Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in DISCRETE MATHEMATICS

Electronic Notes in Discrete Mathematics 57 (2017) 115–120 www.elsevier.com/locate/endm

Isometry groups of combinatorial codes

Serhii Dyshko [1]

IMATH
Université de Toulon, B.P. 20132, 83957 La Garde
France

Abstract

Two isometry groups of a combinatorial code C are described: the group $\mathrm{Iso}(C)$ of isometries of a code to itself and the group $\mathrm{Mon}(C)$ of isometries of a code to itself that extend to monomial maps. Unlike the case of classical linear codes, where these groups are the same, it is shown that for combinatorial codes the groups can be arbitrary different. Particularly, there exist a code with the richest possible group $\mathrm{Iso}(C)$ and the trivial group $\mathrm{Mon}(C)$. The characterization of the groups and the construction of codes with predefined isometry groups are given.

Keywords: combinatorial code, Hamming isometry, extension theorem, group of isometries, monomial map, group action, groups that are closed with respect to an action

1 Isometry groups of combinatorial codes

In the theory of linear error-correcting codes a group of isometries of a linear code is the group of those linear bijections from the code to itself that preserve the Hamming distance. MacWilliams proved in [6] that each linear Hamming isometry of a classical linear code extends to a monomial map, i.e., it acts

[1] Email:`dyshko@univ-tln.fr`

http://dx.doi.org/10.1016/j.endm.2017.02.020

by permutation of coordinates and multiplication of coordinates by nonzero scalars. Consequently, each linear isometry of a linear code to itself extends to a monomial map.

As it was shown in numerous papers [3] [4] [9], for linear codes over module alphabets an analogue of the MacWilliams Extension Theorem does not hold in general. This means that there may exist linear codes over a module alphabet with linear isometries that do not extend to monomial maps. In the context of combinatorial codes, i.e., codes without any algebraic structure, the situation is similar, see [1] [5] [7].

For the cases of combinatorial codes and linear codes over a module alphabet, along with the group of isometries of a code to itself there is observed the subgroup of those isometries that extend to monomial maps. As it was mentioned above, unlike the case of classical linear codes, the two groups may not be the same.

In [10] Wood investigated the question of how different the two groups of a linear code over a matrix module alphabet can be. He showed, under certain assumptions, that there exists a linear code over a matrix module alphabet with predefined isometry groups. We prove a similar statement for combinatorial codes.

Let A be a finite set, called an *alphabet*, and let n be a positive integer. The *Hamming distance* is a function $\rho_H : A^n \times A^n \to \{0, \dots, n\}$, defined as, for $a, b \in A^n$, $\rho_H(a, b) := |\{i \in \{1, \dots, n\} \mid a_i \neq b_i\}|$. The set A^n equipped with the Hamming distance is a metric space called a *Hamming space*. A *code* C is a subset of the Hamming space A^n. The elements of C are called *codewords*.

A map $f : C \to A^n$ is called a *Hamming isometry* if for each two codewords $a, b \in C$, $\rho_H(a, b) = \rho_H(f(a), f(b))$.

For a finite set X, let $\mathfrak{S}(X)$ denote the symmetric group on X. Denote $\mathfrak{S}_n = \mathfrak{S}(\{1, \dots, n\})$, where n is a positive integer.

A map $h : A^n \to A^n$ is called *monomial* if there exists a permutation $\pi \in \mathfrak{S}_n$ and permutations $\sigma_1, \dots, \sigma_n \in \mathfrak{S}(A)$ such that for each $a \in A^n$,

$$h(a) = \left(\sigma_1(a_{\pi(1)}), \dots, \sigma_n(a_{\pi(n)})\right).$$

Let $C \subseteq A^n$ be a code with $m \geq 3$ codewords. Consider the set

$$M = \{1, \dots, m\},$$

called the *set of messages*, and consider an *encoding map* $\lambda : M \to A^n$ of the code C, i.e., an injective map such that $\lambda(M) = C$. For every $g \in \mathfrak{S}(M)$ the map $\lambda g \lambda^{-1} : C \to C$ is a well-defined bijection.