*Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory*
*June 18-24, 2016, Albena, Bulgaria* *pp. 157–161*

# Isometry Groups of Combinatorial Codes

Serhii Dyshko dyshko@univ-tln.fr
IMATH, Université de Toulon
B.P. 20132, 83957 La Garde, France

**Abstract.** Two isometry groups of combinatorial codes are described: the group of automorphisms and the monomial group, which is the group of those automorphisms that extend to monomial maps. Unlike the case of linear codes, where these groups are the same, it is shown that for nonlinear codes the groups can be arbitrary different. Particularly, there exist codes with the full automorphism group and the trivial monomial group. In the paper the two isometry groups are characterized and codes with predefined isometry groups are constructed.

## 1 Introduction

MacWilliams proved in her Ph.D. thesis [6] that each linear isometry of a classical linear code extends to a monomial map. Consequently, the isometry groups of a classical linear code coincide. As it was shown in numerous papers, see [2, 4, 9], for linear codes over module alphabets the extension property does not hold in general. This means that there could exist codes with different automorphism and monomial groups.

In [8] Wood investigated the question of how different can be the two groups of a linear code over a module alphabet. He showed that for any two subgroups of a general linear group, which satisfy some necessary properties, there exists a linear code over a module alphabet with the predefined automorphism and monomial groups.

In this paper we adapt the original proof of [8] to obtain a similar statement for combinatorial codes, i.e., for codes without any algebraic structure. Fortunately, with minor remarks, an analogue of the result of Wood remains correct for combinatorial codes.

Let $A$ be a finite set and let $n$ be a positive integer. Consider the set $A^n$ of all $n$-tuples of elements from $A$. Consider the *Hamming metrics* $\rho_H$ on $A^n$, defined as, for $x, y \in A^n$, $\rho_H(x, y) = |\{i \mid x_i \neq y_i\}|$.

Let $C \subseteq A^n$ be a code. A *Hamming isometry* of $C$ is a map $f : C \to A^n$ that preserves the Hamming metrics, i.e., for all $x, y \in C$,

$$\rho_H(x, y) = \rho_H(f(x), f(y)).$$

An *automorphism* of $C$ is a Hamming isometry $f : C \to A^n$ such that $f(C) = C$.

For a set $X$ let $\mathrm{Sym}(X)$ denote the group of all permutations of elements of $X$. Let $m$ denotes the cardinality of $C$, then, enumerating the codewords of $C$ by numbers in $\{1, \ldots, m\}$, $\mathrm{Sym}(C) \cong S_m$.

A permutation $g : C \to C$ can be seen as a map $C \to A^n$: for every $g \in S_m$ consider the map $f_g : C \to A^n$, defined as $f_g(c) = g(c)$, for all $c \in C$. Define the *group of automorphisms* of $C$,

$$\mathrm{Aut}(C) = \{g \in S_m \mid f_g \text{ is an automorphism}\}.$$

A map $h : A^n \to A^n$ is called *monomial* if there exist a permutation $\pi \in S_n$ and permutations $g_1, \ldots, g_n \in \mathrm{Sym}(A)$ such that for each $a = (a_1, \ldots, a_n) \in A^n$,

$$h(a) = \big(g_1(a_{\pi(1)}), \ldots, g_n(a_{\pi(n)})\big)\,.$$

It is an easy task to show that every monomial map is an automorphism of $A^n$. Define the *group of monomial automorphisms* of $C$,

$$\mathrm{MAut}(C) = \{g \in \mathrm{Aut}(C) \mid f_g \text{ extends to a monomial map}\}.$$

In [1, Theorem 1] it was proven that the groups $\mathrm{Aut}(A^n)$ and $\mathrm{MAut}(A^n)$ are equal. However, for a code $C \subset A^n$, which is a proper subset, it is not true in general.

According to [7], if $C$ is a $q$-ary $(q, 2)$ or $(q + 1, 2)$ MDS code, $q \neq 2$, then $|\mathrm{Aut}(C)| > |\mathrm{MAut}(C)|$, and thus $\mathrm{Aut}(C) \neq \mathrm{MAut}(C)$. The same holds, for example, for $(q, (q-1)^2, q-1)_q$ equidistant codes, where $q \geq 5$, where both $q$ and $q - 1$ are prime powers, see [5]. There the author observed several other families of codes with different $\mathrm{Aut}(C)$ and $\mathrm{MAut}(C)$ groups.

*Remark* 1. In coding theory it is often used the group $\mathrm{Monom}(C)$ of those monomial maps that preserves $C$. Note that $\mathrm{MAut}(C)$ and $\mathrm{Monom}(C)$ are different objects: $\mathrm{MAut}(C)$ is a subgroup of $\mathrm{Sym}(C) \cong S_m$ and $\mathrm{Monom}(C)$ is a subgroup of the full group of monomial maps[1]. However, there exists a connection. Since every monomial map is a Hamming isometry, for each $h \in \mathrm{Monom}(C)$ there exists a unique element $g_h \in \mathrm{Aut}(C)$ such that $h(c) = g_h(c)$, for all $c \in C$. In other words, the action of the map $h$ on $C$ can be seen as a permutation of codewords. By defining the map

$$\mathrm{restr} : \mathrm{Monom}(C) \to \mathrm{Aut}(C), \quad h \mapsto g_h,$$

we have the equality of groups $\mathrm{MAut}(C) = \mathrm{restr}(\mathrm{Monom}(C))$.

The main result is formulated in the next section.

[1] The set of all monomial maps of $A^n$ form a group, which is isomorphic to the wreath product $S_n \wr \mathrm{Sym}(A)$, see [3, Section 2.6].

## 2 Main result

Let $G$ be a group acting on a set $X$. We say that a subgroup $H \leq G$ is *closed under the action*[2] *on* $X$ if $H$ consists of all those elements in $G$ that preserve the orbits of $H$. To be precise, we say that $H$ is closed under the action on $X$, if the equality holds,

$$H = \{g \in G \mid \forall i \in \{1, \ldots, k\},\ \forall x \in O_i,\ g(x) \in O_i\},$$

where $\{O_1, \ldots, O_k\}$ is the set of orbits of $H$ acting on $X$ and $k$ is a positive integer.

Denote $\ell = |A| \geq 2$. Consider the set $\mathcal{P}_\ell$ of all the partitions of the set $\{1, \ldots, m\}$ that have the number of classes not greater than $\ell = |A|$. Let $\alpha = (s_1) \ldots (s_k) \in \mathcal{P}_\ell$, where $\emptyset \neq s_i \subseteq \{1, \ldots, m\}$, for $i \in \{1, \ldots, k\}$, and $k \leq \ell$. The group $S_m$ acts on the set $\mathcal{P}_\ell$ as follows, for $g \in S_m$,

$$g(\alpha) = (g(s_1)) \ldots (g(s_k)),$$

where $g(s_i) = \{g(x) \mid x \in s_i\} \subseteq \{1, \ldots, m\}$, for $i \in \{1, \ldots, k\}$.

In $\mathcal{P}_\ell$ we distinguish a subset

$$\mathcal{P}_\tau = \{(i, j)(\{1, \ldots, m\} \setminus \{i, j\}) \mid 1 \leq i < j \leq m\}.$$

The group $S_m$ naturally acts on $\mathcal{P}_\tau$ and $\mathcal{P}_\ell \setminus \mathcal{P}_\tau$.

**Theorem 1.** *Let $A$ be a finite set alphabet of cardinality $\ell \geq 2$ and let $C$ be a code of cardinality $m \geq 5$ over the alphabet $A$. The following statements hold.*

*(a) The group* $\mathrm{Aut}(C)$ *is closed under the action on $\mathcal{P}_\tau$.*

*(b) The group* $\mathrm{MAut}(C)$ *is an intersection of* $\mathrm{Aut}(C)$ *with a group closed under the action on $\mathcal{P}_\ell \setminus \mathcal{P}_\tau$.*

*(c) For each closed under the action on $\mathcal{P}_\tau$ subgroup $H_2 \leq S_m$, for each closed under the action on $\mathcal{P}_\ell \setminus \mathcal{P}_\tau$ subgroup $H_1 \leq S_m$, there exists a code $C$ of cardinality $m$ such that*

$$\mathrm{MAut}(C) = H_1 \cap H_2 \quad \textit{and} \quad \mathrm{Aut}(C) = H_2.$$

Note that the trivial subgroup $\{e\} < S_m$ is closed under the action on $\mathcal{P}_\ell \setminus \mathcal{P}_\tau$, and the full group $S_m$ is closed under the action on $\mathcal{P}_\ell \setminus \mathcal{P}_\tau$ and $\mathcal{P}_\tau$.

From Theorem 1Main resulttheorem.1 it follows that there exists a code with equal automorphism and monomial groups: putting $H_1 = S_m$, for each

[2] A similar definition of closures and closed groups were introduced in [3, Section 2.4].

closed under the action on $\mathcal{P}_\tau$ subgroup $H_2 \leq S_m$ there exists a code $C$ of cardinality $m$ such that

$$\mathrm{MAut}(C) = \mathrm{Aut}(C) = H_2.$$

Also, the two groups can be arbitrary different: putting $H_1 = \{e\}$ and $H_2 = S_m$, there exists a code $C$ of cardinality $m$ such that

$$\mathrm{MAut}(C) = \{e\} \quad \text{and} \quad \mathrm{Aut}(C) = S_m.$$

**Example 1.** For $m = 5$ and $\ell = 2$, consider the code of the following form.

| 0 | 1 | 2 | 3 | 4 | 6 | 5 | 4 | 3 | 4 | 3 | 2 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 |
| 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |

It is a $(40, 5, 22)$ equidistant binary code with $\mathrm{Aut}(C) = S_5$ and $\mathrm{MAut}(C) = \{e\}$. The numbers over the horizontal line represent the number of occurrences of the column under the line in the code. For instance, in this example, the second column appear once in the code and the first column does not appear anywhere in the code.

*Remark* 2. The behavior of closed subgroup under the action on $\mathcal{P}_\tau$ and $\mathcal{P}_\ell \backslash \mathcal{P}_\tau$ can be different. There exists a subgroup that is closed under the action on $\mathcal{P}_\ell \backslash \mathcal{P}_\tau$ but not closed under the action on $\mathcal{P}_\tau$. For example, if $m = 5$, $\ell = 3$ and the group is $G = \langle (1,2)(3,4), (1,2)(3,5) \rangle < S_5$. There also exists a subgroup that is closed under the action on $\mathcal{P}_\tau$ but not closed under the action on $\mathcal{P}_\ell \backslash \mathcal{P}_\tau$. Consider $m = 5$, $\ell = 2$ and $G = \langle (1,2)(3,4) \rangle < S_5$.

For small codes with the number of codewords not greater than four the statement of the theorem needs to be refined. There exists a full description of isometry groups in a similar way, though one needs to consider various cases.

# References

[1] I. Constantinescu and W. Heise. On the concept of code-isomorphy. *Journal of Geometry*, 57(1-2):63–69, 1996.

[2] Q. H. Dinh and S. R. López-Permouth. On the equivalence of codes over rings and modules. *Finite Fields and Their Applications*, 10(4):615 – 625, 2004.

[3] J. D. Dixon and B. Mortimer. *Permutation Groups*, volume 163 of *Graduate texts in mathematics.* Springer, 1996.

[4] M. Greferath, A. Nechaev, and R. Wisbauer. Finite quasi-Frobenius modules and linear codes. *Journal of Algebra and Its Applications*, 03(03):247–272, 2004.

[5] D. I. Kovalevskaya. On metric rigidity for some classes of codes. *Problems of Information Transmission*, 47(1):15–27, Mar. 2011.

[6] F. J. Macwilliams. *Combinatorial Properties of Elementary Abelian Groups.* Ph.d. thesis, Radcliffe College, 1962.

[7] F. Solov'eva, T. Honold, S. Avgustinovich, and W. Heise. On the extendability of code isometries. *Journal of Geometry*, 61(1-2):2–16, 1998.

[8] J. A. Wood. Isometries of additive codes. Unpublished.

[9] J. A. Wood. Foundations of linear codes defined over finite modules: the extension theorem and the MacWilliams identities. In *Codes over rings*, volume 6 of *Ser. Coding Theory Cryptol.*, pages 124–190. World Sci. Publ., Hackensack, NJ, 2009.