Sixth International Workshop on Optimal Codes and Related Topics
June 16-22, 2009, Varna, Bulgaria *pp. 5-10*

Normality of some binary linear codes

Tsonka Baicheva tsonka@math.bas.bg
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences,
5000 Veliko Tarnovo, BULGARIA

Abstract. We show that all binary codes of lengths 16, 17 and 18, or redundancy 10, are normal. These results have applications in the construction of codes that attain $t[n,k]$, the smallest covering radius of any binary linear code.

1 Introduction

Covering radius is one of the fundamental parameters of a code and has important applications in Computer and Communication Sciences. Its study has attracted many researchers for the past 30 years (see [1], the surveys [2],[3], and the book [4]).

Normality and amalgamated direct sum (ADS) were introduced in [1] to construct good "covering codes", i.e. codes with small covering radius compared to others of the same length and dimension. That approach requires the constituent codes to be normal, a difficult property to establish. Hence much subsequent research has focused on the question: which codes are normal? The purpose of this work is to prove the normality of the binary codes of lengths 16, 17 and 18 or redundancy 10.

2 Some preliminary results

Let F_q^n be the n-dimensional vector space over the finite field with q elements. A *linear code* C is a k-dimensional subspace of F_q^n. The ball of radius t around a word $y \in F_q^n$ is defined by

$$\{x | x \in F_q^n, d(x,y) \leq t\}.$$

Then the covering radius $R(C)$ of a code C is defined as the least possible integer number such that the balls of radius $R(C)$ around the codewords cover the whole F_q^n, i.e.

$$R(C) = \max_{x \in F_q^n} \min_{c \in C} d(x,c).$$

A coset of the code C defined by the vector $x \in F_q^n$ is the set $x+C = \{x+c \mid c \in C\}$. A coset leader of $x+C$ is a vector in $x+C$ of smallest weight. When the code is linear its covering radius is equal to the weight of the heaviest coset leader. We will denote by $[n, k, d]R$ a code of length n, dimension k, minimum distance d and covering radius R.

The function $t_q[n, k]$ is defined as the least value of $R(C)$ when C runs over the class of all linear $[n, k]$ codes over F_q for a given q.

Definition 1 [4] Let C be a binary code of length n and covering radius R. For $i = 1, \ldots, n$ let $C_0^{(i)}$ (respectively $C_1^{(i)}$) denote the set of codewords in which the i-th coordinate is 0 (respectively 1). The integer

$$N^{(i)}(x) = \max_{x \in F_2^n} \{d(x, C_0^{(i)}) + d(x, C_1^{(i)})\}$$

is called the *norm* of C with respect to the i-th coordinate and

$$N_{min} = \min_i N^{(i)}$$

is called the minimum norm of C. (We use the convention that $d(x, 0) = \infty$.) The code C has norm N if $N_{min} \leq N$ and the coordinates i for which $N^{(i)} < N$ are called *acceptable* with respect to N.

The code C is *normal* if it has norm $2R + 1$. If $N^{(i)} \leq 2R + 1$, then we say that the coordinate i is acceptable with respect to $2R + 1$, or that C is normal with respect to the i-th coordinate. If C is not normal then it is an *abnormal* code. An interesting question in this context is to determine which codes are normal and which codes are abnormal.

In the following proposition results about the normality of binary linear codes are summarized.

Proposition 1 *(i) [5] If C is an $[n, k, d]$ code with $n \leq 14$, or $k \leq 5$, or $d \leq 4$, or $R \leq 2$ then C is normal. (ii) [7] All $[n, k, d]R$ codes with $d \geq 2R - 1$ or $R = 3$ are normal. (iii) [6] All binary $[n, k, d]$ codes of $n = 15$ and $n - k \leq 9$ are normal.*

One of the main reasons for studying normal codes is the *amalgamated direct sum* (ADS) construction introduced by Graham and Sloane [1].

Theorem 1 [4] *Assume that A is a normal binary $[n_A, k_A]R_A$ code with the last coordinate acceptable, and B is a normal binary $[n_B, k_B]R_B$ code with the first coordinate acceptable. Then their amalgamated direct sum*

$$A \dot{\oplus} B = \{(a, 0, b) | (a, 0) \in A, (0, b) \in B\} \cup \{(a, 1, b) | (a, 1) \in A, (1, b) \in B\}$$

is an $[n_A + n_B - 1, k_A + k_B - 1]R$ code with $R \leq R_A + R_B$. More generally, if the norm of A with respect to the last coordinate is N_A and the norm of B with respect to the first coordinate is N_B, then the code $A \dot{\oplus} B$ has norm

N_A+N_B-1 *and hence covering radius at most* $\frac{1}{2}(N_A+N_B-1)$. *In particular, if the covering radius of* $A\dot{\oplus}B$ *equals* R_A+R_B, *then* $A\dot{\oplus}B$ *is normal and the overlapping coordinate is acceptable.*

This result is extended in [6].

Theorem 2 *If* A *and* B *are normal with even norms, then* $R(A\dot{\oplus}B) = R(A)+R(B)-1$ *and* $A\dot{\oplus}B$ *is normal.*

Definition 2 *The residual code of* C *with respect to a vector* x*, denoted* $R(C;x)$*, is the code obtained by projecting* C *on the complement of the support of* x.

The following result was proved in [3] by an extension of the idea of residual code to a non-codeword.

Proposition 2 *Let* C *be binary. If* x *is a coset leader of* C *of weight* $R = R(C)$*, then* $R(C;x)$ *is an* $[n-R, k, d' \geq \lceil d/2 \rceil]$ *code.*

The generalization of Proposition 2 is given in [6]. Let $|x|$ stand for the Hamming weight of the vector x.

Proposition 3 *If* x *is a coset leader of* C*, then* $R(C;x)$ *is an* $[n-|x|, k, d' \geq \lceil d/2 \rceil]$ *code.*

Let C_σ be C shortened at i-th coordinate. Cohen, Lobstein, and Sloane [8] give the following sufficient condition for normality.

Proposition 4 *If for some coordinate* i, $R(C_\sigma) \leq R(C)+1$, *then* C *is normal.*

3 All binary linear codes of lengths 16, 17 and 18 or redundancy 10 are normal

In [6] the following results about the normality of the binary linear codes of length 16 or redundancy 10 are obtained.

Theorem 3 *All binary linear codes of length 16 are normal except possibly a* $[16,6,5$ *or* $6]4$ *code having all its shortened subcodes of type* $[15,5,5$ *or* $6]6$.

Theorem 4 *All codes of redundancy 10 are normal except possibly codes of types*

- $[16,6,5$ *or* $6]4$
- $[17+j, 7+j, 6]4$, $j=0,1,2$
- $[17+j, 7+j, 5]4$, $0 \leq j \leq 5$

in which at each coordinate the shortened code has covering radius 6.

We extend this result to codes of lengths 17 and 18.

Theorem 5 (i)*All binary linear codes of length 17 are normal except possibly a* $[17,6,5$ *or* $6]5$ *code having all its shortened subcodes of type* $[16,5,5$ *or* $6]7$.

(ii)*All binary linear codes of length 18 are normal except possibly a* $[18, 6, d \geq 5]5$ *code having all its shortened subcodes of type* $[17, 5, d \geq 5]7$ *and a* $[18, 7, 5$ *or* $6]5$ *code having all its shortened subcodes of type* $[17, 6, 5$ *or* $6]7$.

Proof. (i) By Proposition 1 we may assume that $[17, 6, d \geq 5]$ are the only codes for which we do not know are they normal or not. The maximum minimum distance [9] of a $[17, 6]$ code is 7. Let $d = 7$. Then C_σ is a $[16, 5, d' \geq 7]$ code and from [4, Table 7.1] and Proposition 3 we get that C is a $[17, 6, 7]5$ *or* 6 code with a shortened subcode C_σ of type $[16, 5, d' \geq 7]5$ *or* 6. Finally, by Proposition 4 we may conclude that all $[17, 6, 7]$ codes are normal. Let now $d = 5$ or $d = 6$. C_σ is a $[16, 5, d' \geq 5]$ code. According [4, Table 7.1] and Proposition 3, $5 \leq R(C) \leq 7$ and $5 \leq R(C_\sigma) \leq 7$ and by Proposition 4 we get that the only undecided case are $[17, 6, 5$ *or* $6]5$ codes having subcodes of type $[16, 5, 5$ *or* $6]7$.

(ii) The undecided cases for length 18 are codes of dimensions 6 and 7 (see Proposition 1). Let first C be a $[18, 6, d \geq 5]$ code. For $d = 7$ or $d = 8$, $5 \leq R(C) \leq 7$ by [4, Table 7.1] and Proposition 3 and C_σ is an $[17, 5, d' \geq 7]$ code of $R(C_\sigma) = 6$ *or* 7 ([4, Table 7.1] and Proposition 3). These possibilities are reduced to $[18, 6, 7$ *or* $8]5$ with $[17, 5, 7$ *or* $8]7$ subcodes by Proposition 4. In the similar way we obtain for $d = 5$ or $d = 6$, that C could only be a $[18, 6, 5$ *or* $6]5$ code with a $[17, 5, d' \geq 5]7$ subcode. Combining the results for $d = 5$ *or* 6 and $d = 7$ *or* 8 we get that C could only be a $[18, 6, d \geq 5]5$ code having shortened subcode of type $[17, 5, d \geq 5]7$. Let now C be a $[18, 7, d \geq 5]$ code. Its maximum minimum distance is 7 ([9]). For the $[18, 7, 7]$ codes $R(C) = 5$ *or* 6 and C_σ is of type $[17, 6, d' \geq 7]5$ *or* 6([4, Table 7.1] and Proposition 3). By Proposition 4 all such codes are normal. If $d = 5$ *or* 6 [4, Table 7.1] and Proposition 3 gives $5 \leq R(C) \leq 7$ and $5 \leq R(C_\sigma) \leq 7$ and by Proposition 4 if a code of length 18 and dimension 7 is abnormal it must be a $[18, 7, 5$ *or* $6]5$ code having subcodes of type $[17, 6, 5$ *or* $6]7$. ◇

To complete the proof for normality of the codes from Theorems 3,4 and 5 we have to construct all such codes and check if they are normal or not. The classification results are obtained by the developed by Iliya Bouyukliev package Q-EXTENSION [11] and determination of the covering radii of the classified codes and checking are they normal or not by a programs developed by the author. For example, to solve the case $n = 16$ we have to classify all $[15, 5, 5$ *or* $6]6$ codes. It turned out that there are 2638 such codes and 114 are of covering radius 6. These 114 codes are extended by Q-EXTENTION to 5828 $[16, 6, 5$ *or* $6]$ codes. Among them 4 are of covering radius 4 and all of them pass the check for normality. Unfortunately, this approach is not applicable to the rest of the codes as the number of codes increases very fast. In order to make the classification feasible, we use the following result.

Proposition 5. *Let B be an $[n, k, d]R$ code and let extend it to an $[n + 1, k + 1, d' \leq d]$ code B_1. Then $R(B_1) \leq R(B)$.*

Proof. W.l.o.g. the generator matrix of B_1 can be represented in the following way:

$$G(B_1) = \left[\begin{array}{c|c} A & C \\ \hline 0 & G_B \end{array}\right],$$

where A is a $[1, 1]0$ code and C is a $[n, 1]$ code. Then $R(B_1) \leq R(B) + 0 = R(B)$ (see [10]).

Therefore, to check the normality of the codes from Theorem 4 we can start with the already classified $[15, 5, 5$ *or* $6]$ codes of covering radius 6, to extend them to $[16, 6, 5$ *or* $6]R \leq 6$ codes and to determine the $[16, 6, 5$ *or* $6]6$ codes. Then we extend these $[16, 6, 5$ *or* $6]6$ codes to $[17, 7, 5$ *or* $6]R \leq 6$ codes. From the obtained codes, we determine those of covering radii 4 and 6. We check normality of the $[17, 7, 5$ *or* $6]4$ codes and extend $[17, 7, 5$ *or* $6]6$ codes in order to obtain $[18, 8, 5$ *or* $6]R \leq 6$ codes. The same way we check normality of $[18, 8, 5$ *or* $6]4$ codes and extend $[18, 8, 5$ *or* $6]$ codes to $[19, 9, 5$ *or* $6]R \leq 6$ codes. We continue this chain until we get all $[22, 12, 5]4$ codes and check their normality. In the similar way we construct the codes from Theorem 5 and check are they normal or not. It turned out that all the codes are normal and we can conclude that all binary codes of lengths 16, 17 and 18 or redundancy 10 are normal.

An important result of this investigation is also that we have classification of all normal codes of parameters given in Theorems 3, 4 and 5 and applying the ADS construction to them we can obtain new codes with small covering radius. Some of the codes have even norms and we can apply Theorem 2 to them in order to get even better result. In many cases we can use this construction to obtain codes having the least possible covering radius $t_2[n, k]$. For example, it is known [4, Table 7.1] that $t_2[19, 8] = t_2[20, 9] = t_2[21, 10] = t_2[22, 11] = 4$. The ADS of the classified in this work normal $[17, 7]4$, $[18, 8]4$, $[19, 9]4$ or $[20, 10]4$ codes of norm 8 and a normal $[3, 2]1$ code of norm 2 is a $[19, 8]4$, $[20, 9]4$, $[21, 10]4$ or $[22, 11]4$ code, respectively.

References

[1] R. L. Graham, N. J. A. Sloane, On the covering radius of codes, *IEEE Trans. Inform. Theory* 31, 1985, 385-401.

[2] G. D. Cohen, M. G. Karpovsky, H. F. Mattson, Jr., J. R. Schatz, Covering radius - survey and recent results, *IEEE Trans. Inform. Theory* 31, 1985, 738-740.

[3] G. D. Cohen, S. N. Litsyn, A. C. Lobstein, H. F. Mattson, Jr., Covering radius 1985-1994, *AAECC* (Springer), 8, 1997, 173-239.

[4] G. Cohen, I. Honkala, S. Litsyn, A. Lobstein, *Covering Codes*, North-Holland, Elsevier Science B.V., 1997.

[5] K. E. Kilby, N. J. A. Sloane, On the covering radius problem for codes: I Bounds on normalized covering radius, II Codes of low dimension; normal and abnormal codes, *SIAM J. Algebr. Discr. Methods* 8, 1987, 604-627.

[6] H. Janwa, H. F. Mattson, Jr., Some upper bounds on the covering radii of linear codes over F_q and their applications., *Des., Codes Crypt.* 18, 1999, 163-181.

[7] Xiang-dong Hou, Binary linear quasi-perfect codes codes are normal, *IEEE Trans. Inform. Theory* 37, 1991, 378-379.

[8] G. D. Cohen, A. C. Lobstein, N. J. A. Sloane, Further results on the covering radius of codes, *IEEE Trans. Inform. Theory* 32, 1986, 680-694.

[9] A. E. Brouwer, Bounds on the size of linear codes, in *Handbook of Coding Theory,* V. S. Pless and W. C. Huffman, eds., Elsevier, Amsterdam, 1998, 295-461.

[10] H. F. Mattson, Jr., An improved upper bound on covering radius, *Lect. Notes Comp. Sci.* 228, 1986, 90-106.

[11] I. Bouyukliev, What is Q-extension?, *Serdica J. Comput.* 1 ,2007, 115-130.