ are linear. Hence, by Proposition 5(b), the double-code $S_{a,b}(f)$ also is linear. So, the n-quasigroups f and $f'(\bar{x}) \triangleq f(x_1, \dots, x_{n-1}, \tau(x_n))$ with $\tau \triangleq (\gamma, \delta)$ satisfy $(*)$.

We note finally that either q coincides with one of the f and f', and thus $q \in K_n$; or g has more than two extensions $(q,\ f,\ f')$, and $q \in K_n \cup R_n$ by Corollary 3. $\square$

Theorem 2 (on the number of n-quasigroups). *If $n \geq 5$, then $3^{n+1}2^{2^n+1} \leq v_n \leq (3^{n+1}+1)2^{2^n+1}$.*

PROOF. Put $q \in V_n$ and consider the partial n-quasigroup $g_{\alpha,\beta} = q|_{\Sigma^{n-1}\times\{\alpha,\beta\}}$ for arbitrary $\alpha, \beta \in \Sigma$. If $g_{\alpha,\beta}$ has more than two extensions then, by Corollary 3, we obtain $q \in K_n \cup R_n$. If $q_\alpha \in K_{n-1}$ or $q_\beta \in K_{n-1}$ then $q \in K_n \cup R_n$ by Lemma 4. Hence if $q \notin K_n \cup R_n$ then for all $\alpha, \beta \in \Sigma$ we have $q_\alpha, q_\beta \notin K_{n-1}$ and the partial n-quasigroup $g_{\alpha,\beta}$ has two extensions.

Introduce the notation $T_n \triangleq V_n \backslash K_n$ and $W_n \triangleq T_n \backslash R_n$. It follows from Propositions 9(a) and 17(a) that the sets T_n and W_n are closed under equivalence. Then $q \in W_n$ implies $q_\alpha \in T_n$ for all $\alpha \in \Sigma$ and, by Corollary 2,

$$w_n \leq \frac{3t_{n-1}^2}{2^n}. \tag{13}$$

$(*)$ We claim that the following three inequalities hold. We will prove them by induction on n.

(a) $k_n^\star \leq v_n^\star \leq 2k_n^\star$ whenever $n \geq 1$;

(b) $t_n \leq 2^{2^n+1}$ whenever $n \geq 5$;

(c) $v_n \leq (3^{n+1}+1)2^{2^n+1}$ whenever $n \geq 5$.

When $n \leq 5$, the conditions (a)–(c) are verified by using the exact values of $k_n^\star$, $v_n^\star$, v_n, $t_n = v_n - k_n$ ((12), Theorem 1). By the inductive assumption, (a) holds for $n \in [m]$, and (b), (c) hold for $n = m \geq 5$. Let us show the validity of (a)–(c) for $n = m+1$. From (a) and Theorem 1 with $m \geq 5$, $m-1 > i > 2$ the following holds:

$$v_{m-i+1}^\star v_i^\star \leq 4k_{m-i+1}^\star k_i^\star < 4 \cdot 9 \cdot 2^{2^{m-i+1}+2^i-m-3} < 4 \cdot 3 \cdot 2^{2^{m-1}-m-1} = v_2^\star k_{m-1}^\star \leq v_{m-1}^\star v_2^\star.$$

Since $v_2^\star = 4$, from the estimate for $r_n^\star$ (Proposition 13) we derive

$$r_{m+1}^\star \leq \sum_{i=2}^{m} \binom{m+1}{i} v_{(m+1)-i+1}^\star v_i^\star \leq \sum_{i=2}^{m} \binom{m+1}{i} v_m^\star v_2^\star < 2^{m+1} \cdot v_m^\star \cdot 4.$$

Inserting (c) with $n = m$, we have

$$r_{m+1} < 2^{m+3}(3^{m+1}+1)2^{2^m+1} < 2^{2^{m+1}}. \tag{14}$$

Moreover, from (13) and (b) with $n = m$ we deduce the inequality

$$w_{m+1} \leq \frac{3t_m^2}{2^{m+1}} \leq \frac{3 \cdot 2^{2^{m+1}+2}}{2^{m+1}} < 2^{2^{m+1}}. \tag{15}$$

By the definitions of T_m and W_m we have $t_{m+1} \leq w_{m+1} + r_{m+1}$ and $v_{m+1} = t_{m+1} + k_{m+1}$. Then from (14) and (15) we derive (b) with $n = m+1$, and from Theorem 1 and (b) we obtain (a) and (c) with $n = m+1$. The claim $(*)$ is proved.

It remains to show the lower estimate for v_n. We prove first that the following holds for $n \geq 4$:

$$t_n^\star \geq t_3^\star v_{n-2}^\star. \tag{16}$$

Let $g \in T_3^\star$ and $h \in V_{n-2}^\star$. Then Proposition 16 implies that the n-quasigroup

$$f(x_1, \dots, x_n) \triangleq h(g(x_1, x_2, x_3), x_4, \dots, x_n)$$

is not semilinear. It is easy to check that the different pairs of the reduced $(n-2)$-quasigroup h and 3-quasigroup g correspond to the different reduced n-quasigroups f. Inequality (16) is proved.

From (12) and Theorem 1 we see that $t_3^\star = 18$. Thus, (16) and Theorem 1 imply $v_n^\star = k_n^\star + t_n^\star \geq 3^n 2^{2^n-n-1}$ for $n \geq 4$. Then from Corollary 1 we deduce the inequality $v_n \geq 3^{n+1} 2^{2^n+1}$ for $n \geq 4$. $\square$

The following is straightforward from Theorem 2 and Proposition 8:

Corollary 4 (the asymptotic forms of the number of n-quasigroups and the number of MDS codes). *Let m_n be the number of* MDS-*codes in Σ^n and let v_n be the number of n-quasigroups of order* 4. *Then*

$$v_n = 3^{n+1} 2^{2^n+1}(1 + o(1)), \quad m_n = 3^n 2^{2^{n-1}+1}(1 + o(1)).$$

References

1. *Belousov V. D.*, n-Ary Quasigroups [in Russian], Shtiintsa, Kishinev (1972).
2. *Krotov D. S. and Potapov V. N.*, "On the reconstruction of n-quasigroups of order 4 and the upper bounds on their number," in: Proceedings of the Conference Devoted to the 90th Anniversary of Alexei A. Lyapunov, Novosibirsk, Russia, October 8–11, 2001, pp. 323–327 [http://www.sbras.ru/ws/Lyap2001/2363].
3. *Krotov D. S.*, "On decomposition of $(n, 4^{n-1}, 2)_4$ MDS codes and double-codes," in: Proceedings of Eighth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT-VIII), Sept. 8–14, 2002, Tsarskoe Selo, Russia, pp. 168–171.
4. *Krotov D. S.*, "On decomposability of 4-ary distance 2 MDS codes, double-codes, and n-quasigroups of order 4," arXiv.org eprint math.CO/0509358, 2005. Available at http://arxiv.org/abs/math/0509358 (submitted to Discrete Mathematics).
5. *Krotov D. S.*, "Lower estimates for the number of m-quasigroups of order 4 and for the number of perfect binary codes," Diskret. Anal. Issled. Oper. Ser. 1, **7**, No. 2, 47–53 (2000).
6. *Mullen G. L. and Weber R. E.*, "Latin cubes of order ≤ 5," Discrete Math., **32**, No. 3, 291–298 (1988).

V. N. Potapov; D. S. Krotov
Sobolev Institute of Mathematics, Novosibirsk, Russia
E-mail address: vpotapov@math.nsc.ru; krotov@math.nsc.ru