On the Normality of (Non-Mixed and Mixed) Optimal Covering Codes

Gerzson Kéri

Budapest, Thursday, 8 July, 2010

19th International Symposium on the Mathematical Theory of Networks and Systems

1. Introduction and Notation

***n*-tuple** : *n*-dimensional vector, whose coordinates are symbols from a finite alphabet such as $\{1, 2\}$ or $\{0, 1\}$ or $\{Y, N\}$ or $\{\bullet, \bullet\}$ or $\{1, 2, 3\}$ or $\{0, 1, 2\}$ or $\{1, 2, x\}$ etc.

Code of length *n* : a collection of *n*-tuples.

Hamming space : the collection of all *n*-tuples.

Hamming distance of two *n*-tuples : the number of coordinates where the corresponding symbols are different.

Sphere in the Hamming space : the set of such *n*-tuples that are within a given distance /- the radius -/ of a given *n*-tuple /- the center -/.

Covering code of length n with a given radius : a collection of n-tuples so that the union of the corresponding spheres entirely cover the Hamming space.

Optimal covering code of length n, with covering radius R : a covering code of least possible cardinality for the given parameters n, R.

Perfect code : the covering with spheres are one-fold.

Notation for the size of optimal covering codes : $K_q(n, R)$

Description of codes:

a) Exact (scientific) form

$$
\begin{array}{ll}
\{ & (c_{11}, c_{12}, \dots, c_{1n}), \\
 & (c_{21}, c_{22}, \dots, c_{2n}), \\
 & \dots\dots\dots\dots\dots\dots \\
 & (c_{M1}, c_{M2}, \dots, c_{Mn})\}
\end{array}
$$

or

$$
\begin{array}{rcl}
c_1 & = & (c_{11}, c_{12}, \dots, c_{1n}), \\
c_2 & = & (c_{21}, c_{22}, \dots, c_{2n}), \\
. & . & \dots\dots\dots\dots\dots\dots \\
c_M & = & (c_{M1}, c_{M2}, \dots, c_{Mn}).
\end{array}
$$

Description of codes (continued):

b) Arrangement of the codewords into a matrix

$$\begin{pmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ . & . & \dots & . \\ c_{M1} & c_{M2} & \dots & c_{Mn} \end{pmatrix}$$

c) Arrangement of the codewords into an array or file

$$\begin{matrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ . & . & \dots & . \\ c_{M1} & c_{M2} & \dots & c_{Mn} \end{matrix}$$

Example for spheres (For the rest of the paper, we shall restrict to using the alphabet $\{0, 1, \ldots, q-1\}$)

$$C = \{(0,1,0),(1,0,1)\}$$

Sphere at center c_1 (with radius $R = 1$):

$$\{(0,0,0),(0,1,0),(0,1,1),(1,1,0)\}$$

Sphere at center c_2 (with radius $R = 1$):

$$\{(0,0,1),(1,0,0),(1,0,1),(1,1,1)\}$$

The given example shows that $K_2(3,1) = 2$.

2. Normality

The notion of normality was introduced by Graham and Sloane (1985) for binary linear codes.

Normal codes are useful especially for the so called ADS construction to produce a compound covering codes with good properties whose constituents are normal codes.

Later a lot of papers appeared by Honkala, Lobstein, Östergård, and other authors about the features and applications of normal and subnormal codes.

Normality was defined also for nonlinear and nonbinary codes.

Definition

Let $C \subset H = Z_q^n$ be a code with covering radius R, and let i be an arbitrary index $(1 \leq i \leq n)$. Let C_j denote the set of all such codewords, whose i-th coordinate value is j $(0 \leq j \leq q-1)$. The code C is called to be normal with respect to the i-th coordinate if

$$\sum_{j=0}^{q-1} d(x, C_j) \leq qR + q - 1. \qquad (1)$$

holds for every $x \in Z_q^n$.

A code $C \subset H = Z_q^n$ is called simply normal if it is normal with respect to at least one coordinate. A code $C \subset H = Z_q^n$ that is not normal is called abnormal.

The extension of normality for mixed codes in $Z_{q_1}^{n_1} Z_{q_2}^{n_2}$ and for mixed codes with arbitrary number of different q_i-s is straightforward.

For $q = 2$ the equality defining normality reduces to

$$d(x, C_0) + d(x, C_1) \leq 2R + 1;$$

for $q = 3$ to

$$d(x, C_0) + d(x, C_1) + d(x, C_2) \leq 3R + 2;$$

and so on.

Repetition codes are normal for arbitrary q.

Conjecture: Binary optimal covering codes are normal.

It is an experience that all known binary optimal covering codes are normal. This is far not the case for nonbinary codes.

Binary perfect covering codes are proved to be normal. We shall see that the opposite of this is true for nonbinary codes.

Next 3 sheets:

1. Example for binary normal code and ADS construction with it.
2. Example for ternary perfect code and ADS construction with it.
3. Example for ternary normal code and ADS construction with it.

$K_2(6,1) = 12$, $K_2(8,2) \leq 12$:

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$K_3(4,1) = 9$, $K_3(7,3) > 9$ (≥ 11 is proved):

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 1 & 2 & 0 & 1 \\ 2 & 0 & 2 & 1 \\ 2 & 1 & 0 & 2 \\ 2 & 2 & 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 2 & 2 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 2 & 2 & 2 \\ 1 & 1 & 2 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 1 & 1 & 1 & 1 \\ 2 & 0 & 2 & 1 & 1 & 1 & 1 \\ 2 & 1 & 0 & 2 & 2 & 2 & 2 \\ 2 & 2 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

(Here the covering radius of the resulted code is greater than 3.)

$L_3(4,1) = 12$, $K_3(7,3) \leq 12$ (≥ 11 is proved):

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 2 & 2 & 2 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 1 & 2 & 1 & 0 \\ 2 & 0 & 2 & 2 \\ 2 & 1 & 1 & 0 \\ 2 & 2 & 0 & 2 \\ 2 & 2 & 2 & 1 \end{bmatrix} \qquad \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 2 & 2 & 2 & 2 & 2 & 2 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 & 2 & 2 & 2 \\ 1 & 1 & 2 & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 & 0 & 0 \\ 2 & 0 & 2 & 2 & 2 & 2 & 2 \\ 2 & 1 & 1 & 0 & 0 & 0 & 0 \\ 2 & 2 & 0 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 1 & 1 & 1 & 1 \end{bmatrix}$$

3. On the minimum distance of normal codes

Definition

The minimum distance $d_{\min}(C)$ of a code $C \subseteq H$ is the smallest value among the Hamming distances between any pair of different codewords, i.e.

$$d_{\min}(C) = \min\{d(x, y) : x, y \in C, x \neq y\}.$$

(The single letter d can also be used instead of $d_{\min}(C)$ if it does not cause any kind of ambiguity.)

The following relation between the minimum distance and covering radius of normal codes provides a lucid explanation for the dissimilarity between the behavior of binary and non-binary codes with respect to normality that was revealed in the previous sections.

Theorem

Let $C \subset Z_q^n$ be a normal code with covering radius R and minimum distance d; then the following inequality holds

$$d \leq R + 1 + \frac{R}{q-1}. \tag{2}$$

Proof.

According to the definition of a *normal code*, inequality (1)

$$\sum_{j=0}^{q-1} d(x, C_j) \leq qR + q - 1.$$

holds for every $x \in Z_q^n$. For a codeword x, according to the definition of the minimum distance we have $d(x, C_j) \geq d$ if $x \notin C_j$ and $d(x, C_j) = 0$ if $x \in C_j$. By this, (1) leads to the inequality

$$(q-1)d \leq qR + q - 1.$$

□

Further examples:

$K_3(3,1) = 5$ - unique, abnormal

$K_3(4,1) = 9$ - unique, abnormal

$K_3(5,1) = 27$ - 17 inequivalent optimal codes, all are normal

$K_3(6,1)$ - unknown

$K_3(4,2) = 3$ - unique (repetition code), normal

$K_3(5,2) = 8$ - unique, abnormal

$K_3(6,2)$ - unknown

$K_3(6,3) = 6$ - 28 optimal codes, 24 are normal, 4 are abnormal

Thank you for your attention.