General isometries of codes

Serhii DYSHKO

IMATH, Université de Toulon

The MacWilliams Extension Theorem

Let L be a finite field, m be a positive integer and L^m be a Hamming space.

Definition

For two codes $C_1, C_2 \subseteq L^m$, the map $f : C_1 \to C_2$ is called an **isometry**, if it preserves the Hamming metrics.

Theorem (MacWilliams Extension Theorem)

Let $C \subseteq L^m$ be a linear code. Each linear isometry of C extends to a linear isometry of space.

Theorem

All possible linear isometries $h : L^m \to L^m$ are ***monomial****:*

- *multiplication of the coordinates by elements of $L \setminus \{0\}$*
- *permutation of the coordinates*

Extendibility of isometries

Let $K \subseteq L$ be a pair of finite fields.

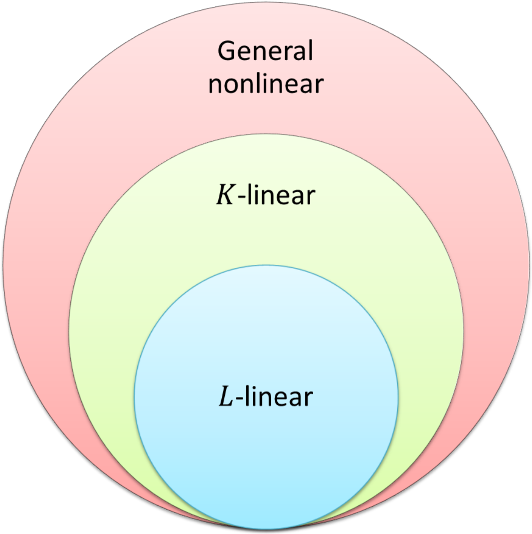
Definition

Code C is called K-**linear** if it is a K-linear subspace in L^m.

$$\begin{tikzcd} L^m \arrow[r, "h"] & L^m \\ C_1 \arrow[u, "\iota"'] \arrow[r, "f"] & C_2 \arrow[u, "\iota"'] \end{tikzcd}$$

Question: Can K-linear isometry $f : C_1 \to C_2$ be extended to the K-linear isometry $h : L^m \to L^m$?

Codes diagram $K \subseteq L$



Example of unextendible isometry

Let $L = \mathbb{F}_4$ (generated by $\omega^2 = \omega + 1$), $K = \mathbb{F}_2$ and $m = 3$.
Consider the following $\mathbb{F}_2$-linear codes C_1, C_2 and $\mathbb{F}_2$-linear map f:

$$C_1 = \begin{matrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{matrix} \xrightarrow{f} \begin{matrix} 1 & 1 & 0 \\ \omega & \omega & 0 \\ \omega^2 & \omega^2 & 0 \\ 0 & 0 & 0 \end{matrix} = C_2.$$

The map f is an isometry and cannot be extended to an $\mathbb{F}_2$-linear isometry of $\mathbb{F}_4^3$:

Theorem

All possible K-linear isometries of L^m are **general monomial**

- *action of* $\mathrm{Aut}_K(L)$ *on the coordinate*
- *permutation of the coordinates*

Extendibility of K-linear isometries

Theorem (Extension theorem for K-linear codes)

Let $K \subseteq L$ be a pair of finite fields. If the length of a K-linear code is not greater than the cardinality of the field K, then all K-linear isometries of the code are extendible.

Remark

The results of the theorem cannot be improved: for any pair of fields $K \subset L$ there exists a K-linear code C of the length greater than $|K|$ with unextendible K-linear isometry.

Generator matrix

A K-linear code C can be presented by the generator matrix:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \dots & a_{km} \end{pmatrix} \in \mathrm{M}_{k\times m}(L)$$

where code C is the K-span of A's rows.

Example

Defined previously $\mathbb{F}_2$-linear codes $C_1, C_2 \subset \mathbb{F}_4^3$ have the following generator matrices:

$$C_1 \text{ with } A_1 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \text{ and } C_2 \text{ with } A_2 = \begin{pmatrix} 1 & 1 & 0 \\ \omega & \omega & 0 \end{pmatrix}.$$

Generator matrix and spaces

Consider L as a n-dimensional vector space over K. Chose a K-basis $b_1, \dots, b_n$ in L. For each $a_{ij} \in L$ let $a_{ij} = \sum_{l=1}^{n} b_l a_{ij}^{(l)}$, for $a_{ij}^{(l)} \in K$.

$$A = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{k1} & \dots & a_{km} \end{pmatrix} \Rightarrow V_1, \dots, V_m$$

$$B = \begin{pmatrix} \overbrace{\begin{matrix} a_{11}^{(1)} & \dots & a_{11}^{(n)} \\ \vdots & \ddots & \vdots \\ a_{k1}^{(1)} & \dots & a_{k1}^{(n)} \end{matrix}}^{V_1} & \dots & \overbrace{\begin{matrix} a_{1m}^{(1)} & \dots & a_{1m}^{(n)} \\ \vdots & \ddots & \vdots \\ a_{km}^{(1)} & \dots & a_{km}^{(n)} \end{matrix}}^{V_m} \end{pmatrix}$$

$B \in \mathrm{M}_{k \times mn}(K)$ is the K-generator matrix of K-linear code C. Spaces $V_1, \dots, V_m$ are K-subspaces in K^k with $\dim_K V_i \leq n$.

Maps and spaces

Let C_1 and C_2 be K-linear codes with generator matrices A_1 and A_2. Let $f : C_1 \to C_2$ be a K-linear map that maps the row i of A_1 to the row i of A_2.

$$A_1 = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{k1} & \dots & a_{km} \end{pmatrix} \xrightarrow{f} \begin{pmatrix} c_{11} & \dots & c_{1m} \\ \vdots & \ddots & \vdots \\ c_{k1} & \dots & c_{km} \end{pmatrix} = A_2$$

$$V_1, \dots, V_m \quad \to \quad U_1, \dots, U_m$$

The tuple of spaces $V_1, \dots, V_m$ corresponds to A_1 and $U_1, \dots, U_m$ corresponds to A_2.

Main theorem

Theorem (Isometry criterium)

Let C_1, C_2 be K-linear codes in L^m and $f : C_1 \to C_2$ be a K-linear map. The map f is isometry if, and only if, the following equality holds:

$$\sum_{i=1}^{m} \frac{1}{|V_i|} \mathbb{1}_{V_i} = \sum_{i=1}^{m} \frac{1}{|U_i|} \mathbb{1}_{U_i}$$

Extendibility and trivial solution

$$\sum_{i=1}^{m} \frac{1}{|V_i|} \mathbb{1}_{V_i} = \sum_{i=1}^{m} \frac{1}{|U_i|} \mathbb{1}_{U_i}$$

There is always a **trivial solution:** if tuples of subspaces $V_1, \dots, V_m$ and $U_1, \dots, U_m$ coincide (up to permutations), then they satisfy the equation.

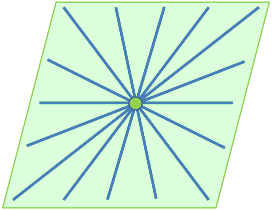
Theorem

The K-linear code isometry $f : C_1 \to C_2$ is extendible, iff the solution of the equation is trivial.

Nontrivial solution example

Let $L = \mathbb{F}_4$ (generated by $\omega^2 = \omega + 1$) and $K = \mathbb{F}_2$ and $m = 3$. Consider the following code $\mathbb{F}_2$-linear map:

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \xrightarrow{f} \begin{pmatrix} 1 & 1 & 0 \\ \omega & \omega & 0 \end{pmatrix}$$



Isomorphism of $\mathbb{F}_2$-spaces
$\mathbb{F}_4 \cong \mathbb{F}_2^2 : 1 \longmapsto 10, \omega \longmapsto 01$

$$\begin{pmatrix} 0\,0 & 1\,0 & 1\,0 \\ 1\,0 & 0\,0 & 1\,0 \end{pmatrix} \xrightarrow{f} \begin{pmatrix} 1\,0 & 1\,0 & 0\,0 \\ 0\,1 & 0\,1 & 0\,0 \end{pmatrix}$$

$$\langle(0\,1)\rangle, \langle(1\,0)\rangle, \langle(1\,1)\rangle \to \mathbb{F}_2^2,\ \mathbb{F}_2^2,\ (0\,0)$$

The equality $\sum_{i=1}^{m} \frac{1}{|V_i|} \mathbb{1}_{V_i} = \sum_{i=1}^{m} \frac{1}{|U_i|} \mathbb{1}_{U_i}$ becomes:

$$\mathbb{1}_{\langle(0\,1)\rangle} + \mathbb{1}_{\langle(1\,0)\rangle} + \mathbb{1}_{\langle(1\,1)\rangle} = \mathbb{1}_{\mathbb{F}_2^2} + 2 \cdot \mathbb{1}_{(0\,0)}$$

$$\sum_{i=1}^{m} \frac{1}{|V_i|} \mathbb{1}_{V_i} = \sum_{i=1}^{m} \frac{1}{|U_i|} \mathbb{1}_{U_i}$$

Theorem

There exists a nontrivial solution of equation iff $m > |K|$.

Theorem (Extension theorem for K-linear codes)

Let $K \subseteq L$ be a pair of finite fields. If the length of a K-linear code is not greater than the cardinality of the field K, then all K-linear isometries of the code are extendible.

Conclusions

- ☑ Prove the analogue of MacWilliams theorem for the code length $m \leq |K|$
- ☑ Describe the code isometries with the threshold code length $m = |K| + 1$
- ☑ Describe the code automorphisms with the code length $m = |K| + 1$

Thank you!
Any questions?

Appendix

Importance

If we know, whether the isometries of code are extendible, we can:

1. Describe all code isometries
2. Identify the codes with the same metric parameters
3. Determine, if the codes are equivalent
4. Simplify the task of codes classification

Additive ($\mathbb{F}_p$-linear) codes are important, because quantum stabilizer codes are additive.

Example

Let $m = |K| + 1$. Consider two K-linear codes $C_1 = \langle v_1, v_2 \rangle_K$ and $C_2 = \langle u_1, u_2 \rangle_K$ of length $|K| + 1$ with

$$\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 & \dots & 1 \\ 1 & x_1 & x_2 & \dots & x_{|K|} \end{pmatrix} \xrightarrow{f} \begin{pmatrix} 0 & 1 & 1 & \dots & 1 \\ 0 & \omega & \omega & \dots & \omega \end{pmatrix} = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix} \ ,$$

where $x_i \in K$ are all different and $\omega \in L \setminus K$.
Define the K-linear map $f : C_1 \to C_2$ on the generators of C_1 in the following way: $f(v_1) = u_1$ and $f(v_2) = u_2$.
The map f is an isometry. But, there is no general monomial transformation that acts on C_1 in the same ways as the map f.

Known nonlinear analogues

Classes of nonlinear codes, for which the analogue of extension theorem holds (by S. Augustinovich & F. Solov'eva):

1. All perfect q-ary codes, except $[7, 4, 3]_2$ and $[4, 2, 3]_3$ Hamming codes.
2. All q-ary $(n, n-1)$ MDS codes for $n > 4$.
3. Binary linear $[n, n-1, 2]$ codes, where $n \neq 4$

And does not holds:

1. All q-ary $(q, 2)$ and $(q+1, 2)$ MDS codes, except for $(2, 2)$ and $(3, 2)$
2. A binary linear code with parameters $[4, 3, 2]$
3. Equidistant codes with parameters $(n, q, 3)_q$, $n \geq 4$,$q \geq 10$,and $(6, 6, 4)_3$