Isometry Groups of Combinatorial Codes

Serhii DYSHKO

IMATH, Université de Toulon, France

ACCT 2016 19 June

- $\Sigma = \{0, \dots, q-1\}$ is a finite set alphabet, $q \ge 2$
- A q-ary code C is a subset of Σⁿ
- A map f : C → C is a Hamming isometry if

$$\forall x, y \in C, \quad \rho_H(x, y) = \rho_H(f(x), f(y))$$

• A map
$$h: \Sigma^n \to \Sigma^n$$
 is **monomial** if

$$\forall x \in \Sigma^n, \quad h(x_1, \ldots, x_n) = (\sigma_1(x_{\pi(1)}), \ldots, \sigma_n(x_{\pi(n)})),$$

for some permutations $\pi \in \mathfrak{S}_n$ and $\sigma_i \in \mathfrak{S}_q$

• Group of automorphisms

 $\mathsf{Iso}(C) = \{f : C \to C \mid f \text{ is a Hamming isometry}\}\$

Group of monomial automorphisms

 $\mathsf{Mon}(C) = \{f : C \to C \mid f \text{ extends to a monomial map}\}\$

Denoting m = |C| and {f : C → C | f is bijective} ≅ 𝔅_m, the inclusions hold,

$$\mathsf{Mon}(\mathcal{C}) \leq \mathsf{Iso}(\mathcal{C}) \leq \mathfrak{S}_m$$

Problem

Find out how different can be Mon(C) and Iso(C).

Theorem (MacWilliams Extension Theorem^{*}, 1962) For a classical \mathbb{F}_q -linear code C the groups are equal,

$$\operatorname{Mon}_{\mathbb{F}_q}(C) = \operatorname{Iso}_{\mathbb{F}_q}(C)$$

Theorem (Wood, 2015)

Let $R = M_{r \times r}(\mathbb{F}_q)$ be a matrix ring. Let $A = M_{r \times k}(\mathbb{F}_q)$ be a matrix module alphabet, k > r. For any two groups $H_1 \le H_2 \le GL_{k \times k}(\mathbb{F}_q)$ (that satisfy some necessary conditions) there exists an R-linear code $C \subseteq A^n$ such that

$$\mathsf{Mon}_R(\mathcal{C})=\mathit{H}_1$$
 and $\mathsf{Iso}_R(\mathcal{C})=\mathit{H}_2$

Theorem (main result)

Let m and q be integers, $m \ge 5$, $q \ge 2$. For each two subgroups $H_1 \le H_2 \le \mathfrak{S}_m$ (that satisfy some necessary conditions) there exists a q-ary code C with m codewords such that

$$Mon(C) = H_1$$
 and $Iso(C) = H_2$.

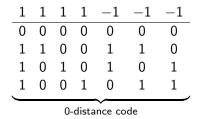
Corollary

Let m and q be integers, $m \ge 5$, $q \ge 2$. There exists a q-ary code C of cardinality m such that

$$Mon(C) = \{e\}$$
 and $Iso(C) = \mathfrak{S}_m$.

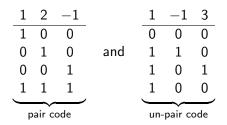
- allow codes to have negative number of columns
- 0-distance codes: $\forall x, y \in C$, $\rho_H(x, y) = 0$

Example



- pair codes: each column contains 2 ones and m-2 zeros
- un-pair codes: each column does not contains 2 ones and m - 2 zeros

Example



• Each code *C* uniquely decomposes into a sum¹ of a 0-distance code and a pair code,

$$C=C_0+C_p$$

The equalities hold

$$Mon(C) = Mon(C_0) \cap Mon(C_p)$$

 $Iso(C) = Iso(C_p)$

• For a pair code P and an un-pair code $U = U_p + U_0$,

 $Mon(U) = Mon(U_0)$ Iso(P) = Mon(P)

 $^{1}X + Y$ represents the concatenation of codes X and Y

Serhii DYSHKO

University of Toulon, France

Isometry Groups of Combinatorial Codes

$$Mon(C) = H_1$$
 and $Iso(C) = H_2$

Proof (of the main theorem)

• Find a (large) pair code P with

$$Mon(P) = H_2.$$

• Find a un-pair code U with

$$Mon(U) = H_1.$$

• Using the decomposition $U = U_p + U_0$, define

$$C = P + U_0$$

• Calculate for $C = P + U_0$,

$$egin{aligned} \mathsf{Mon}(\mathcal{C}) &= \mathsf{Mon}(\mathcal{P}) \cap \mathsf{Mon}(\mathcal{U}_0) \ &= \mathcal{H}_2 \cap \mathsf{Mon}(\mathcal{U}) \ &= \mathcal{H}_2 \cap \mathcal{H}_1 = \mathcal{H}_1 \end{aligned}$$

$$lso(C) = lso(P)$$

= Mon(P)
= H₂

Thank you

Appending: A binary extremal code

Example

Is a $(40,5,22)_2$ equidistant binary code with $Iso(C) \cong \mathfrak{S}_5$ and $Mon(C) = \{e\}.$

Appendix: A non-binary extremal code

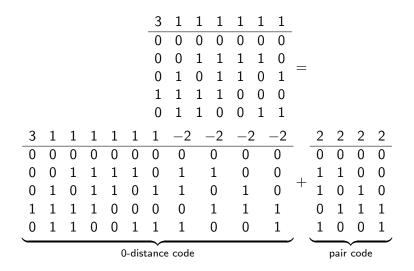
Example

Is a $(9, 4, 7)_3$ equidistant ternary code with $Iso(C) \cong \mathfrak{S}_4$ and $Mon(C) = \{e\}.$

Appendix: Two groups of a code

- $\mathsf{lso}(C) = \langle (1,2,3), (1,2), (4,5) \rangle$
- $Mon(C) = \langle (1, 2, 3), (1, 2) \rangle$
- g = (4,5) is a Hamming isometry, but does not extend to a monomial map

Appendix: Unique decomposition of a code



Serhii DYSHKO

9/9

Appendix: Closure of a group

Definition

Let G be a group acting on the set X. Let H be a subgroup of G. The closure \overline{H} of H under the action on X is defined as follows,

$$ar{H} = \{ g \in G \mid orall O \in X/H, \ g(O) = O \}$$

The group *H* is called **closed** under the action on *X* if $H = \overline{H}$.

Appendix: Set of partitions

- Let q, m be two positive integers
- Define the set of partitions of the set M = {1,..., m} with at most q classes,

$$\mathcal{P} = \big\{ \{c_1,\ldots,c_t\} \mid c_1 \sqcup \cdots \sqcup c_t = M, \ t \leq q \big\},\$$

where $c_i \subseteq M$, for $i \in \{1, ..., t\}$, and \sqcup denotes the disjoint union of sets.

• Define the following subset of \mathcal{P} ,

$$\mathcal{P}_2 = \left\{ \left\{ \{i,j\}, \{M \setminus \{i,j\}\} \right\} \mid \{i,j\} \subset M \right\}.$$

Appendix: The main theorem

Theorem

Let q be an integer, $q \ge 2$ and let C be a q-ary code of cardinality $m \ge 5$ or m = 3. The following statements hold.

- The group Iso(C) is closed under the action on \mathcal{P}_2 .
- The group Mon(C) is equal to an intersection of Iso(C) with a subgroup of \mathfrak{S}_m closed under the action on $\mathcal{P} \setminus \mathcal{P}_2$.
- For each closed under the action on $\mathcal{P} \setminus \mathcal{P}_2$ subgroup $H_1 \leq \mathfrak{S}_m$, for each closed under the action on \mathcal{P}_2 subgroup $H_2 \leq \mathfrak{S}_m$, there exists a q-ary code C of cardinality $m \geq 5$ such that

$$Mon(C) = H_1 \cap Iso(C)$$
 and $Iso(C) = H_2$.