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, $q \geq 2$
- A q-ary code C is a subset of Σ^n
- A map $f : C \to C$ 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

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

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

- **Group of automorphisms**

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

- **Group of monomial automorphisms**

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

- Denoting $m = |C|$ and $\{f : C \to C \mid f \text{ is bijective}\} \cong \mathfrak{S}_m$, the inclusions hold,

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

Problem

Find out how different can be $\mathrm{Mon}(C)$ and $\mathrm{Iso}(C)$.

Theorem (MacWilliams Extension Theorem*, 1962)

For a classical $\mathbb{F}_q$-linear code C the groups are equal,

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

Theorem (Wood, 2015)

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

$$\mathrm{Mon}_R(C) = H_1 \quad \textit{and} \quad \mathrm{Iso}_R(C) = H_2$$

Theorem (main result)

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

$$\mathrm{Mon}(C) = H_1 \quad \textit{and} \quad \mathrm{Iso}(C) = H_2.$$

Corollary

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

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

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

Example

$$\underbrace{\begin{array}{ccccccc} 1 & 1 & 1 & 1 & -1 & -1 & -1 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}}_{\text{0-distance code}}$$

- **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

$$\underbrace{\begin{array}{ccc} 1 & 2 & -1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{array}}_{\text{pair code}} \quad \text{and} \quad \underbrace{\begin{array}{ccc} 1 & -1 & 3 \\ \hline 0 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{array}}_{\text{un-pair code}}$$

- Each code C uniquely decomposes into a sum[1] of a 0-distance code and a pair code,

$$C = C_0 + C_p$$

- The equalities hold

$$\mathrm{Mon}(C) = \mathrm{Mon}(C_0) \cap \mathrm{Mon}(C_p)$$
$$\mathrm{Iso}(C) = \mathrm{Iso}(C_p)$$

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

$$\mathrm{Mon}(U) = \mathrm{Mon}(U_0)$$
$$\mathrm{Iso}(P) = \mathrm{Mon}(P)$$

[1] $X + Y$ represents the concatenation of codes X and Y

$$\mathrm{Mon}(C) = H_1 \quad \text{and} \quad \mathrm{Iso}(C) = H_2$$

Proof (of the main theorem)

- Find a (large) pair code P with
$$\mathrm{Mon}(P) = H_2.$$
- Find a un-pair code U with
$$\mathrm{Mon}(U) = H_1.$$
- Using the decomposition $U = U_p + U_0$, define
$$C = P + U_0$$

- Calculate for $C = P + U_0$,

$$\begin{aligned} \mathrm{Mon}(C) &= \mathrm{Mon}(P) \cap \mathrm{Mon}(U_0) \\ &= H_2 \cap \mathrm{Mon}(U) \\ &= H_2 \cap H_1 = H_1 \end{aligned}$$

$$\begin{aligned} \mathrm{Iso}(C) &= \mathrm{Iso}(P) \\ &= \mathrm{Mon}(P) \\ &= H_2 \end{aligned}$$

$\square$

Thank you

Appending: A binary extremal code

Example

1	2	3	4	6	5	4	3	4	3	2	2	1
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	1	1	1	1	1	1	0	0
0	1	0	0	1	0	1	1	1	0	0	1	1
0	0	1	0	1	1	0	1	0	1	0	1	0
0	0	0	1	1	1	1	0	0	0	1	0	1

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

Appendix: A non-binary extremal code

Example

$$\begin{array}{ccccccccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 0 & 2 & 0 & 1 & 1 & 2 & 2 \\
1 & 1 & 1 & 1 & 2 & 2 & 2 & 0 & 0
\end{array}$$

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

Appendix: Two groups of a code

$$\begin{matrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{matrix} \quad \xrightarrow{(4,5)} \quad \begin{matrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{matrix}$$

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

Appendix: Unique decomposition of a code

$$\begin{array}{ccccccc}
3 & 1 & 1 & 1 & 1 & 1 & 1 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 1
\end{array} =$$

$$\underbrace{\begin{array}{ccccccccccc}
3 & 1 & 1 & 1 & 1 & 1 & 1 & -2 & -2 & -2 & -2 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1
\end{array}}_{\text{0-distance code}} + \underbrace{\begin{array}{cccc}
2 & 2 & 2 & 2 \\
\hline
0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 \\
1 & 0 & 0 & 1
\end{array}}_{\text{pair code}}$$

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 $\bar{H}$ of H under the action on X is defined as follows,

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

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

Appendix: Set of partitions

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

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

  where $c_i \subseteq M$, for $i \in \{1, \dots, t\}$, and $\sqcup$ denotes the disjoint union of sets.
- Define the following subset of $\mathcal{P}$,

$$\mathcal{P}_2 = \Big\{ \big\{ \{i, j\}, \{M \setminus \{i, j\}\} \big\} \; \Big| \; \{i, j\} \subset M \Big\}.$$

Appendix: The main theorem

Theorem

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

- *The group $\mathrm{Iso}(C)$ is closed under the action on $\mathcal{P}_2$.*
- *The group $\mathrm{Mon}(C)$ is equal to an intersection of $\mathrm{Iso}(C)$ 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*

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