ISSN 1990-4789, Journal of Applied and Industrial Mathematics, 2007, Vol. 1, No. 3, pp. 373–379. © Pleiades Publishing, Ltd., 2007.
Original Russian Text © V.N. Potapov, 2006, published in Diskretnyi Analiz i Issledovanie Operatsii, Ser. 1, 2006, Vol. 13, No. 4, pp. 49–59.

A Lower Bound for the Number of Transitive Perfect Codes

V. N. Potapov

Sobolev Institute of Mathematics, pr. Akad. Koptyuga 4, Novosibirsk, 630090 Russia
Received March 9, 2006

Abstract—We construct at least $\frac{1}{8n^2\sqrt{3}}e^{\pi\sqrt{2n/3}}(1+o(1))$ pairwise nonequivalent transitive extended perfect codes of length $4n$ as $n \to \infty$.

DOI: 10.1134/S199047890703012X

INTRODUCTION

The isometries of the Boolean n-cube transforming a given subset A of this n-cube into itself are called the *automorphisms* of A. A set is called *transitive* if it is an orbit under the action of its own automorphism group. The transitive perfect codes of length 15 were considered in [1]. In [2], there were constructed $\lfloor \frac{1}{2}\log_2 n\rfloor^2$ nonequivalent transitive perfect (and extended perfect) codes with various values of the following two parameters: the dimension of the linear span (the rank) and the dimension of the kernel of the code.

In the present article, using the construction of [5], we prove that (as $n \to \infty$) there are at least $\frac{1}{8n^2\sqrt{3}}e^{\pi\sqrt{2n/3}}(1+o(1))$ pairwise nonequivalent transitive extended perfect codes of length $4n$. All transitive perfect codes of length n constructed in this article have rank $n-\log_2 n$.

1. THE MAIN DEFINITIONS

Let $E_k = \{0, 1, \dots, k-1\}$. Denote by E_k^n the set of all ordered collections (called *vertices*) of length n. By the *Hamming distance* $d(\overline{x}, \overline{y})$ between the collections $\overline{x} = (x_1, x_2, \dots, x_n)$ and $\overline{y} = (y_1, y_2, \dots, y_n)$ we mean the number of those positions in which the elements of $\overline{x}$ and $\overline{y}$ are distinct. The set of all vertices at distance not greater than 1 from $\overline{x}$ is called the *ball* of radius 1 with center $\overline{x}$ and is denoted by $\mathcal{B}(\overline{x})$. By an *edge* of direction i we mean the set of vertices differing only in the ith position.

We denote by $\mathcal{E}_i(\overline{x})$ the edge of direction i containing a vertex $\overline{x} \in E_k^n$.

Denote by $E_{2,0}^n$ and $E_{2,1}^n$ the subsets of E_2^n consisting of all vertices with even and odd number of units respectively. A set $C \subset E_{2,0}^n$ ($C \subset E_{2,1}^n$) is called an *extended perfect code* (with distance 4) of length n if $|\mathcal{B}(\overline{x}) \cap C| = 1$ for each vertex $\overline{x} \in E_{2,1}^n$ ($\overline{x} \in E_{2,0}^n$). A set $M \subset E_k^n$ is called an MDS-*code* (with distance 2) of length n if $|\mathcal{E}_i(\overline{x}) \cap M| = 1$ for any $i = 1, \dots, n$ and $\overline{x} \in E_k^n$. This definition implies that an extended perfect code is a cardinality maximal subset of E_2^n with distance at least 4 between the vertices, and an MDS-code is a maximal subset of E_k^n with distance at least 2 between the vertices. It is known that extended perfect codes of length n exist for $n = 2^t$ where t is a positive integer, and MDS-codes with distance 2 exist for all positive integers n and k.

A function $f : E_k^n \to E_k$ is called an *n-quasigroup of order k* if $f(\overline{x}) \neq f(\overline{y})$ for every two vertices $\overline{x}, \overline{y} \in E_k^n$ such that $d(\overline{x}, \overline{y}) = 1$. Let $G(f) = \{(\overline{x}, f(\overline{x})) \mid \overline{x} \in E_k^n\}$ be the graph of f. Obviously, the mapping $G(\cdot)$ establishes a one-to-one correspondence between the n-quasigroups and MDS-codes of length $n+1$.

Let $\tau : \{1, \dots, n\} \to \{1, \dots, n\}$ be a permutation (i.e., $\tau \in S_n$), and let $\overline{\sigma} = (\sigma_1, \dots, \sigma_n)$ be a collection of permutations of the form $\sigma_i : E_k \to E_k$ (i.e., $\overline{\sigma} \in S_k^n$). Given an arbitrary vertex $\overline{x} \in E_k^n$, we define $\overline{x}_\tau = (x_{\tau(1)}, \dots, x_{\tau(n)})$ and $\overline{\sigma x} = (\sigma_1(x_1), \dots, \sigma_n(x_n))$. Take $A \subseteq E_k^n$. Introduce the notation

$$A_\tau = \{\overline{x}_\tau \mid \overline{x} \in A\}, \qquad \overline{\sigma}A = \{\overline{\sigma x} \mid \overline{x} \in A\}.$$

A set (code) $A \subseteq E_k^n$ will be called *transitive* if for every two vertices $\overline{x}$ and $\overline{y}$ of A there exist a permutation $\tau \in S_n$ of coordinates and some permutations $\overline{\sigma} \in S_k^n$ of symbols in each coordinate such that $\overline{\sigma y} = \overline{x}_\tau$ and $\overline{\sigma} A = A_\tau$. Clearly, one of the vertices in the definition may be fixed.

The main goal of the present paper is to prove the following

Theorem. *As $n \to \infty$, there exist at least $\frac{1}{8n^2\sqrt{3}} e^{\pi\sqrt{2n/3}}(1+o(1))$ pairwise nonequivalent transitive extended perfect codes of length $4n$.*

Henceforth we will consider the *normalized* codes, i.e., the codes with the property $\overline{0} \in A$. In case $k=2$ the definition of transitivity of a code A can be written as follows: a code $A \subseteq E_2^n$ is transitive if for each vertex $\overline{x} \in A$ there exists a permutation $\tau \in S_n$ such that $\overline{x} + A = A_\tau$. Here and in the sequel the sum is understood by modulo 2.

We will call a normalized code $A \subseteq E_k^n$ *isotopically transitive* if for each vertex $\overline{x} \in A$ there exists a collection of permutations $\overline{\sigma} \in S_k^n$ such that $\overline{\sigma}(\overline{0}) = \overline{x}$ and $A = \overline{\sigma} A$. For $k=2$, this notion coincides with the notion of *linearity*: $A + \overline{x} = A$ for every $\overline{x} \in A$.

Call an n-quasigroup *normalized* if $f(\overline{0}) = 0$. A normalized n-quasigroup is called *isotopically transitive* if for every vertex $\overline{a} \in E_k^n$ there exist permutations $\overline{\sigma} \in S_k^n$ and $\sigma_{n+1} \in S_k$ such that $\overline{\sigma}(\overline{0}) = \overline{a}$, $\sigma_{n+1}(0) = f(\overline{a})$, and $f(\overline{\sigma x}) = \sigma_{n+1}(f(\overline{x}))$ for all $\overline{x} \in E_k^n$. These definitions imply the following

Proposition 1. *An n-quasigroup f is isotopically transitive if and only if the* MDS-*code $G(f)$ of length $n+1$ is isotopically transitive.*

The codes $A, B \subseteq E_k^n$ are called *equivalent* if there exist permutations $\tau \in S_n$ and $\overline{\sigma} \in S_k^n$ such that $A_\tau = \overline{\sigma} B$ (in case $A, B \subset E_2^n$, there exist a permutation $\tau \in S_n$ and a vertex $\overline{x} \in E_2^n$ such that $A_\tau = \overline{x} + B$).

Proposition 2. *Equivalent codes are transitive* (*isotopically transitive*) *simultaneously.*

The construction in [5] and [6] connects MDS-codes and extended perfect codes. We consider a particular case of this construction. Fix a linear extended perfect code $R \subset E_2^n$ (a Hamming code). Let $M \subset E_4^n$ be a normalized MDS-code (not depending of $\overline{r}$). Define the partitions of $E_{2,0}^4$ and $E_{2,1}^4$ into codes by the equality

$$C_a^r = C_0 + (1+r)\overline{e}_4 + \overline{e}_a,$$

where $r \in \{0,1\}$, $a \in E_4$, $C_0 = \{\overline{0}, \overline{1}\} \subset E_2^4$, and $\overline{e}_i \in E_2^4$ are the basis vectors with 1 in the ith coordinate (we assume that $\overline{e}_0 = \overline{e}_4$). Thus, we have

$$C_0^0 = \{(0000),(1111)\}, \qquad C_1^0 = \{(0110),(1001)\}, \qquad C_2^0 = \{(0101),(1010)\},$$
$$C_3^0 = \{(0011),(1100)\}, \qquad C_0^1 = \{(0001),(1110)\}, \qquad C_1^1 = \{(0111),(1000)\},$$
$$C_2^1 = \{(0100),(1011)\}, \qquad C_3^1 = \{(0010),(1101)\}.$$

Define a normalized extended perfect code $C \subset E_{2,0}^{4n}$ by the equality

$$C = \bigcup_{\overline{r} \in R} \bigcup_{\overline{a} \in M} C_{a_1}^{r_1} \times C_{a_2}^{r_2} \times \cdots \times C_{a_n}^{r_n}. \tag{1}$$

2. TRANSITIVE CODES

It is easy to see that all extended perfect codes of length 4 can be represented as $\{\overline{v}, \overline{v}+\overline{1}\}$; i.e., as cosets C_a^r of the code $C_0^0 = \{\overline{0}, \overline{1}\} \subset E_2^4$. We show that, for $k=4$, a permutation of coordinates corresponds to a permutation of cosets.

Proposition 3. (a) *For each $b \in E_k$, there exists a permutation $\sigma \in S_4$ such that*

$$C_a^r + \overline{e}_b + \overline{e}_4 = C_{\sigma(a)}^r$$

for all $a \in E_4$ and $r \in \{0,1\}$.

(b) *For each permutation $\tau \in S_4$, there exists a permutation $\sigma \in S_4$ such that $\left(C_a^0\right)_\tau = C_{\sigma(a)}^0$ for all $a \in E_4$.*

(c) *For each permutation $\sigma \in S_4$, there exists a permutation $\tau \in S_4$ such that*

$$C^r_{\sigma(a)} + \overline{e}_{\sigma(0)} + \overline{e}_4 = \left(C^r_a\right)_\tau$$

for all $a \in E_4$ and $r \in \{0, 1\}$.

Proof. (a), (b). We consider a partition J of $E^4_{2,0}$ into the codes C^0_0, C^0_1, C^0_2, and C^0_3. It is clear that a permutation of coordinates and an addition of a vertex with an even number of units transform the elements of J to the elements of J, i.e., it generates a permutation. Since $C^r_a = r\overline{e}_4 + C^0_a$, the permutation σ does not depend on $r \in \{0, 1\}$.

(c) We obtain from (a) the equality $C^r_{\sigma(a)} + \overline{e}_{\sigma(0)} + \overline{e}_4 = C^r_{\tau(a)}$ in which the permutation τ does not depend on $r \in \{0, 1\}$. Since $C^r_{\sigma(0)} + \overline{e}_{\sigma(0)} + \overline{e}_4 = C^r_0$, we have $\tau(0) = 0$. Then, it is easy to see that $C^r_{\tau(a)} = (C^r_a)_\tau$ for $a \neq 0$. Moreover, $C^r_0 = (C^r_0)_\pi$ for an arbitrary permutation π that leaves invariant the last coordinate. Proposition 3 is proved. □

Lemma 1. *Let M be an isotopically transitive* MDS*-code of length n. Then the extended perfect code C of length $4n$, defined by* (1)*, is transitive.*

Proof. Represent the vertex $\overline{y} \in C$ in the form $\overline{y} = (\widetilde{y}_1, \widetilde{y}_2, \dots, \widetilde{y}_n)$ where $\widetilde{y}_i = (1 + r_i)\overline{e}_4 + \overline{e}_{b_i} + \delta\overline{1}$, $\delta \in \{0, 1\}$, and $\overline{r} \in R$. The linearity of the code R implies that if $\overline{y} = (\widetilde{y}_1, \widetilde{y}_2, \dots, \widetilde{y}_n) \in C$ then $(\widetilde{y}_1 + r_1\overline{e}_4, \widetilde{y}_2 + r_2\overline{e}_4, \dots, \widetilde{y}_n + r_n\overline{e}_4) \in C$ for every $\overline{r} \in R$. By the definition of C^r_a, we infer that if $\overline{y} = (\widetilde{y}_1, \widetilde{y}_2, \dots, \widetilde{y}_n) \in C$ then $(\widetilde{y}_1 + \delta_1\overline{1}, \widetilde{y}_2 + \delta_2\overline{1}, \dots, \widetilde{y}_n + \delta_n\overline{1}) \in C$ for every $\overline{\delta} \in E^n_2$. Hence

$$\overline{y} + C = v(\overline{b}) + C, \tag{2}$$

where $v(\overline{b}) = (\overline{e}_4 + \overline{e}_{b_1}, \dots, \overline{e}_4 + \overline{e}_{b_n})$ and $\overline{b} \in M$. Since the code M is isotopically transitive, there exists a collection of permutations $\overline{\sigma}$ satisfying the equations $\overline{\sigma}M = M$ and $\overline{\sigma}\overline{0} = \overline{b}$. It follows from Proposition 3 (c) that there exist permutations $\tau_i \in S_4$ $(i = 1, \dots, n)$ such that

$$C^r_{\sigma_i(a)} + \overline{e}_{b_i} + \overline{e}_4 = \left(C^r_a\right)_{\tau_i} \tag{3}$$

for all $a \in E_4$ and $r \in \{0, 1\}$. The equalities (1)–(3) imply

$$\begin{aligned}
\overline{y} + C = v(\overline{b}) + \bigcup_{\overline{r} \in R} \bigcup_{\overline{a} \in M} C^{r_1}_{a_1} \times C^{r_2}_{a_2} \times \dots \times C^{r_n}_{a_n} \\
= v(\overline{b}) + \bigcup_{\overline{r} \in R} \bigcup_{\overline{a} \in \overline{\sigma}M} C^{r_1}_{a_1} \times C^{r_2}_{a_2} \times \dots \times C^{r_n}_{a_n} \\
= \bigcup_{\overline{r} \in R} \bigcup_{\overline{a} \in M} (\overline{e}_4 + \overline{e}_{b_1} + C^{r_1}_{\sigma_1(a_1)}) \times (\overline{e}_4 + \overline{e}_{b_2} + C^{r_2}_{\sigma_2(a_2)}) \times \dots \times (\overline{e}_4 + \overline{e}_{b_n} \\
+ C^{r_n}_{\sigma_n(a_n)}) = \bigcup_{\overline{r} \in R} \bigcup_{\overline{a} \in M} \left(C^{r_1}_{a_1}\right)_{\tau_1} \times \left(C^{r_2}_{a_2}\right)_{\tau_2} \times \dots \times \left(C^{r_n}_{a_n}\right)_{\tau_n} = C_\pi
\end{aligned}$$

for a suitable permutation $\pi \in S_{4n}$. Lemma 1 is proved. □

3. EQUIVALENT CODES

Denote by $I = \{I(1), I(2), \dots, I(n)\}$ the partition of $\{1, 2, \dots, 4n\}$ into the quadruples of the form $I(j) = \{4j - 3, 4j - 2, 4j - 1, 4j\}$. Take $\tau \in S_{4n}$. Denote by I_τ the partition consisting of the sets $\{\tau(4j - 3), \tau(4j - 2), \tau(4j - 1), \tau(4j)\}$. Let the permutation $\tau \in S_{4n}$ be such that $I = I_\tau$. Then τ is generated by the permutation $\tau^* \in S_n$ of elements of the partition I and the family of permutations $\tau_1, \tau_2, \dots, \tau_n \in S_4$, where τ_i is a permutation of the set $I(j)$.

Proposition 4. *Let C and C' be extended perfect codes of length $4n$ satisfying* (1) *with* MDS*-codes M and M' respectively. Assume that the codes C and C' are equivalent, i.e., $C'_\tau = \overline{y} + C$ for some $\tau \in S_{4n}$ and $\overline{y} \in E^{4n}_2$. If $I = I_\tau$ then the* MDR*-codes M and M' are equivalent.*

Proof. Since C and C' are normalized, $\overline{y} \in C$. Represent the vertex $\overline{y} \in C$ as $\overline{y} = (\widetilde{y}_1, \widetilde{y}_2, \dots, \widetilde{y}_n)$ where $\widetilde{y}_i = (1 + r_i)\overline{e}_4 + \overline{e}_{b_i} + \delta\overline{1}$ and $\delta \in \{0, 1\}$. Using Proposition 3 (a), we find the permutations $\sigma_i \in S_4$, $i = 1, \dots, n$, such that

$$C^r_{a_i} + \overline{e}_{b_i} + \overline{e}_4 = C^r_{\sigma_i(a_i)},$$

where $r \in \{0, 1\}$. Then from (1)–(2) we infer that

$$\overline{y} + C = \bigcup_{\overline{r} \in R} \bigcup_{\overline{a} \in M} (\overline{e}_4 + \overline{e}_{b_1} + C^{r_1}_{a_1}) \times (\overline{e}_4 + \overline{e}_{b_2} + C^{r_2}_{a_2}) \times \dots \times (\overline{e}_4 + \overline{e}_{b_n} + C^{r_n}_{a_n})$$
$$= \bigcup_{\overline{r} \in R} \bigcup_{\overline{a} \in \overline{\sigma} M} C^{r_1}_{a_1} \times C^{r_2}_{a_2} \times \dots \times C^{r_n}_{a_n}.$$

Since $C'_\tau = \overline{y} + C$ and $I = I_\tau$, (24) implies the equality $\overline{r}_{\tau^*} = \overline{r}$ for all $\overline{r} \in R$.

Consider the vertices of the codes C and C' which have an even number of units in each four coordinates with indices $4i + 1$, $4i + 2$, $4i + 3$, and $4i + 4$ (where i is a positive integer). By $C'_\tau = \overline{y} + C$ and (4), we have

$$\bigcup_{\overline{a} \in \overline{\sigma} M} C^0_{a_1} \times C^0_{a_2} \times \dots \times C^0_{a_n} = \bigcup_{\overline{a} \in M'} (C^0_{a_{\tau^*(1)}})_{\tau_1} \times (C^0_{a_{\tau^*(2)}})_{\tau_2} \times \dots \times (C^0_{a_{\tau^*(n)}})_{\tau_n}.$$

Then, by Proposition 3 (b), we obtain

$$\bigcup_{\overline{a} \in \overline{\sigma} M} C^0_{a_1} \times C^0_{a_2} \times \dots \times C^0_{a_n} = \bigcup_{\overline{a} \in M'} C^0_{\sigma'_1(a_{\tau^*(1)})} \times C^0_{\sigma'_2(a_{\tau^*(2)})} \times \dots \times C^0_{\sigma'_n(a_{\tau^*(n)})}$$
$$= \bigcup_{\overline{a} \in \overline{\sigma'}(M'_{\tau^*})} C^0_{a_1} \times C^0_{a_2} \times \dots \times C^0_{a_n}.$$

Thus, $\overline{\sigma} M = \overline{\sigma'}(M'_{\tau^*})$, i.e., the MDS-codes M and M' are equivalent. Proposition 4 is proved. □

We call by an *orthogonal complement to the code* $A \subseteq E^n$ the linear space

$$A^\perp = \{\overline{x} \in E^n \mid \langle \overline{x}, \overline{y} \rangle = 0 \text{ for all } \overline{y} \in A\}.$$

It is known that the orthogonal complement $R^\perp$ to the linear code $R \subseteq E^n$ is the Hadamard code and it has dimension $\log_2 n + 1$. Here and in the sequel $\log n = \log_2 n$.

Put $r^4 = (rrrr)$, where $r \in \{0, 1\}$, and, for a vertex $\overline{p} \in E^n$, $\overline{p}^4 = (p^4_1, p^4_2, \dots, p^4_n)$. Let $\overline{p} \in R^\perp$. Then $\overline{p}^4 \in C^\perp$, where the code C is defined by (1). Obviously, the set $R^{\perp 4} = \{\overline{p}^4 \mid \overline{p} \in R^\perp\}$ is a linear subspace of dimension $\log n + 1$ of $C^\perp$. It was shown in [4] that the dimension of $C^\perp$ must be equal to either $\log n + 1$, or $\log n + 2$, or $\log n + 3$; and in the last case the extended perfect code C is linear.

Proposition 5. *Let* $\tau, \pi \in S_{4n}$. *If* $(R^{\perp 4})_\tau = (R^{\perp 4})_\pi$ *then* $I_\tau = I_\pi$.

Proof. Without loss of generality, we may assume that π is the identity permutation.

Let $I_\tau \neq I$. Without loss of generality we may assume that the permutation τ sends to the first and second positions the elements from different members of the partition, i.e., $\tau^{-1}(1) \in I(i)$ and $\tau^{-1}(2) \in I(j)$, where $i \neq j$. From the well-known property of the Hadamard code we find a vertex $\overline{p} \in R^\perp$ such that $p_i \neq p_j$. Let $\overline{v} = \overline{p}^4_\tau$. Then the choice of $\overline{p}$ implies that $v_1 \neq v_2$. Hence $\overline{v} \notin R^{\perp 4}$. Proposition 5 is proved. □

Let $M(C)$ be the set of the MDS-codes that correspond to the codes equivalent to the extended perfect code C, i.e., $M' \in M(C)$ if there exists an extended perfect normalized code C' that is equivalent to C and satisfies the equality (1) with the MDS-code M'.

The formulation and proof of the following lemma belong to D. S. Krotov.

Lemma 2. *Let C be a nonlinear extended perfect code of length* $4n$ *satisfying* (1). *Then* $M(C)$ *contains at most* $2n - 1$ *equivalence classes of* MDS-*codes.*

Proof. Let M' and M'' be nonequivalent MDS-codes of $M(C)$. Then there exist codes C' and C'' satisfying (1) with the MDS-codes M' and M'' respectively and, moreover,

$$C'_{\tau'} + \overline{y} = C = C''_{\tau''} + \overline{z} \tag{4}$$

for some permutations $\tau', \tau'' \in S_{4n}$ and vertices $\overline{y}, \overline{z} \in C$.

It follows from Proposition 4 that $I_{\tau'} \neq I_{\tau''}$, and Proposition 5 implies

$$(R^{\perp 4})_{\tau''} \neq (R^{\perp 4})_{\tau'}. \tag{5}$$

By (4), we see that $(C'^{\perp})_{\tau'} = (C''^{\perp})_{\tau''} = C^{\perp}$. Therefore, $(R^{\perp 4})_{\tau''} \subseteq C^{\perp}$ and $(R^{\perp 4})_{\tau'} \subseteq C^{\perp}$; moreover, as it was noted earlier, the dimension of $(R^{\perp 4})$ is $\log n + 1$, and the dimension of $C^{\perp}$ is $\log n + 2$ (the dimension $\log n + 1$ is impossible by (5), and $\log n + 3$ is impossible by nonlinearity of C).

The linear code R is contained in $E^n_{2,0}$; hence, $\overline{1} \in R^{\perp}$. The number of possible choices of distinct hypersubspaces in $C^{\perp}$, containing the vertex $\overline{1}$, is equal to one-half of the size of $C^{\perp}$ minus 1; i.e., $2n-1$. Since for each pair of the nonequivalent MDS-codes M' and M'' there exists a pair of distinct hypersubspaces in $C^{\perp}$, the set $M(C)$ splits at most into $2n-1$ equivalence classes. Lemma 2 is proved. ◻

4. THE NUMBER OF TRANSITIVE CODES

Define on the set E_4 the following binary operations: We will denote by $\oplus$ the addition that is isomorphic to the addition in the group $Z_2 \times Z_2$; and by $*$, the addition isomorphic to the addition in the group Z_4. The tables of these operations are as follows:

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

$\oplus$	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 are well known and easily verified:

Proposition 6. *There are no permutations $\sigma_0, \sigma_1, \sigma_2 \in S_4$ such that $\sigma_0(\sigma(x_1) * \sigma(x_2)) = x_1 \oplus x_2$.*

Proposition 7. (a) *The n-quasigroup $f(x_1, x_2, \ldots, x_n) = x_1 * x_2 * \cdots * x_n$ is isotopically transitive.*

(b) *The n-quasigroup $h(x_1, x_2, \ldots, x_n) = x_1 \oplus x_2 \oplus \cdots \oplus x_n$ is isotopically transitive. Moreover, for every vertex $\overline{a} \in E_4^n$ and each permutation $\sigma_0 \in S_4$ such that $\sigma_0(0) = h(\overline{a})$, there exists a family of permutations $\overline{\sigma} \in S_4^n$ for which the equalities $\overline{\sigma}\overline{0} = \overline{a}$ and $h(\overline{\sigma x}) = \sigma_0(h(\overline{x}))$ hold.*

Proof. (a) Let $a_1 * a_2 * \cdots * a_n = a_0$. Let $\sigma_i(y) = y * a_i$ for all $i = 0, \ldots, n$. The associativity and commutativity of $*$ imply the equality

$$f(\overline{\sigma x}) = (x_1 * a_1) * (x_2 * a_2) * \cdots * (x_n * a_n) = x_1 * x_2 * \cdots * x_n * a_0 = \sigma_0(f(\overline{x})).$$

(b) Let $\varphi \in S_4$ be such that $\varphi(0) = 0$. We will show that

$$\varphi(a) \oplus \varphi(b) = \varphi(a \oplus b) \tag{6}$$

for arbitrary $a, b \in E_4$. Consider the three cases:

1) If $a = 0$ ($b = 0$) then $\varphi(0) \oplus \varphi(b) = \varphi(b \oplus 0)$.

2) If $a = b$ then $\varphi(a) \oplus \varphi(a) = 0 = \varphi(0) = \varphi(a \oplus a)$.

3) Let $a \neq 0, b \neq 0$, and $a \neq b$. Denote by c the forth element of E_4 ($a \neq c$, $b \neq c$, and $0 \neq c$). We see from the table for operation $\oplus$ that $a \oplus b \notin \{a, b, 0\}$ and $\varphi(a) \oplus \varphi(b) \notin \{\varphi(a), \varphi(b), 0\}$, i.e., $a \oplus b = c$ and $\varphi(a) \oplus \varphi(b) = \varphi(c)$.

Let $a_1 \oplus a_2 \oplus \dots \oplus a_n = a_0$. For the permutation $\sigma_0 \in S_4$ ($\sigma_0(0) = a_0$), we define the permutation $\varphi(y) = \sigma_0(y) \oplus a_0$. It is clear that $\varphi(0) = 0$. Let $\sigma_i(y) = \varphi(y) \oplus a_i$ for all $i = 1, \dots, n$. Then, by (6), we have

$$h(\overline{\sigma x}) = (\varphi(x_1) \oplus a_1) \oplus (\varphi(x_2) \oplus a_2) \oplus \dots \oplus (\varphi(x_n) \oplus a_n) = \varphi(h(\overline{x})) \oplus a_0 = \sigma_0(h(\overline{x})).$$

Proposition 7 is proved. □

Proposition 8. *Let f be an isotopically transitive n-quasigroup and*

$$h(y_1, y_2, \dots, y_m) = y_1 \oplus y_2 \oplus \dots \oplus y_m.$$

Then the $(n+m-1)$-quasigroup $f(x_1, \dots, x_{i-1}, h(\overline{y}), x_{i+1}, \dots, x_n)$ is isotopically transitive.

Proof. Without loss of generality, we assume that $i = n$. Let $\overline{b} \in E_4^m$, $h(\overline{b}) = a_n$, and $\overline{a} \in E_4^n$. The assumptions imply that there exist permutations $\overline{\sigma} \in S_4^n$ and $\sigma_0 \in S_4$ satisfying the equations $\overline{\sigma}\overline{0} = \overline{a}$, $\sigma_0(0) = f(\overline{a})$, and $f(\overline{\sigma x}) = \sigma_0(f(\overline{x}))$ for all $\overline{x} \in E_4^n$. It follows from Proposition 7 that there exists a family of permutations $\overline{\tau} \in S_4^m$ such that $h(\overline{\tau y}) = \sigma_n(h(\overline{y}))$ and $\overline{\tau}\overline{0} = \overline{b}$. Then

$$\begin{aligned} f(\sigma_1(x_1), \dots, \sigma_{n-1}(x_{n-1}), h(\overline{\tau y})) &= f(\sigma_1(x_1), \dots, \sigma_{n-1}(x_{n-1}), \sigma_n(h(\overline{y}))) \\ &= \sigma_0(f(x_1, \dots, x_{n-1}, h(\overline{y}))). \end{aligned}$$

Proposition 8 is proved. □

Lemma 3. *Let $p(n)$ be the number of distinct representations of n as a nonordered sum of some positive integers. Then the number of equivalence classes of isotopically transitive* MDS*-codes of length $n+1$ is at least $p(n)$.*

Proof. Let $\{x_1, x_2, \dots, x_n\}$ be the set of coordinates. Consider a partition $J = \{J(1), J(2), \dots, J(k)\}$. By the *specter* of the partition, we call the vector $Sp(J) = (|J(i_1)|, |J(i_2)|, \dots, |J(i_k)|)$, where $|J(i_1)| \le |J(i_2)| \le \dots \le |J(i_k)|$. Define the function

$$h(\widetilde{x}_{J(i)}) = x_{j_1} \oplus \dots \oplus x_{j_{|J(i)|}},$$

where $J(i) = \{j_1, \dots, j_{|J(i)|}\}$ and $g_J(\overline{x}) = h(\widetilde{x}_{J(1)}) * h(\widetilde{x}_{J(2)}) * \dots * h(\widetilde{x}_{J(k)})$. We will prove by contradiction that distinction of the specters $Sp(J) \ne Sp(I)$ implies nonequivalence of the MDS-codes $G(g_J)$ and $G(g_I)$. Assume that there exist the permutations $\tau \in S_{n+1}$ and $\overline{\sigma} \in S_4^{n+1}$ such that

$$\{(x_1, x_2, \dots, x_{n+1}) \mid g_J(\overline{\sigma x}) = \sigma_{n+1}(x_{n+1})\} = \{(x_1, x_2, \dots, x_{n+1}) \mid g_I(\overline{x}_\tau) = x_{\tau(n+1)}\}.$$

Without loss of generality we can set $|I| \le |J|$. Since $Sp(J) \ne Sp(I)$, there exist variables x_i and x_j from two different elements of the partition J such that $x_{\tau^{-1}(i)}$ and $x_{\tau^{-1}(j)}$ belong to the same element of I. In the equalities $g_J(\overline{\sigma x}) = \sigma_{n+1}(x_{n+1})$ and $g_I(\overline{x}_\tau) = x_{\tau(n+1)}$, we substitute zeros for all variables, but x_i, x_j, and x_{n+1}. From the first equality, we obtain $\sigma_i(x_i) * \sigma_j(x_j) * c = \sigma_{n+1}(x_{n+1})$, where $c \in E_4$, or, in other form,

$$\sigma_0(\sigma_i(x_i) * \sigma_j(x_j)) = x_{n+1}, \tag{7}$$

where $\sigma_0 \in S_4$. From the second equality, in dependence on which element of the partition I contains the variable $x_{\tau^{-1}(n+1)}$, we obtain

$$x_i \oplus x_j = x_{n+1}, \quad \text{or} \quad x_i \oplus x_j \oplus x_{n+1} = 0, \quad \text{or} \quad (x_i \oplus x_j) * x_{n+1} = 0.$$

By Proposition 6, each of these equalities contradicts (7). This implies that (7) is false.

Propositions 7 and 8 imply the translational transitivity of the MDS-codes $G(g_I)$ for an arbitrary partition I. The MDS-codes corresponding to distinct specters are nonequivalent. It is clear that the number of distinct specters $Sp(I)$ equals $p(n)$. Lemma 3 is proved. □

Now, we estimate the number of nonequivalent transitive extended perfect codes.

Proof of the theorem. It follows from Lemma 3 that there are $p(n-1)$ pairwise nonequivalent isotopically transitive MDS-codes of length n. Lemma 1 implies that, inserting any of these MDS-codes in (1), we obtain a transitive extended perfect code of length $4n$. It is easy to see that among these codes the only perfect extended code, which corresponds to the n-quasigroup $h(\overline{x}) = x_1 \oplus x_2 \oplus \cdots \oplus x_{n-1}$, is linear. Then Lemma 2 implies that at most $2n-1$ extended perfect codes constructed above may be found in the same equivalence class. It was shown in [3] that

$$p(n) = \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{2n/3}}(1+o(1)) \text{ as } n \to \infty.$$

Hence, as $n \to \infty$, there exist at least

$$\frac{p(n-1)-1}{2n-1} = \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{2n/3}}(1+o(1))$$

pairwise nonequivalent transitive extended perfect codes of length $4n$. The theorem is proved. □

ACKNOWLEDGMENTS

The author was supported by the Russian Foundation for Basic Research (project no. 05–01–00364).

REFERENCES

1. S. A. Malyugin, "On Transitive Perfect Codes of Length 15," in *Proceedings of the Conference on Discrete Analysis and Studies of Operations* (Sobolev Inst. Mat., Novosibirsk, 2004), p. 96.
2. F. I. Solov'eva, "On Construction of Transitive Codes," Problemy Peredachi Informatsii **41** (3), 23–31 (2005).
3. G. E. Andrews, *The Theory of Partitions* (Addison-Wesley, London, 1976).
4. S. V. Avgustinovich, O. Heden, and F. I. Solov'eva, "The Classification of Some Perfect Codes," Design Codes Cryptogr. **31** (3), 313–318 (2004).
5. K. Phelps, "A General Product Construction for Error Correcting Codes," SIAM J. Algebraic and Discrete Methods **5** (2), 224–228 (1984).
6. V. A. Zinoviev, "On Generalized Concatenated Codes," in *Topics in Information Theory. Colloq. Math. Soc. J. Bolyai*, Ed. by I. Csiszar and P. Elias (North-Holland, Amsterdam, 1977), pp. 587–592.