ISSN 1995-0802, Lobachevskii Journal of Mathematics, 2018, Vol. 39, No. 7, pp. 1024–1038. © Pleiades Publishing, Ltd., 2018.

On Calculation of Monomial Automorphisms of Linear Cyclic Codes

V. S. Kugurakov[1*], A. Gainutdinova[1], and T. Anisimova[1***]**

(Submitted by F. M. Ablayev)

[1]*Department of Theoretical Cybernetics, Institute of Computational Mathematics and Information Technologies, Kazan (Volga Region) Federal University, ul. Kremlevskaya 18, Kazan, Tatarstan, 420008 Russia*

Received December 6, 2017

Abstract—A description of the monomial automorphisms group of an arbitrary linear cyclic code in term of polynomials is presented. This allows us to reduce a task of code's monomial automorphisms calculation to a task of solving some system of equations (in general, nonlinear) over a finite field. The results are illustrated with examples of calculating the full monomial automorphisms groups for two codes.

DOI: 10.1134/S1995080218070168

Keywords and phrases: *Linear cyclic codes, monomial automorphisms of codes.*

1. INTRODUCTION

This paper is devoted to calculation of the full monomial automorphisms groups of linear cyclic codes. The knowledge of code's automorphisms allows us to refine a code's structure and can be used when designing error-correcting decoding algorithms. We start with needed definitions and notions. Let $\mathbb{F}_q$ be a finite field of q elements, $\mathbb{F}_q^*$ be its multiplicative group, $\mathbb{F}_q^n$ be a set of vectors of length n over $\mathbb{F}_q$. Any non-empty set $C \subseteq \mathbb{F}_q^n$ is called a code over $\mathbb{F}_q$ of length n; if C is a linear subspace over $\mathbb{F}_q$, then the code C is called a *linear code*. For short, we call a linear code V of length ν over $\mathbb{F}_q$, which is invariant under the cyclic shift of vectors, as $C(\nu, q)$-*code*.

A component-wise product of vectors $\mathbf{v} = (v_1, v_2, \dots, v_n)$ and $\mathbf{w} = (w_1, w_2, \dots, w_n)$ is determined as $\mathbf{v} \circ \mathbf{w} = (v_1w_1, v_2w_2, \dots, v_nw_n)$. For vectors $\mathbf{v} = (v_1, v_2, \dots, v_n) \in \mathbb{F}_q^n$, $\mathbf{c} = (c_1, c_2, \dots, c_n) \in (\mathbb{F}_q^*)^n$, and a permutation $\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$ on the set of indexes $I_n = \{1, 2, \dots, n\}$ (π is an element of symmetric group S_n on n points) we determine the following vectors: $\mathbf{v}^\pi = (v_{\pi(1)}, v_{\pi(2)}, \dots, v_{\pi(n)})$ is a permutation of components of vector $\mathbf{v}$ by the action π; $\mathbf{v}^{(\pi,\mathbf{c})} = (c_1v_{\pi(1)}, c_2v_{\pi(2)}, \dots, c_nv_{\pi(n)})$ is a result of transformation of the vector $\mathbf{v}$ under the action $(\pi, \mathbf{c})$.

Notice that $(\mathbf{v}^\pi)^\rho = \mathbf{v}^{\pi\rho}$ and $(\mathbf{v}^{(\pi,\mathbf{a})})^{(\rho,\mathbf{b})} = (\mathbf{v}^\pi \circ \mathbf{a})^{(\rho,\mathbf{b})} = \mathbf{v}^{\pi\rho} \circ \mathbf{a}^\rho \circ \mathbf{b} = \mathbf{v}^{\pi\rho} \circ \mathbf{a}^{(\rho,\mathbf{b})}$, where $\pi\rho$ is a product of permutations π and ρ with multiplication on the left, i.e $\pi\rho(x) = \pi(\rho(x))\ \forall x \in I_n$.

For a code $V \subseteq \mathbb{F}_q^n$, $\pi \in S_n$, $\mathbf{c} \in (\mathbb{F}_q^*)^n$ we assume $V^\pi = \{\mathbf{v}^\pi | \mathbf{v} \in V\}$, $V^{(\pi,\mathbf{c})} = V^\pi \circ \mathbf{c} = \{\mathbf{v}^{(\pi,\mathbf{c})} | \mathbf{v} \in V\}$. A transformation $(\pi, \mathbf{c})$, preserving the code V, i.e. $V^{(\pi,\mathbf{c})} = V$, is called a *monomial automorphism* of the code V. A set $\mathrm{MAut}(V)$ of all such automorphisms forms a group with multiplication (on the left): $(\rho, \mathbf{b}) \times (\pi, \mathbf{a}) = (\pi\rho, \mathbf{a}^{(\rho,\mathbf{b})})$.

*E-mail: vladimir.kugurakov@kpfu.ru

**E-mail: aida.ksu@gmail.com

***E-mail: tanya14-1995@mail.ru