Eleventh International Workshop on Algebraic and Combinatorial Coding Theory
June 16-22, 2008, Pamporovo, Bulgaria *pp. 119-124*

On permutation automorphism groups of q-ary Hamming codes

Evgeny V. Gorkunov evgumin@gmail.com
Novosibirsk State University, RUSSIA

Abstract. It is established that for any $q > 2$ the permutation automorphism group of a q-ary Hamming code of length $n = (q^m - 1)/(q - 1)$ is isomorphic to the unitriangular group $\mathbf{UT}_m(q)$.

1 Introduction

Let $\mathbb{F}_q^n$ be a vector space of dimension n over $GF(q)$ where q is a prime power. In contrast to the traditional code automorphism group definitions considered in [1, 2], all transformations of the space $\mathbb{F}_q^n$ are taken into consideration in the papers [3–8]. In this paper, following the approach started in [3–8] we prove that the permutation automorphism group of a q-ary Hamming code of length $n = (q^m - 1)/(q - 1)$ is isomorphic to the unitriangular group $\mathbf{UT}_m(q)$.

The study of codes automorphism groups is an important topic in the theory of error-correcting codes. Almost all obtained results on the topic concern binary codes. Phelps in [9] established that every finite group is isomorphic to the full permutation automorphism group of some perfect binary code. Unfortunately, the result does not elucidate the structure of the full automorphism group of the code. It is proved in [4, 5] that there exist perfect binary codes with trivial automorphism groups. The permutation automorphism group of well-known Vasil'ev code was investigated in the paper [8].

It is well known (see [1]) that the permutation automorphism group of the binary Hamming code $\mathcal{H}_2^n$ of length $n = 2^m - 1$ is isomorphic to the general linear group $\mathbf{GL}_m(2)$. Solov'eva and Topalova (see [6]) showed that the order of the automorphism group of an arbitrary perfect binary code is not greater than the order of the automorphism group of the Hamming code with the same length. In addition, these authors in [7] established that the only perfect binary code that has an automorphism group of maximal order within all perfect binary codes of the same length is the Hamming code. A similar result was independently obtained by Malyugin in [10]. Semilinear automorphisms of a q-ary Hamming code that preserve the Hamming weight are investigated in [2, Sec. 7].

The Hamming distance $d(x, y)$ between vectors $x, y \in \mathbb{F}_q^n$ is the number of coordinates where x and y differ. Any subset C of the space $\mathbb{F}_q^n$ is a *q-ary code*

of length n. If for some $e \geq 0$ every $x \in \mathbb{F}_q^n$ is within the distance e from exactly one codeword of C, then the code C is called *e-perfect* (in the sequel simply *perfect*). It is well known (see [1]) that nontrivial perfect codes over $\mathbb{F}_q$ must have length $n = (q^m - 1)/(q - 1)$ for some integer $m \geq 2$ and cardinality q^{n-m}.

A code is *linear* if it is a subspace of $\mathbb{F}_q^n$. The Hamming codes are the only linear perfect codes. However Lindström (see [11]) presented group perfect codes nonequivalent to any linear code.

2 Definitions of codes automorphism groups

A mapping $\varphi\colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ is called an *isometry* of the space $\mathbb{F}_q^n$ if for any two vectors $x, y \in \mathbb{F}_q^n$ the following equality holds: $d(x, y) = d(\varphi(x), \varphi(y))$.

Suppose $\pi \in S_n$, where S_n is the symmetric group on n elements of the ground set $\{1, 2, \ldots, n\}$. The action of the permutation π on any vector $x = (x_1, \ldots, x_n)$ from $\mathbb{F}_q^n$ is defined by

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

Following [3] by a *configuration* we call an isometry $\sigma\colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ such that

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

where σ_i are permutations from the symmetric group S_q acting on the field $\mathbb{F}_q$.

It is widely known (see, e.g., [12–14]) that the automorphism group of the space $\mathbb{F}_q^n$ is a semidirect product of the group S_n on the group S_q^n of all configurations, i.e.

$$\mathrm{Aut}(\mathbb{F}_q^n) = S_n \leftthreetimes S_q^n = \{(\pi; \sigma)\colon \pi \in S_n,\ \sigma = (\sigma_1, \ldots, \sigma_n) \in S_q^n\}.$$

The group of all isometries of $\mathbb{F}_q^n$ mapping a code C into itself is called the *automorphism group* of the code C:

$$\mathrm{Aut}(C) = \{(\pi; \sigma) \in \mathrm{Aut}(\mathbb{F}_q^n)\colon (\pi; \sigma)(C) = C\}.$$

It is should be noted that the q-ary code automorphism group definition given in [2] takes into account the only semilinear mappings preserving the Hamming weight of codewords.

Multiplying all elements of the field $\mathbb{F}_q$ by some nonzero element $\beta \in \mathbb{F}_q$ we get the permutation τ_β from S_q:

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

By S_q^* we denote the set of all $q-1$ such permutations. Define the *monomial automorphism group* of a code C as

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

Let ε be the identity configuration, i.e. all its components are the identity permutations. It is natural to identify the isometry $(\pi;\varepsilon)$ with the permutation π. Define the *permutation automorphism group* of a code C as

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

3 The group $\mathrm{PAut}(\mathcal{H}_q^n)$

In this section we are going to prove that for any $q > 2$ the permutation automorphism group of a q-ary Hamming code of length n is isomorphic to the unitriangular group $\mathbf{UT}_m(q)$ where $n = (q^m-1)/(q-1)$. Let us start with the definitions of some groups of matrices over $\mathbb{F}_q$. The *general linear group* consists of all nonsingular $m \times m$ matrices and is denoted by $\mathbf{GL}_m(q)$. The set of $m \times m$ matrices with units on the main diagonal and zeros above (under) the diagonal is called the *lower (upper) unitriangular group*. Both these groups are isomorphic to each other. The map taking each lower unitriangular matrix L to the upper unitriangular matrix $R = L^{-\mathsf{T}}$ is an isomorphism between these two groups. Taking that into account we will further denote the groups by $\mathbf{UT}_m(q)$.

The parity check matrix H_m of the q-ary Hamming code $\mathcal{H}_q^n$ of length $n = (q^m-1)/(q-1)$ consists of n pairwise linear independent column vectors from $\mathbb{F}_q^m$. In the sequel we will use the parity check matrix H_m given in the following way. Consider all nonzero vectors of length m that have 1 as their first nonzero coordinate. Let α be a primitive element of $\mathbb{F}_q$. In the case $m = 2$ we have

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

Let for any m we have $H_m = \begin{bmatrix} h_1 & h_2 & \dots & h_n \end{bmatrix}$. Then H_{m+1} can be defined by

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

here $\mathbf{0}$ is the all-zero vector of length m. Let T_m denote the column set of the matrix H_m. If $K \in \mathbf{GL}_m(q)$, then the multiplication $y = Kx$ gives a linear mapping on $\mathbb{F}_q^m$. It is not difficult to prove the following

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

Note that the linear map mentioned above is a bijection on T_m if the matrix L is *lower* unitriangular (in opposite to an upper unitriangular matrix U in the rule $y = xU$). In the following lemma we will show that in the group $\mathbf{GL}_m(q)$ there are no bijections acting on the set T_m besides those described in Lemma 1.

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

Proof. We prove the statement by induction on m. Consider the Hamming code parity check matrix H_m multiplied on the left by a matrix U. For $m = 1$, there is nothing to prove since $UH_1 = [u_{11}][1] = [u_{11}]$, where $u_{11} \neq 0$ and $u_{11} \neq 1$.

Suppose the statement is true for matrices of order m. Now we prove it for a matrix U of order $m + 1$. A matrix U can be represented as follows

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

where $\widetilde{U}$ is a $m \times m$ submatrix, a column vector b and a row vector c have length m and $\beta \in \mathbb{F}_q$. We have

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

There are the following four possible cases to check.

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

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

2. Let either $\det \widetilde{U} = 0$ or $\widetilde{U} \in \mathbf{UT}_m(q)$, and at the same time $b \neq \mathbf{0}$. In this case, the vector b is collinear with some vector of the set T_m. Hence we have $b = \gamma h_k$ for some $\gamma \in \mathbb{F}_q$ and $h_k \in T_m$.

If $\det \widetilde{U} = 0$, then there is a vector h_j in T_m such that $\widetilde{U}h_j = \mathbf{0}$.

On the other hand, if $\widetilde{U} \in \mathbf{UT}_m(q)$, then we can apply Lemma 1. Namely, in the set T_m there is a vector h_j that is assigned the vector h_k under the action of the matrix $\widetilde{U}$. So we have $\widetilde{U}h_j = h_k$.

Combining these two subcases we can conclude that the matrix UH_{m+1} has a submatrix of the form

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

where δ equals either 0 or 1 in accordance with the subcases considered above. Since the set $\{\delta, \delta + \alpha^0\gamma, \delta + \alpha^1\gamma, \ldots, \delta + \alpha^{q-2}\gamma\}$ coincides with the set of all field elements, then for $q > 2$ one can find an integer l from $[0, q-2]$ such that $\delta + \alpha^l\gamma \neq 0$ and $\delta + \alpha^l\gamma \neq 1$. Hence,

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

3. If $\widetilde{U} \in \mathbf{UT}_m(q)$ and $b = \mathbf{0}$, then we have $\beta \neq 0$ for $\det U \neq 0$. In addition, we obtain $\beta \neq 1$ for $U \notin \mathbf{UT}_{m+1}(q)$. This implies that

$$U \begin{bmatrix} \mathbf{0} \\ 1 \end{bmatrix} = \begin{bmatrix} \mathbf{0} \\ \beta \end{bmatrix} \notin T_{m+1} \quad \text{and therefore} \quad h = \begin{bmatrix} \mathbf{0} \\ 1 \end{bmatrix}.$$

4. It should be noted that the conditions $\det \widetilde{U} = 0$ and $b = \mathbf{0}$ are not compatible since $\det U \neq 0$. □

Theorem 1. *For any $n = (q^m - 1)/(q-1)$, where $m \geq 2, q > 2$, it is true that*

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

Proof. It is known (see, e.g., [2]) that the Hamming code monomial automorphism group is isomorphic to the general linear group, namely $\mathrm{MAut}(\mathcal{H}_q^n) \cong \mathbf{GL}_m(q)$. The isomorphism $\theta\colon \mathrm{MAut}(\mathcal{H}_q^n) \to \mathbf{GL}_m(q)$ can be defined by

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

Here H_m is the parity check matrix of the Hamming code $\mathcal{H}_q^n$, the matrix M is a monomial $n \times n$ matrix and $K \in \mathbf{GL}_m(q)$.

By Lemmas 1 and 2 we have $\theta(\mathrm{PAut}(\mathcal{H}_q^n)) = \mathbf{UT}_m(q)$. Therefore a restriction of the isomorphism θ on the permutation automorphism group $\varphi = \theta|_{\mathrm{PAut}(\mathcal{H}_q^n)}$ is an isomorphism between $\mathrm{PAut}(\mathcal{H}_q^n)$ and $\mathbf{UT}_m(q)$. This proves the theorem. □

The author is very grateful to professor Faina I. Solov'eva for constant attention to this work, useful discussions and significant improvements in appearance of the paper.

References

[1] F. J. MacWilliams, N. J. A. Sloane, *The THeory of Error-Correcting Codes*, Amsterdam: North-Holland, 1977.

[2] W. C. Huffman, Codes and groups, V. S. Pless, W. C. Huffman, eds., Handbook of coding theory. Amsterdam – New York: Elsevier Science 17,1998, 1345-1440.

[3] F. I. Solov'eva, S. V. Avgustinovich, T. Honold, W. Heise, On the extendability of code isometries, *J. Geom.* 61, 1998, 3-16.

[4] S. V. Avgustinovich, F. I. Solov'eva, Perfect binary codes with trivial automorphism group, *Proc. Intern. Workshop Inform. Theory*, Killarney, Ireland, 1998, 114-115.

[5] S. A. Malyugin, Perfect codes with trivial automorphism group, *Proc. Second Intern. Workshop OCRT*, Sozopol, Bulgaria, 1998, 163-167.

[6] F. I. Solov'eva, S. T. Topalova, On the automorphism groups of perfect binary codes and Steiner triple systems, *Probl. Inform. Transm.* 36, 2000, 331-335.

[7] F. I. Solov'eva, S. T. Topalova, Perfect binary codes and Steiner triple systems with automorphism groups of maximal order, *Discr. Analysis Oper. Res.* 7, 2000, 101-110 (in Russian).

[8] S. V. Avgustinovich, F. I. Solov'eva, O. Heden, On the structure of symmetry groups of Vasil'ev codes, *Probl. Inform. Transm.* 41, 2005, 105-112.

[9] K. T. Phelps, Every finite group is the automorphism group of some perfect code, *J. Combin. Theory*, Ser. A, 43, 1986, 45-51.

[10] S. A. Malyugin, On the order of the automorphism group of perfect binary codes, *Discr. Analysis Oper. Res.*, 7, 2000, 91-100 (in Russian).

[11] B. Lindström, On group and nongroup perfect codes in q symbols, *Math. Scand.* 25, 1969, 149-158.

[12] A. V. Babash, M. M. Gluhov, G. P. Shankin, On transformations of sets of words over a finite alphabet which do not propagate errors, *Discr. Math. Appl.* 7, 1997, 437-454.

[13] I. Constantinescu, W. Heise, On the concept of code-isomorphy, *J. Geom.* 57, 1996, 63-69.

[14] P. M. Winkler, Isometric embeddings in products of complete graphs, *Discr. Appl. Math.* 7, 1984, 221-225.