ISSN 0032-9460, Problems of Information Transmission, 2009, Vol. 45, No. 4, pp. 309–316. © Pleiades Publishing, Inc., 2009.
Original Russian Text © E.V. Gorkunov, 2009, published in Problemy Peredachi Informatsii, 2009, Vol. 45, No. 4, pp. 18–25.

CODING THEORY

The Group of Permutation Automorphisms of a q-ary Hamming Code

E. V. Gorkunov

Novosibirsk State University
evgumin@gmail.com

Received May 30, 2008; in final form, October 15, 2009

Abstract—We prove that the group of permutation automorphism of a q-ary Hamming code of length $n = (q^m - 1)/(q - 1)$ is isomorphic to the unitriangular group $\mathbf{UT}_m(q)$ if the code has a parity-check matrix composed of all columns of the form $(0 \dots 0\, 1 * \dots *)^{\mathsf{T}}$. We also show that the group of permutation automorphisms of a cyclic Hamming code cannot be isomorphic to $\mathbf{UT}_m(q)$. We thus show that equivalent codes can have different permutation automorphism groups.

DOI: 10.1134/S0032946009040024

1. INTRODUCTION

Let V_q^n be a linear space of dimension n over the Galois field $\mathbb{F}_q = GF(q)$, where $q = p^r$ is a power of a prime p, $r \geq 1$ being an integer. In the literature one can find several definitions of the automorphism group of a code. Unlike the traditional definition (see, e.g., [1, 2]), the authors of [3] define it as a subgroup of the *whole* isometry group of the space V_q^n that contains the code as a subset. Following the latter definition, in the present paper we study the permutation automorphism group of a q-ary Hamming code.

Studying automorphism groups of codes is one of important lines of investigation in the theory of error-correcting codes. Many presently known facts concern binary codes only. There is a well-known result [4] that every finite group is isomorphic to the permutation automorphism group of some perfect binary code. However, the structure of the complete automorphism group of this code remains unknown. The antipodal property (see [5]) of perfect binary codes implies that the automorphism group of an arbitrary such code contains the identity permutation of coordinates and the translation by the all-one vector $\mathbf{1}$. If the automorphism group of a perfect binary code consists only of these two transformations, it is said to be trivial. In [6, 7], existence of perfect binary codes with trivial automorphism groups was proved. Nonlinear perfect binary codes were first presented in the pioneering work [8]. However, the study of symmetry groups of Vasil'ev codes was started not long ago (see [9]). We may say that [9] deals with the permutation automorphism group, since for binary codes its definition coincides with the definition of the symmetry group.

It is known [1] that the permutation automorphism group of a binary Hamming code $\mathcal{H}_2^n$ of length $n = 2^m - 1$ is isomorphic to the general linear group $\mathbf{GL}_m(2)$. Since the Hamming code is linear, its automorphism group $\mathrm{Aut}(\mathcal{H}_2^n)$ satisfies $\mathrm{Aut}(\mathcal{H}_2^n) = \mathbf{GL}_m(2) \leftthreetimes \mathcal{H}_2^n$, whence we get

$$|\mathrm{Aut}(\mathcal{H}_2^n)| = |\mathbf{GL}_m(2)| \cdot |\mathcal{H}_2^n| = 2^{n-m}(2^m - 1)(2^m - 2) \dots (2^m - 2^{m-1}). \tag{1}$$

In [10] it is shown that the order of the automorphism group of an arbitrary binary perfect code is not greater than the order of the automorphism group of the Hamming code of the same length.

In [11] this result was improved: it was shown that, among binary perfect codes, only the Hamming code has the maximum possible order of the automorphism group, which is given by (1). A similar result was obtained in [12].

In [2, Section 7] one can find a proof of the fact that the general semilinear group $\mathbf{\Gamma L}_m(q)$ is isomorphic to the group of all semilinear[1] automorphisms of a q-ary Hamming code that preserve weights of codewords. In this statement, semilinear bijections on the space V_q^n that preserve weights of codewords are considered as the most general automorphisms of codes. Studying the permutation automorphism group of a code is of interest, since in the general case this group is only known to be a subgroup of the whole automorphism group of the code. Below we show that different Hamming codes of the same length, though are equivalent, may have different permutation automorphism groups. In the present paper we give a characterization of the permutation automorphism group of a Hamming code that has a parity-check matrix composed of all columns with the first nonzero coordinate equal to 1.

2. DEFINITIONS AND NOTIONS

Let us give necessary definitions. The *Hamming distance* $d(x, y)$ between vectors x, y in V_q^n is the number of coordinates in which these vectors differ. An arbitrary subset C of V_q^n is called a *q-ary code* of length n. Elements of C are referred to as *codewords*. If the set of spheres of radius t centered at codewords of C form a partition of the linear space V_q^n, the code is said to be *t-perfect*, or simply *perfect* if this does not cause ambiguity. Throughout what follows, by a perfect code we mean a 1-perfect code. It is commonly known (see [1]) that a nontrivial perfect code over the Galois field $\mathbb{F}_q$ must be of length $n = (q^m - 1)/(q - 1)$ for some integer $m \geq 2$ and of cardinality q^{n-m}.

A code C is *linear* if it forms a linear subspace in V_q^n. Parameters of a linear q-ary code of dimension k with code distance d are briefly written as $[n, k, d]_q$. The only linear perfect codes are Hamming codes. However, as is shown in [13], there exist group perfect q-ary codes that are not equivalent to linear codes.

Recall also that the *general linear group* $\mathbf{GL}_m(q)$ is the group of all nonsingular matrices of order m over $\mathbb{F}_q$. The group of matrices whose entries on the main diagonal are ones and all entries above (below) it are zeros is called the *lower* (*upper*) *unitriangular group* and is denoted by $\mathbf{UT}_m(q)$. The unitriangular groups are isomorphic; the map that takes a lower unitriangular matrix L to the upper unitriangular matrix $R = L^{-\mathsf{T}} = (L^{-1})^{\mathsf{T}}$ defines an isomorphism between the groups.

Let a group G act on a set A; then by $\mathrm{St}_G(T)$ we denote the stabilizer of a subset $T \subset A$ under the action of G on A.

In what follows we consider the action of the general linear group $\mathbf{GL}_m(q)$ on the set of vectors of length m defined by left multiplication of a vector by a matrix.

Now we consider the notion of an automorphism of a code and its particular cases. A map $\varphi\colon V_q^n \to V_q^n$ is called an *isometry* of V_q^n if for any two vectors $x, y \in V_q^n$ we have $d(x, y) = d(\varphi(x), \varphi(y))$.

The action of a permutation $\pi \in S_n$, where S_n is the symmetric group of permutations of order n of the set $\{1, 2, \ldots, n\}$, on an arbitrary vector $x = (x_1, \ldots, x_n)$ of the space V_q^n is defined by

$$\pi(x) = \left(x_{\pi^{-1}(1)}, \ldots, x_{\pi^{-1}(n)}\right).$$

[1] A function f defined on a linear space V^n over a field K is said to be semilinear if in the Galois group $\mathrm{Gal}(K)$ there is an automorphism γ of K such that for any vectors $x, y \in V^n$ and any elements $\alpha, \beta \in K$ we have $f(\alpha x + \beta y) = \gamma(\alpha) f(x) + \gamma(\beta) f(y)$.

Following [3], by a *configuration* we call a map $\sigma\colon V_q^n \to V_q^n$ defined as follows:

$$\sigma(x) = (\sigma_1(x_1), \ldots, \sigma_n(x_n)),$$

where σ_i are permutations from the symmetric group S_q of order q acting on elements of $\mathbb{F}_q$.

In 1956, A.A. Markov [14] proved that the automorphism group of V_q^n is the semidirect product of S_n and the group S_q^n of all configurations of V_q^n; i.e.,

$$\mathrm{Aut}(V_q^n) = S_n \leftthreetimes S_q^n = \{(\pi;\sigma) \mid \pi \in S_n,\ \sigma = (\sigma_1, \ldots, \sigma_n) \in S_q^n\}.$$

In this product, the group S_n naturally acts on S_q^n by permuting components σ_i of an ordered collection σ.

The *automorphism group* of a code C is the group of all isometries of V_q^n that map C onto itself:

$$\mathrm{Aut}(C) = \{(\pi;\sigma) \in \mathrm{Aut}(V_q^n) \mid (\pi;\sigma)(C) = C\}.$$

For a field $\mathbb{F}_q$ with a primitive element α, multiplication of all elements of the field by a nonzero element β is a permutation from S_q of the form

$$\tau_\beta = \begin{pmatrix} 0 & \alpha^0 & \alpha^1 & \ldots & \alpha^{q-2} \\ 0 & \alpha^0\beta & \alpha^1\beta & \ldots & \alpha^{q-2}\beta \end{pmatrix}.$$

Denote the set of all the $q-1$ such permutations by S_q^*. The *monomial automorphism group* of a code C is the set

$$\mathrm{MAut}(C) = \{(\pi;\sigma) \in \mathrm{Aut}(C) \mid \sigma \in (S_q^*)^n\}.$$

Let ε denote the configuration all components of which are identical permutations. It is natural to identify an isometry $(\pi;\varepsilon)$ with the permutation π. The *permutation automorphism group* of a code C is the set

$$\mathrm{PAut}(C) = \{\pi \in \mathrm{Aut}(C)\}.$$

Consider an arbitrary $[n,k,d]_q$ code, i.e., a linear code of length n and dimension k with code distance d. Its generator matrix contains k linearly independent rows. One can easily check the following statement.

Proposition 1. *The monomial automorphism group of an $[n,k,d]_q$ code is isomorphic to a subgroup of $\mathbf{GL}_k(q)$.*

For the binary case, the proof can be found in [1]. If a linear code has large enough dimension ($k > n/2$) and code distance $d \geq 3$, its description via a parity-check matrix yields a stronger statement. It follows from a well-known theorem, which can be found, e.g., in [2].

Theorem 1 (see [2, Theorem 7.1]). *Let C be an $[n,k,d]_q$ code with code distance $d \geq 3$ and with an $m \times n$ parity-check matrix H, where $m = n - k$. Then*

(i) *If $(M;\gamma) \in \mathrm{Aut}(C)$, where M is a monomial $n \times n$ matrix and $\gamma \in \mathrm{Gal}(\mathbb{F}_q)$, then there exists a unique matrix $N \in \mathbf{GL}_m(q)$ such that $N^{\mathsf{T}}H = (H\gamma^{-1})M^{\mathsf{T}}$;*

(ii) *The map $\Theta\colon \mathrm{Aut}(C) \to \mathbf{\Gamma L}_m(q)$ given by $(M;\gamma)\Theta = (N;\gamma)$ on the set of semilinear automorphisms of C is an isomorphism whose image consists of all pairs $(N;\gamma)$ such that the matrices $N^{\mathsf{T}}H$ and $H\gamma^{-1}$ are obtained from each other by multiplying by a monomial matrix.*

Thus, the theorem implies the following result.

Proposition 2. *The monomial automorphism group of a linear $[n,k,d]_q$ code with code distance $d \geq 3$ and with an $m \times n$ parity-check matrix, where $m = n - k$, is isomorphic to a subgroup of $\mathbf{GL}_m(q)$.*

Another consequence of Theorem 1 is as follows.

Proposition 3. *If C is a linear $[n,k,d]_q$ code with code distance $d \geq 3$ and with an $m \times n$ parity-check matrix H whose columns form a set T, then*

$$\mathrm{PAut}(C) \cong \mathrm{St}_{\mathbf{GL}_m(q)}(T).$$

3. DESCRIPTION OF THE GROUP $\mathrm{PAut}(\mathcal{H}_q^n)$

We investigate the permutation automorphism group of a q-ary Hamming code defined by a parity-check matrix consisting of all nonzero vectors whose first nonzero coordinate is 1. Below we need the following inductive definition for the parity-check matrix H_m of the Hamming code $\mathcal{H}_q^n$ of length $n = \dfrac{q^m-1}{q-1}$. In the case of $m = 2$, we have

$$H_2 = \begin{pmatrix} 0 & 1 & 1 & 1 & \dots & 1 \\ 1 & 0 & \alpha^0 & \alpha^1 & \dots & \alpha^{q-2} \end{pmatrix}.$$

For an arbitrary m, the parity-check matrix H_{m+1} of the Hamming code of length $nq+1$ is defined via the parity-check matrix $H_m = \begin{pmatrix} h_1 & h_2 & \dots & h_n \end{pmatrix}$ of a code of length n as follows:

$$H_{m+1} = \begin{pmatrix} \mathbf{0} & h_1 & h_1 & h_1 & \dots & h_1 & \dots & h_n & h_n & h_n & \dots & h_n \\ 1 & 0 & \alpha^0 & \alpha^1 & \dots & \alpha^{q-2} & \dots & 0 & \alpha^0 & \alpha^1 & \dots & \alpha^{q-2} \end{pmatrix},$$

where $\mathbf{0}$ is the all-zero vector of length m.

Denote by T_m the set of columns of the parity-check matrix H_m. We have the following fact.

Lemma 1. *Any matrix $L \in \mathbf{UT}_m(q)$ defines a bijection on the set T_m.*

Proof. If we use left multiplication of vectors by the matrix L, then, to obtain the bijection on T_m, we should consider lower unitriangular matrices (in contrast to right multiplication by an upper unitriangular matrix). For an arbitrary vector h in T_m, define a map $\varphi\colon T_m \to V_q^m$ according to the rule

$$\varphi(h) = Lh.$$

Note that the set T_m is finite. Since $\det L \neq 0$, φ is injective. Therefore, it suffices to show that $\varphi(T_m) \subset T_m$.

Let $h = (0 \ \dots \ 0 \ 1 \ \xi_{j+1} \ \dots \ \xi_m)^{\mathsf{T}} \in T_m$, where $\xi_{j+1}, \dots, \xi_m \in \mathbb{F}_q$. Then

$$\varphi(h) = Lh = \begin{pmatrix} 1 & \dots & 0 & 0 & 0 & \dots & 0 \\ & \ddots & \vdots & \vdots & \vdots & & \vdots \\ & & 1 & 0 & 0 & \dots & 0 \\ & & & 1 & 0 & \dots & 0 \\ & * & & & 1 & \dots & 0 \\ & & & & & \ddots & \vdots \\ & & & & & & 1 \end{pmatrix} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ \xi_{j+1} \\ \vdots \\ \xi_m \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ \psi_{j+1} \\ \vdots \\ \psi_m \end{pmatrix},$$

where $\psi_i = \ell_{ij} + \sum\limits_{k=j+1}^{i-1} \ell_{ik}\xi_k + \xi_i$, $i = j+1, j+2, \dots, m$.

Thus, $\varphi(h) \in T_m$, which proves the lemma. $\triangle$

In the next lemma we show that in the general linear group $\mathbf{GL}_m(q)$ there are no bijections on T_m other than those described in Lemma 1.

Lemma 2. *If a matrix U belongs to $\mathbf{GL}_m(q) \setminus \mathbf{UT}_m(q)$, where $m \geq 1$ and $q > 2$, then in the set T_m there is a vector h such that $Uh \notin T_m$.*

Proof. We consider the result of left multiplication of the parity-check matrix H_m of the Hamming code by the matrix U and prove the lemma by induction on m.

For $m = 1$, the claim of the lemma trivially follows from the equalities $UH_1 = \begin{pmatrix} u_{11} \end{pmatrix} \begin{pmatrix} 1 \end{pmatrix} = \begin{pmatrix} u_{11} \end{pmatrix}$, since $u_{11} \neq 0$ and $u_{11} \neq 1$. Though this is sufficient for the induction basis, we give a proof for the case $m = 2$, since this case illustrates the essence of the proof in detail.

Let $m = 2$. If $U = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}$, then multiplying U by H_2 results in

$$\begin{aligned} UH_2 &= \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 & 1 & \dots & 1 \\ 1 & 0 & \alpha^0 & \alpha^1 & \dots & \alpha^{q-2} \end{pmatrix} \\ &= \begin{pmatrix} u_{12} & u_{11} & u_{11} + \alpha^0 u_{12} & u_{11} + \alpha^1 u_{12} & \dots & u_{11} + \alpha^{q-2} u_{12} \\ u_{22} & u_{21} & u_{21} + \alpha^0 u_{22} & u_{21} + \alpha^1 u_{22} & \dots & u_{21} + \alpha^{q-2} u_{22} \end{pmatrix}. \end{aligned}$$

Depending on the form of the matrix U, the following cases are possible.

1. If $u_{11} \neq 0$ and $u_{11} \neq 1$, then

$$U \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} u_{11} \\ u_{21} \end{pmatrix} \notin T_2, \quad \text{and the desired vector } h \text{ is } \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

2. If $u_{11} = 0$ or $u_{11} = 1$, but $u_{12} \neq 0$, then the set

$$\left\{ u_{11}, u_{11} + \alpha^0 u_{12}, u_{11} + \alpha^1 u_{12}, \dots, u_{11} + \alpha^{q-2} u_{12} \right\}$$

coincides with the set of all elements of $\mathbb{F}_q$. Therefore, for $q > 2$ there exists an integer ℓ in the range $[0, q-2]$ such that

$$u_{11} + \alpha^\ell u_{12} \neq 0 \qquad \text{and} \qquad u_{11} + \alpha^\ell u_{12} \neq 1.$$

Then

$$U \begin{pmatrix} 1 \\ \alpha^\ell \end{pmatrix} = \begin{pmatrix} u_{11} + \alpha^\ell u_{12} \\ u_{21} + \alpha^\ell u_{22} \end{pmatrix} \notin T_2, \quad \text{and therefore } h = \begin{pmatrix} 1 \\ \alpha^\ell \end{pmatrix}.$$

3. If $u_{11} = 1$ and $u_{12} = 0$, then the condition $\det U \neq 0$ implies $u_{22} \neq 0$, and taking into account that $U \notin \mathbf{UT}_2(q)$, we find $u_{22} \neq 1$. Hence,

$$U \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ u_{22} \end{pmatrix} \notin T_2, \quad \text{and} \quad h = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

4. Finally, the equalities $u_{11} = u_{12} = 0$ are impossible since $\det U \neq 0$.

Thus, the lemma holds for $m = 2$ too.

Now we prove the lemma for matrices of order $m + 1$ under the assumption that it holds for matrices of order m. We represent a matrix U of order $m + 1$ in the form

$$U = \begin{pmatrix} \widetilde{U} & b \\ c & \beta \end{pmatrix},$$

where $\widetilde{U}$ is a submatrix of order m, the last column contains a column vector b of length m, the last row contains a row vector c of length m, and the entry at their intersection is an element β of $\mathbb{F}_q$.

Then

$$UH_{m+1} = \begin{pmatrix} \widetilde{U} & b \\ c & \beta \end{pmatrix} \begin{pmatrix} \mathbf{0} & h_1 & h_1 & \dots & h_1 & \dots & h_n & h_n & \dots & h_n \\ 1 & 0 & \alpha^0 & \dots & \alpha^{q-2} & \dots & 0 & \alpha^0 & \dots & \alpha^{q-2} \end{pmatrix}$$
$$= \begin{pmatrix} b & \widetilde{U}h_1 & \widetilde{U}h_1 + \alpha^0 b & \dots & \widetilde{U}h_1 + \alpha^{q-2}b & \dots & \widetilde{U}h_n & \widetilde{U}h_n + \alpha^0 b & \dots & \widetilde{U}h_n + \alpha^{q-2}b \\ \beta & ch_1 & ch_1 + \alpha^0\beta & \dots & ch_1 + \alpha^{q-2}\beta & \dots & ch_n & ch_n + \alpha^0\beta & \dots & ch_n + \alpha^{q-2}\beta \end{pmatrix}.$$

Similarly to the proof of the lemma for $m = 2$, the following four cases are possible, each of them imposing certain conditions on U.

1. If $\det \widetilde{U} \neq 0$ and $\widetilde{U} \notin \mathbf{UT}_m(q)$, then by the induction hypothesis there is a vector $h_j \in T_m$ such that $\widetilde{U}h_j \notin T_m$. Then

$$U \begin{pmatrix} h_j \\ 0 \end{pmatrix} = \begin{pmatrix} \widetilde{U}h_j \\ ch_j \end{pmatrix} \notin T_{m+1}, \quad \text{and therefore } h = \begin{pmatrix} h_j \\ 0 \end{pmatrix}.$$

2. Let $\det \widetilde{U} = 0$ or $\widetilde{U} \in \mathbf{UT}_m(q)$, but $b \neq \mathbf{0}$. In this case the vector b is collinear to one of the vectors of T_m; i.e., for some $\gamma \in \mathbb{F}_q$ and $h_k \in T_m$ we have $b = \gamma h_k$.

Then we have two possibilities:

(a) If $\det \widetilde{U} = 0$, then there exists a vector h_j in T_m such that $\widetilde{U}h_j = \mathbf{0}$;
(b) If $\widetilde{U} \in \mathbf{UT}_m(q)$, then by Lemma 1 in the set T_m there is a vector h_j that is taken to h_k by the action of $\widetilde{U}$, i.e., $\widetilde{U}h_j = h_k$.

Anyhow, in the matrix UH_{m+1} we can select a submatrix

$$\begin{pmatrix} \delta h_k & (\delta + \alpha^0\gamma)h_k & (\delta + \alpha^1\gamma)h_k & \dots & (\delta + \alpha^{q-2}\gamma)h_k \\ ch_j & ch_j + \alpha^0\beta & ch_j + \alpha^1\beta & \dots & ch_j + \alpha^{q-2}\beta \end{pmatrix},$$

where δ is either 0 or 1 (accordingly to the cases (a) and (b)). Since the set

$$\left\{\delta, \delta + \alpha^0\gamma, \delta + \alpha^1\gamma, \dots, \delta + \alpha^{q-2}\gamma\right\}$$

coincides with the field $\mathbb{F}_q$, for $q > 2$ there exists an integer $\ell \in [0, q-2]$ such that

$$\delta + \alpha^\ell\gamma \neq 0 \qquad \text{and} \qquad \delta + \alpha^\ell\gamma \neq 1.$$

Then

$$U \begin{pmatrix} h_j \\ \alpha^\ell \end{pmatrix} = \begin{pmatrix} (\delta + \alpha^\ell\gamma)h_k \\ ch_j + \alpha^\ell\beta \end{pmatrix} \notin T_{m+1}, \quad \text{and} \quad h = \begin{pmatrix} h_j \\ \alpha^\ell \end{pmatrix}.$$

3. If $\widetilde{U} \in \mathbf{UT}_m(q)$ and $b = \mathbf{0}$, then from $\det U \neq 0$ we get $\beta \neq 0$, and since $U \notin \mathbf{UT}_{m+1}(q)$, we have $\beta \neq 1$. Hence,

$$U \begin{pmatrix} \mathbf{0} \\ 1 \end{pmatrix} = \begin{pmatrix} \mathbf{0} \\ \beta \end{pmatrix} \notin T_{m+1}, \quad \text{and therefore we may take } h = \begin{pmatrix} \mathbf{0} \\ 1 \end{pmatrix}.$$

4. It remains to note that the conditions $\det \widetilde{U} = 0$ and $b = \mathbf{0}$ cannot hold simultaneously, since this contradicts the inequality $\det U \neq 0$.

Thus, all cases are considered, and Lemma 2 is proved. $\triangle$

Now we can state the main result of the paper, which describes the permutation automorphism group of a q-ary Hamming code that has a parity-check matrix of the form specified above.

Theorem 2. *For any Hamming code of length* $n = \dfrac{q^m - 1}{q - 1}$, *where* $m \geq 2$ *and* $q > 2$, *that has a parity-check matrix consisting of columns of the form* $(0 \ldots 0\, 1 * \ldots *)^{\mathsf{T}}$, *we have*

$$\mathrm{PAut}(\mathcal{H}_q^n) \cong \mathbf{UT}_m(q).$$

Proof. It is known [2] that $\mathrm{MAut}(\mathcal{H}_q^n) \cong \mathbf{GL}_m(q)$. This isomorphism $\theta\colon \mathrm{MAut}(\mathcal{H}_q^n) \to \mathbf{GL}_m(q)$ can be defined as

$$\theta\colon M \mapsto K, \quad \text{where} \quad KH_m = H_m M^{-\mathsf{T}}.$$

Here, H_m is the parity-check matrix of the Hamming code $\mathcal{H}_q^n$, M is a monomial matrix of order n, and K is a matrix from $\mathbf{GL}_m(q)$. In the case where the monomial matrix is a permutation matrix P, the last equality takes the form

$$KH_m = H_m P^{-\mathsf{T}} = H_m P.$$

Hence, using Lemmas 1 and 2, we find the image of the permutation automorphism group of the Hamming code under the isomorphism θ; namely, $\theta(\mathrm{PAut}(\mathcal{H}_q^n)) = \mathbf{UT}_m(q)$. Hence, the restriction of θ to the permutation automorphism group, i.e., the map $\varphi = \theta|_{\mathrm{PAut}(\mathcal{H}_q^n)}$, is an isomorphism between $\mathrm{PAut}(\mathcal{H}_q^n)$ and $\mathbf{UT}_m(q)$. $\triangle$

Remark. The following example demonstrates the importance of the condition imposed on the parity-check matrix in Theorem 2. Consider a cyclic Hamming code $\mathcal{H}_q^n$ (such a code exists if n and $q - 1$ are relatively prime [1, ch. 7, Exercise 8]). Note that the permutation automorphism group of such a code contains a subgroup of order $n = q^{m-1} + \ldots + q + 1$, generated by cyclic shifts of coordinates of codewords. At the same time, $|\mathbf{UT}_m(q)| = q^{\frac{m(m-1)}{2}}$. Since $q = p^r$ and n is not divisible by p, the group $\mathbf{UT}_m(q)$ cannot contain a subgroup of order n. The simplest example is the Hamming code $\mathcal{H}_4^5$ with the parity-check matrix $H_2 = \begin{pmatrix} 0 & 1 & \alpha & \alpha & 1 \\ 1 & \alpha & \alpha & 1 & 0 \end{pmatrix}$. Exhaustive search easily shows that $|\mathrm{PAut}(\mathcal{H}_4^5)| = 10$, while, clearly, $|\mathbf{UT}_2(4)| = 4$. Thus, permutation automorphism groups of Hamming codes of the same length can be different, despite the fact that all these codes are monomially equivalent.

The author is deeply grateful to Prof. F.I. Solov'eva for posing the problem, valuable remarks, and permanent assistance in the work on this paper.

REFERENCES

1. MacWilliams, F.J. and Sloane, N.J.A., *The Theory of Error-Correcting Codes*, Amsterdam: North-Holland, 1977. Translated under the title *Teoriya kodov, ispravlyayushchikh oshibki*, Moscow: Svyaz', 1979.

2. Huffman, W.C., Codes and Groups, *Handbook of Coding Theory*, Pless, V.S. and Huffman, W.C., Eds., Amsterdam: Elsevier, 1998, ch. 6, pp. 1345–1440.

3. Constantinescu, I. and Heise, W., On the Conept of Code-Isomorphy, *J. Geom.*, 1996, vol. 57, no. 1–2, pp. 63–69.

4. Phelps, K.T., Every Finite Group Is the Automorphism Group of Some Perfect Code, *J. Combin. Theory, Ser. A*, 1986, vol. 43, no. 1, pp. 45–51.

5. Shapiro, G.S. and Slotnik, D.L., On the Mathematical Theory of Error Correcting Codes, *IBM J. Res. Dev.*, 1959, vol. 3, pp. 68–72.

6. Avgustinovich, S.V. and Solov'eva, F.I., Perfect Binary Codes with Trivial Automorphism Group, in *Proc. Int. Workshop on Inf. Theory, Killarney, Ireland, 1998*, pp. 114–115.

7. Malyugin, S.A., Perfect Codes with Trivial Automorphism Group, *Proc. 2nd Int. Workshop on Optimal Codes and Related Topics, Sozopol, Bulgaria, 1998*, Sofia, 1998, pp. 163–167.

8. Vasil'ev, Yu.L., On Nongroup Closely Packed Codes, *Probl. Kibern.*, 1962, vol. 8, pp. 337–339.

9. Avgustinovich, S.V., Solov'eva, F.I., and Heden, O., On the Structure of Symmetry Groups of Vasil'ev Codes, *Probl. Peredachi Inf.*, 2005, vol. 41, no. 2, pp. 42–49 [*Probl. Inf. Trans.* (Engl. Transl.), 2005, vol. 41, no. 2, pp. 105–112].

10. Solov'eva, F.I. and Topalova, S.T., On Automorphism Groups of Perfect Binary Codes and Steiner Triple Systems, *Probl. Peredachi Inf.*, 2000, vol. 36, no. 4, pp. 53–58 [*Probl. Inf. Trans.* (Engl. Transl.), 2000, vol. 36, no. 4, pp. 331–335].

11. Solov'eva, F.I. and Topalova, S.T., Perfect Binary Codes and Steiner Triple Systems with Maximal Orders of Automorphism Groups, *Diskretn. Anal. Issled. Oper., Ser. 1*, 2000, vol. 7, no. 4, pp. 101–110.

12. Malyugin, S.A., On the Order of Automorphism Group of Perfect Binary Codes, *Diskretn. Anal. Issled. Oper., Ser. 1*, 2000, vol. 7, no. 4, pp. 91–100.

13. Lindström, B., On Group and Nongroup Perfect Codes in q Symbols, *Math. Scand.*, 1969, vol. 25, pp. 149–158.

14. Markov, A.A., On Transformations without Error Propagation, *Izbrannye trudy* (Selected Works), vol. II: *Teoriya algorifmov i konstruktivnaya matematika. Matematicheskaya logika. Informatika i smezhnye voprosy* (Theory of Algorithms and Constructive Mathematics. Mathematical Logic. Information Science and Related Topics), Nagornyi, N.M., Ed., Moscow: MCCME, 2003, pp. 70–93.