Strong Isometries of Codes

Sergey Avgustinovich **Evgeny Gorkunov**

Sobolev Institute of Mathematics
Novosibirsk State University
<avgust@math.nsc.ru>
<evgumin@gmail.com>

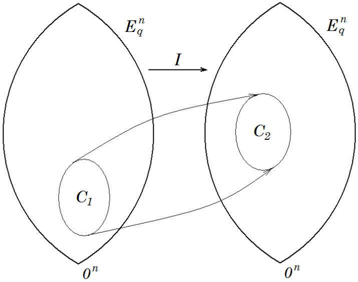
Algebraic and Combinatorial Coding Theory
June 15–21, 2012

Notation

- E_q^n – a q-ary cube – the set of all words of length n over an alphabet of q symbols
- $d(x, y) = |\{i \colon x_i \neq y_i\}|$ – the Hamming distance
- $w(x) = |\{i \colon x_i \neq 0\}|$ – weight of x
- $C \subseteq E_q^n$ – a q-ary code of length n
- $d(C) = \min\{d(x, y) \colon x, y \in C, x \neq y\}$ – the minimum distance of C

Equivalent codes

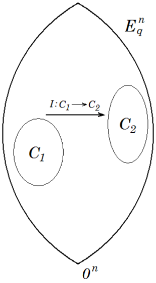
Two codes are equivalent if there is an isometry of E_q^n that maps one of the codes into the other one



Equivalent codes are identical from a metrical point of view.
They have the same structure and equaled metrical parameters.
Equivalent codes embedded in E_q^n in the similar way.

Isometric codes

Two codes are isometric if there is *any isometry* between them, a bijection preserving distances between codewords



Isometric, but not equivalent codes

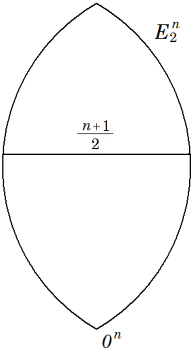
There are many Hadamard codes that are isometric, but not equivalent

Problem statement

What kind of metric invariants makes codes to be equivalent and which of them are not sufficient for that?

Testing sets

A subset $T \subseteq E_q^n$ is called a testing set for a class $\mathcal{K}$ of codes if any codes $C_1, C_2 \in \mathcal{K}$ are equal whenever $C_1 \cap T = C_2 \cap T$.



Avgustinovich, 1995

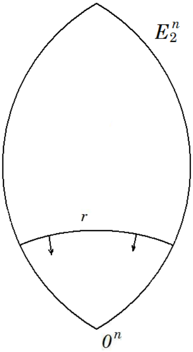
The codewords of a perfect code are determined by its codewords on the middle layer of E_2^n

Avgustinovich, Vasilyeva, 2000

The values of a centred function are determined by its values on the middle layer of E_2^n

Testing sets

A subset $T \subseteq E_q^n$ is called a testing set for a class $\mathcal{K}$ of codes if any codes $C_1, C_2 \in \mathcal{K}$ are equal whenever $C_1 \cap T = C_2 \cap T$.



Avgustinovich, Vasilyeva, 2006

The values of a centred function in a ball with radius $r \leq \frac{n+1}{2}$ are determined by its values on the sphere of radius r

Isometries

An isometry preserves all distances between codewords.

- [Avgustinovich, 1994]
  If perfect binary codes are isometric, then they are equivalent
- [Solov'eva, Avgustinovich, Honold, Heise, 1998]
  Every isometry between q-ary perfect codes is extendable to an isometry of the space E_q^n,
  i.e. q-ary perfect codes are *metricaly rigid*
  (one exception: ternary perfect codes of length 4 are not)

Weak isometries

A weak isometry between two codes preserves minimal distances between their codewords.

Codes that are equivalent whenever they are weakly isometric:

- [Avgustinovich, 1998]
  Perfect binary codes
- [Mogilnykh, 2009]
  Preparata codes
- [Mogilnykh, Östergård, Pottonen, Solov'eva, 2009]
  Extended perfect binary codes

Strong isometries of binary codes

A mapping between two binary codes that preserves dimensions of all their subcodes.

Dimension of a binary code C

$\mathrm{Dim}(C)$ denotes the dimension of minimal face of E_2^n that contains the code

Remark

$$\mathrm{Dim}\{x, y\} = d(x, y)$$

Example

$$C = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix},$$

$$\mathrm{Dim}(C) = 3$$

Strong isometries of binary codes

- [Avgustinovich, 2000]
  If binary codes are strongly isometric, then they are equivalent
- Each strong isometry can be extended to an isometry of the Boolean cube
- [Avgustinovich, Gorkunov, 2010]
  If a mapping between two binary codes preserves *dimensions of their subcodes with even cardinality*, then the mapping can be extended to an isometry of the Boolean cube.
  We refer to such a mapping as a *semistrong isometry*
- If binary codes are semistrongly isometric, then they are equivalent

Correlation coefficients

Unessential positions

If all codewords of a code C have the same symbol at the i-th position, we call the position unessential for the code C.
$N(C)$ – the set of all unessential positions of C

Correlation coefficients

For subcodes $C_1, C_2 \subseteq C$ with $C_1 \cap C_2 = \varnothing$, we refer to the number of positions from $N(C_1) \cap N(C_2)$ at which codewords from different subcodes are distinct as correlation coefficient of C_1 and C_2 and denote it by $K(C_1, C_2)$, i.e.

$$K(C_1, C_2) = |\{i \in N(C_1) \cap N(C_2) \colon x_i \neq y_i \text{ for any } x \in C_1 \text{ and } y \in C_2\}|$$

Examples

$$C = \left[\begin{array}{cccccccc} 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 2 & 0 & 1 \\ \hline 0 & 0 & 1 & 0 & 2 & 0 & 1 & 2 \\ 0 & 1 & 1 & 2 & 2 & 2 & 0 & 2 \end{array}\right] \begin{array}{c} C_1 \\ \\ C_2 \end{array} \longrightarrow K(C_1, C_2) = 3$$

Simple eqations

- $K(x, y) = d(x, y)$ for any $x, y \in E_3^n$
- $K(\{x, y\}, \varnothing) = n - d(x, y)$ for any $x, y \in E_3^n$
- $K(C, \varnothing) = n - \mathrm{Dim}(C)$,
  where $\mathrm{Dim}(C)$ is dimension of the code $C \subseteq E_3^n$ in the sense mentioned above

Examples

$$C = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ \hline 0 & 0 & 0 & 1 & 0 & 2 & 0 & 1 \\ \hline 0 & 0 & 1 & 0 & 2 & 0 & 1 & 2 \\ \hline 0 & 1 & 1 & 2 & 2 & 2 & 0 & 2 \end{bmatrix} \begin{matrix} \\ \\ x \\ y \\ \\ \end{matrix} \longrightarrow K(x, y) = 6$$

Simple eqations

- $K(x, y) = d(x, y)$ for any $x, y \in E_3^n$
- $K(\{x, y\}, \varnothing) = n - d(x, y)$ for any $x, y \in E_3^n$
- $K(C, \varnothing) = n - \mathrm{Dim}(C)$,
  where $\mathrm{Dim}(C)$ is dimension of the code $C \subseteq E_3^n$ in the sense mentioned above

Examples

$$C = \left[\begin{array}{cccccccc} 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 2 & 0 & 1 \\ \hline 0 & 0 & 1 & 0 & 2 & 0 & 1 & 2 \\ 0 & 1 & 1 & 2 & 2 & 2 & 0 & 2 \end{array}\right] \begin{array}{c} \\ x \\ y \\ \\ \\ \end{array} \longrightarrow K(\{x,y\},\varnothing) = 6$$

Simple eqations

- $K(x,y) = d(x,y)$ for any $x, y \in E_3^n$
- $K(\{x,y\},\varnothing) = n - d(x,y)$ for any $x, y \in E_3^n$
- $K(C,\varnothing) = n - \mathrm{Dim}(C)$, where $\mathrm{Dim}(C)$ is dimension of the code $C \subseteq E_3^n$ in the sense mentioned above

Examples

$$C = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 & 2 & 0 & 1 & 2 \\ 0 & 1 & 1 & 2 & 2 & 2 & 0 & 2 \end{bmatrix} \longrightarrow K(C, \varnothing) = 1$$

Simple eqations

- $K(x, y) = d(x, y)$ for any $x, y \in E_3^n$
- $K(\{x, y\}, \varnothing) = n - d(x, y)$ for any $x, y \in E_3^n$
- $K(C, \varnothing) = n - \mathrm{Dim}(C)$,
  where $\mathrm{Dim}(C)$ is dimension of the code $C \subseteq E_3^n$ in the sense mentioned above

Strong isometries of q-ary codes

$I\colon C_1 \to C_2$ – a bijection between two ternary codes preserving correlation coefficient of any pair of subcodes of C_1, i.e.

$$K(A,B) = K(I(A), I(B)) \quad \text{for any } A, B \subseteq C_1$$

We refer to a bijection between codes preserving correlation coefficients of its subcodes as a strong isometry

We say that two codes are strongly isometric if there exists a strong isometry between them

Strong isometries of q-ary codes

Theorem

Any strong isometry between ternary codes can be extended to an isometry of the whole space E_3^n

Corollary

Strongly isometric ternary codes are equivalent

Alphabet partitions

For each column of a code matrix, the symbols of the alphabet $\{1, 2, 3\}$ yield an alphabet partiotion of the set of row indeces

Example

$$C = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 & 2 & 0 & 1 & 2 \\ 0 & 1 & 1 & 2 & 2 & 2 & 0 & 2 \end{bmatrix}$$

- The column C_4 has $\{\{1, 4\}, \{2, 3\}, \{5\}\}$ as its alphabet partition
- The columns C_5 and C_8 have $\{\{1, 2, 3\}, \{4, 5\}, \varnothing\}$ as their alphabet partitions

Alphabet partitions

For each column of a code matrix, the symbols of the alphabet $\{1,2,3\}$ yield an alphabet partiotion of the set of row indeces

Example

$$C = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 & 2 & 0 & 1 & 2 \\ 0 & 1 & 1 & 2 & 2 & 2 & 0 & 2 \end{bmatrix}$$

- The column C_4 has $\{\{1,4\},\{2,3\},\{5\}\}$ as its alphabet partition
- The columns C_5 and C_8 have $\{\{1,2,3\},\{4,5\},\varnothing\}$ as their alphabet partitions

Alphabet partitions and codes

Lemma

If code matrices M_1 and M_2 have the same multisets of alphabet partitions, then corresponding codes are equivalent

Partial order on alphabet partitions

Define a partial order $\preccurlyeq$ by the rule

$$(P_1, Q_1, R_1) \preccurlyeq (P_2, Q_2, R_2) \text{ if and only if}$$

$$P_1 \subseteq P_2,\ Q_1 \supseteq Q_2,\ \text{and } R_1 \supseteq R_2,$$

where $(P_1, Q_1, R_1), (P_2, Q_2, R_2)$ are two alphabet partitions

Alphabet partitions and correlation coefficients

Consider a code $C \subseteq E_3^n$, its code matrix M, and
an alphabet partition $\mathcal{P} = (P, Q, R)$.
Let $k(\mathcal{P})$ be the number of columns of M with the partition $\mathcal{P}$.
The following equalities are true.

Direct formula

$$K(Q, R) = \sum_{\mathcal{Q} \preccurlyeq \mathcal{P}} k(\mathcal{Q})$$

Inversion of direct formula

$$k(\mathcal{P}) = \sum_{(P',Q',R') \preccurlyeq \mathcal{P}} (-1)^{|P|-|P'|} K(Q', R')$$