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

Gerzson Kéri
Computer and Automation Research Institute,
Hungarian Academy of Sciences
H-1111 Budapest Kende u. 13-17, Hungary
e-mail: keri@sztaki.hu

***Abstract*— According to the experiences, it is a known fact that some essential features of normal codes are quite different for binary and for non-binary codes. After giving some explanation concerning this observation by referring to an old conjecture with its partial proof, its possible extensions and restrictions, and by giving some counterexamples in Section 3, subsequently an interesting inequality between the minimum distance and covering radius of normal codes is expounded in Section 4, which provides a lucid explanation for the observed dissimilarity between the behavior of binary and non-binary codes.**

Keywords: covering codes, mixed codes, normal and abnormal codes.

I. Introduction

We consider covering codes in either non-mixed or mixed Hamming spaces denoted by $H = Z_q^n$ for non-mixed spaces, $H = Z_{q_1}^{n_1} Z_{q_2}^{n_2}$, $H = Z_{q_1}^{n_1} Z_{q_2}^{n_2} Z_{q_3}^{n_3}$ (etc.) for mixed spaces, where $Z_q = \{0, 1, \ldots, q-1\}$.

The Hamming distance $d(x, y)$ between two words $x, y \in H$ is the number of coordinates in which they differ.

We continue with the definition of some coding theoretic notions that are most important for the rest of the paper.

Definition 1: The covering radius of a code $C \subseteq H$ is the smallest positive integer R such that for an arbitrary $x \in H$, there exists one (or more) $y \in C$ with $d(x, y) \le R$. In other words,

$$R = \max\{d(x, C) \mid x \in H\}$$

where

$$d(x, C) = \min\{d(x, y) \mid y \in C\}.$$

Definition 2: 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.

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

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

Definition 3: Let $C \subset H = Z_q^n$ be a code with covering radius R, and let i be an arbitrary index ($1 \le i \le n$). Let C_j denote the set of all such codewords, whose i-th coordinate value is j ($0 \le j \le q-1$). The code C is called to be normal with respect to the i-th coordinate if

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

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.

A straightforward extension of Definition 3 for mixed codes in $Z_{q_1}^{n_1} Z_{q_2}^{n_2}$ is as follows.

Definition 4: Let $C \subset H = Z_{q_1}^{n_1} Z_{q_2}^{n_2}$ be a code with covering radius R, and let i be an arbitrary index that corresponds to a coordinate from the first set of coordinates ($1 \le i \le n_1$). Let C_j denote the set of all such codewords, whose i-th coordinate value is j ($0 \le j \le q_1 - 1$). The code C is normal with respect to the i-th coordinate if

$$\sum_{j=0}^{q_1-1} d(x, C_j) \le q_1 R + q_1 - 1. \tag{2}$$

holds for every $x \in Z_{q_1}^{n_1} Z_{q_2}^{n_2}$.

Similarly, C is normal with respect to the i-th coordinate from the second coordinate set if

$$\sum_{j=0}^{q_2-1} d(x, C_j) \le q_2 R + q_2 - 1. \tag{3}$$

holds for every $x \in Z_{q_1}^{n_1} Z_{q_2}^{n_2}$, where C_j are defined again according to the value in the i-the coordinate.

We say that C is q_1-normal (q_2-normal) if it is normal with respect to at least one coordinate from the first (second) set of coordinates.

The extension of normality with respect to given coordinates to mixed codes with arbitrary number of different q_i-s is straightforward.

Definition 5: A covering code is called *optimal* if it has minimum cardinality among codes with given parameters n_i and R; the minimum cardinality is denoted by

$$K_q(n, R),\ K_{q_1,q_2}(n_1, n_2, R),\ K_{q_1,q_2,q_3}(n_1, n_2, n_3, R),$$

and analogous notations are used for arbitrary number of different q_is.

The research was supported in part by OTKA grants K 60480, K 77420.

II. AMALGAMATED DIRECT SUM OF NORMAL CODES

Let $C \subset Z_q^{n_1}$ and $D \subset Z_q^{n_2}$ be arbitrary covering codes. Let C_j denote the set of all such codewords of C, whose last coordinate value is j. Also, let D_j denote the set of all such codewords of D, whose first coordinate value is j. Now, let $C'_j \subset Z_q^{n_1-1}$, $D'_j \subset Z_q^{n_2-1}$ denote the sets whose elements are obtained by omitting the last (first) coordinates from the codewords contained in C_j (D_j).

The *amalgamated direct sum* (usually abbreviated as ADS) of C and D is then defined as

$$\bigcup_{i=0}^{q-1} \{(c', j, d') \mid c' \in C'_j, d' \in D'_j\}.$$

It is known that within some circumstances the covering radius of the ADS is equal to (or less than) the sum of the covering radii of the two components. This is the case, in particular, when C is normal with respect to its last coordinate and D is normal with respect to its first coordinate, see [11, Theorem 1]. The generalization of the ADS construction to mixed codes with special regard to the covering radius and normality is studied in [12].

Now, we concentrate to the easiest special case of the ADS construction, i.e., to the case when one of the codes C and D is a repetition code. It is easy to show that a q-ary repetition code of any length n is normal with respect to all of its coordinates. This is also the assertion of [11, Lemma 1].

Let us assume that a given q-ary code with N coordinates, M codewords, and covering radius R,

$$\begin{aligned} C = \{ \ & (c_{11}, c_{12}, \ldots, c_{1N}), \\ & (c_{21}, c_{22}, \ldots, c_{2N}), \\ & \ldots\ldots\ldots\ldots\ldots\ldots \\ & (c_{M1}, c_{M2}, \ldots, c_{MN})\} \subset Z_q^N \end{aligned}$$

is normal with respect to its last coordinate. Take the amalgamated direct sum of C with a q-ary repetition code D having $kq+1$ coordinates where k is an arbitrary positive integer, i.e., with

$$\begin{aligned} D = \{ \ & (0, 0, \ldots, 0), \\ & (1, 1, \ldots, 1), \\ & \ldots\ldots\ldots\ldots\ldots\ldots \\ & (q-1, q-1, \ldots, q-1)\} \subset Z_q^{kq+1}. \end{aligned}$$

As arbitrary $x \in Z_q^{kq+1}$ has at least $q+1$ identical coordinates, and x can be chosen so that it contains either q or $q+1$ coordinates of value i for any $i = 0, 1, \ldots, q-1$, consequently the covering radius of D is $(kq+1)-(q+1) = (k-1)q$.

According to a general theorem [11, Theorem 1] regarding the covering radius of the amalgamated direct sum of normal codes, the ADS of C and D

$$\begin{aligned} \{ \ & (c_{11}, c_{12}, \ldots, c_{1N}, c_{1N}, \ldots, c_{1N}) \\ & (c_{21}, c_{22}, \ldots, c_{2N}, c_{2N}, \ldots, c_{2N}) \\ & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ & (c_{M1}, c_{M2}, \ldots, c_{MN}, c_{MN}, \ldots, c_{MN})\} \subset Z_q^{N+kq} \end{aligned}$$

has covering radius $R + (k-1)q$ or less.

III. A CONJECTURE, RELATED INEQUALITIES AND COUNTEREXAMPLES

The following conjecture for the binary case was discussed and partially proved in [2]:

Conjecture 1: $K_2(n+2, R+1) \leq K_2(n, R)$ for all $R \neq n$.

The ADS construction of a binary normal code C with a binary repetition code of three coordinates proves that Conjecture 1 is valid in all such cases when a normal optimal covering code exists that attains $K_2(n, R)$.

Another open question, related to Conjecture 1, is the following: Is it always true that among the optimal covering codes attaining $K_2(n, R)$ there exist one or more normal codes? As regards the analogous question about non-binary codes it can be shown easily that for $q \geq 3$ any q-ary perfect optimal covering code is abnormal. (We will return to this question in the second note to Theorem 5 in Section IV.)

The ADS construction of a q-ary normal code with a repetition code of $q+1$ coordinates proves the following assertion:

Proposition 1: If $R \neq n$ and there is a normal optimal covering code attaining $K_q(n, R)$, then

$$K_q(n+q, R+q-1) \leq K_q(n, R). \tag{4}$$

The assertion of Proposition 1 can be extended for arbitrary types of mixed covering codes. Hereafter we formulate the analogous inequalities for mixed ternary/binary codes, which cover the most frequently studied type of mixed codes.

Proposition 2: If $R \neq t+b$ and there is a 3-normal mixed optimal covering code attaining $K_{3,2}(t, b, R)$, then

$$K_{3,2}(t+3, b, R+2) \leq K_{3,2}(t, b, R). \tag{5}$$

Proposition 3: If $R \neq t+b$ and there is a 2-normal mixed optimal covering code attaining $K_{3,2}(t, b, R)$, then

$$K_{3,2}(t, b+2, R+1) \leq K_{3,2}(t, b, R). \tag{6}$$

At this point the question arises spontaneously whether inequalities (4)-(6) are valid in general, without the hypothesis on the existence of normal optimal codes. The answer for this question is negative, which is evident from the following counterexamples, taking the exact values from [6], e.g.

$K_3(6, 3) = 6 > K_3(3, 1) = 5,$
$K_3(8, 4) = 9 > K_3(5, 2) = 8,$
$K_4(8, 5) = 8 > K_4(4, 2) = 7,$
$K_{3,2}(4, 4, 3) = 10 > K_{3,2}(1, 4, 1) = 8,$
$K_{3,2}(5, 2, 3) = 7 > K_{3,2}(2, 2, 1) = 6,$
$K_{3,2}(6, 3, 5) = 4 > K_{3,2}(6, 1, 4) = 3,$
$K_{3,2}(8, 4, 7) = 4 > K_{3,2}(8, 2, 6) = 3.$

For the special case, however, when $q = 2, R = 1$, inequality (4) has been proved without assuming normality, i.e., the assertion of the following theorem is true:

Theorem 4: $K_2(n+2, 2) \leq K_2(n, 1)$ holds for arbitrary $n \geq 2$.

This is essentially the same as *Proposition 2.2* in [2], where the assertion was appended by the words: *"except perhaps for $n = 9$ and $n = 16$"*. These exceptional cases has been arranged later, by proving that $K_2(11, 2) \leq 44$ [3] and $K_2(18, 2) \leq 2944$ [13].

To close this section, we give some examples for the application of Proposition 1 and Proposition 2. By repeated application of the first of these, we obtain

$K_3(3u + 4, 2u + 1) \leq 12,$
$K_3(3u + 5, 2u + 1) \leq 27$

for arbitrary $u \geq 1$; by repeated application of the other, we obtain

$K_{3,2}(3u + 1, 4, 2u + 1) \leq 10,$
$K_{3,2}(3u + 1, 5, 2u + 1) \leq 16,$
$K_{3,2}(3u + 1, 6, 2u + 2) \leq 10,$
$K_{3,2}(3u + 2, 3, 2u + 1) \leq 12,$
$K_{3,2}(3u + 2, 5, 2u + 2) \leq 12,$
$K_{3,2}(3u + 3, 1, 2u + 1) \leq 10,$
$K_{3,2}(3u + 3, 2, 2u + 1) \leq 16,$
$K_{3,2}(3u + 4, 1, 2u + 1) \leq 18,$
$K_{3,2}(3u + 4, 2, 2u + 2) \leq 11$

for arbitrary $u \geq 1$ again.

IV. On the minimum distance of normal codes

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

$$d \leq R + 1 + \frac{R}{q - 1}. \qquad (7)$$

Proof: According to the definition of a *normal code*, inequality (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

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

which can be arranged easily to have the form (7). ■

Notes and conclusions.

- It is a basic coding theoretic inequality that $d \leq 2R+1$ holds in general, for any code, thus (7) is always true for binary codes, without the assumption of normality.
- A covering code is said to be perfect if $d = 2R + 1$. For $q \geq 3$, (7) implies that $d \leq R+1+R/2 < 2R+1$. Consequently, any non-binary perfect code is abnormal.
- Any non-binary code with covering radius $R > 1$ and minimum distance $d = 2R$ is abnormal if $q > 3$ or $R > 2$.

Generalizations.

- A covering code is said to be subnormal if there exists a partition of C into q nonempty subsets $C_0, C_1, \ldots C_{q-1}$ such that (1) holds for every $x \in Z_q^n$. Clearly, inequality (7) remains valid if $C \subset Z_q^n$ is a subnormal code with covering radius R and minimum distance d.
- Let $C \subset Z_{q_1}^{n_1} Z_{q_2}^{n_2}$, $Z_{q_1}^{n_1} Z_{q_2}^{n_2} Z_{q_3}^{n_3}$ (etc.) be a q_i-normal code for at least one i with covering radius R and minimum distance d. Then inequality (7) remains valid again with a slight modification as follows. In this case, q should be replaced in (7) by the largest such q_i for which the code C is q_i-normal.

References

[1] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*, North-Holland, Amsterdam (1997).
[2] G. D. Cohen, A. C. Lobstein, and N. J. A. Sloane, On a conjecture concerning coverings of Hamming space, *Applied algebra, algorithmics and error-correcting codes (Toulouse, 1984)*, Lecture Notes in Computer Science, Vol. 228, Springer-Verlag, Berlin (1986), 79-89.
[3] I. S. Honkala and H. O. Hämäläinen, A new construction for covering codes, *IEEE Trans. Inform. Theory*, 34 (1988), 1343–1344.
[4] I. S. Honkala and H. O. Hämäläinen, Bounds for abnormal binary codes, *IEEE Trans. Inform. Theory*, 37 (1991), 372–375.
[5] G. Kéri, On small covering codes in arbitrary mixed Hamming spaces, *Studia Sci. Math. Hungar.*, 44 (2007), 517–534.
[6] G. Kéri, Tables for covering codes, http://www.sztaki.hu/∼keri/codes.
[7] G. Kéri and P. R. J. Östergård, On the covering radius of small codes, *Studia Sci. Math. Hungar.*, 40 (2003), 243–256.
[8] G. Kéri and P. R. J. Östergård, The number of inequivalent $(2R + 3, 7)R$ optimal covering codes, *J. Integer Seq.*, 9 (2006), Article 06.4.7 (electronic).
[9] G. Kéri and P. R. J. Östergård, Further results on the covering radius of small codes, *Discrete Math.*, 307 (2007), 69–77.
[10] G. Kéri and P. R. J. Östergård, On the minimum size of binary codes with length $2R + 4$ and covering radius R, *Des. Codes Cryptogr.*, 48 (2008), 165–169.
[11] A. C. Lobstein and G. J. M. van Wee, On normal and subnormal q-ary codes, *IEEE Trans. Inform. Theory*, 35 (1989), 1291–1295.
[12] P. R. J. Östergård and H. O. Hämäläinen, A new table of binary/ternary mixed covering codes, *Des. Codes Cryptogr.*, 1 (1997), 151–178.
[13] P. R. J. Östergård and M. K. Kaikkonen, New upper bounds for binary covering codes, *Discrete Math.*, 178 (1998), 165–179.
[14] G. J. M. van Wee, More binary covering codes are normal, *IEEE Trans. Inform. Theory*, 36 (1990), 1466–1470.