Discrete Mathematics 125 (1994) 229–239
North-Holland

On the normality of multiple covering codes

Iiro Honkala

Department of Mathematics, University of Turku, 20500 Turku 50, Finland

Received 12 July 1991
Revised 24 January 1992

Abstract

A binary code C of length n is called a μ-fold r-covering if every binary word of length n is within Hamming distance r of at least μ codewords of C. The normality and the amalgamated direct sum (ADS) construction of 1-fold coverings have been extensively studied. In this paper we generalize the concepts of subnormality and normality to μ-fold coverings and discuss how the ADS construction can be applied to them. In particular, we show that for $r=1,2$ all binary linear μ-fold r-coverings of length at least $2r+1$ and μ-fold normal.

1. Introduction

A binary code of length n is a nonempty subset of $\mathbb{F}_2^n$, where $\mathbb{F}_2=\{0,1\}$ is the field of two elements. If $x_i=(x_i(1),\ldots,x_i(n))\in\mathbb{F}_2^n$ for $i=1,2$, their Hamming distance $d(x_1,x_2)$ is the number of indices j for which $x_1(j)\neq x_2(j)$, and the weight $\mathrm{wt}(x)$ of $x\in\mathbb{F}_2^n$ is the number of nonzero coordinates in x. Suppose that C is an (n,M) code, i.e. $C\subseteq\mathbb{F}_2^n$ and $|C|=M$. The smallest of the pairwise Hamming distances $d(c_1,c_2)$ between different codewords $c_1,c_2\in C$ is called the minimum distance of the code C. If a code C is a linear subspace of $\mathbb{F}_2^n$, of dimension k, then the code C is linear and it is called an $[n,k]$ code.

We say that a code C is a μ-fold r-covering if for all $x\in\mathbb{F}_2^n$ we have

$$|B_r(x)\cap C|\geqslant\mu.$$

Here

$$B_r(x)=\{y\in\mathbb{F}_2^n\mid d(y,x)\leqslant r\}$$

denotes the Hamming sphere of radius r. The smallest r for which C is a μ-fold r-covering is called the *μ-fold covering radius* and is denoted by $\mathrm{CR}^\mu(C)$. If $\mu=1$, then

Correspondence to: Iiro Honkala, Department of Mathematics, University of Turku, 20500 Turku 50, Finland.

SSDI 0012-365X(92)00201-W

C is a 1-fold r-covering or briefly an r-covering and $\mathrm{CR}^1(C)$ is the covering radius $\mathrm{CR}(C)$ of C.

The covering radius of codes has been extensively studied in recent years (see e.g. [2, 15]). In constructing new codes from the known ones the amalgamated direct sum (ADS) construction introduced in [4] has turned out to be most useful. Using this construction we can efficiently combine two binary codes [4, 3]. In [5] the concept of a binary subnormal code was introduced. If the resulting code in the ADS construction is not required to be linear, it is sufficient to assume that one of the codes is subnormal and the other is normal [6]. These concepts have been generalized to nonbinary codes in [16] and in a different way in [17, 8, 18]. The concepts of normality and subnormality have also been studied in several other papers (see e.g. [7, 9–14, 19, 20]).

The problem of studying multiple coverings is a natural generalization of the covering radius problems of codes and has been discussed in [1, 21]. In this paper we first generalize subnormality and normality to multiple coverings in Section 2 and discuss how the ADS can be applied to multiple coverings. In Section 3 we study binary linear codes and show that many of them are in fact μ-fold normal in the sense of our definition. We show that if an $[n, k]$ code C is a μ-fold r-covering with $n \geqslant 2r+1$ and $r \leqslant 2$, then C is μ-fold normal. We also show that if an $[n, k]$ code C is a 2-fold r-covering with minimum distance $d=1$ and $r<n$, then C is 2-fold normal.

2. Basic definitions and results

Suppose that C is an (n, M) code which is a μ-fold r-covering. If $c \in C$, $x \in \mathbb{F}_2^n$ and $d(x, c) \leqslant r$, we say that c *r-covers* x, or simply that c covers x when r is clear from the context. So, C is a μ-fold r-covering if each point $x \in \mathbb{F}_2^n$ is r-covered by at least μ codewords.

When we study μ-fold coverings, we often want to know the distance from x to the nearest codewords of C. Assume that $x \in \mathbb{F}_2^n$ is given, and that the codewords $c_1, c_2, \ldots, c_M$ of C are indexed in such a way that

$$d(x, c_1) \leqslant d(x, c_2) \leqslant \cdots \leqslant d(x, c_M).$$

We then denote

$$d^t(x, C) = d(x, c_t).$$

So, $d^t(x, C)$ gives the tth smallest of the distances between x and the codewords of C. If $t > M$ we define $d^t(x, C) = \infty$ (cf. [12]).

We now generalize the concepts of subnormality and normality to μ-fold r-coverings.

Definition 2.1. Suppose C is a binary (n, M) code. We say that C has μ-fold subnorm S if there is a partition $C_1 \cup C_2$ of C such that

$$d^i(x, C_1) + d^{\mu+1-i}(x, C_2) \leqslant S \quad \text{for all } i = 1, 2, \ldots, \mu \text{ and } x \in \mathbb{F}_2^n. \tag{1}$$

If C has μ-fold subnorm $2r+1$ we say that C is a subnormal μ-fold r-covering. If C is a subnormal μ-fold $\mathrm{CR}^{\mu}(C)$-covering then C is called μ-fold subnormal.

It is clear that if C has μ-fold subnorm $2r+1$, then it is indeed a μ-fold r-covering: for any $x\in\mathbb{F}_2^n$ and $i=1,2,\ldots,\mu$, we have $d^i(x,C_1)\leqslant r$ or $d^{\mu+1-i}(x,C_2)\leqslant r$, and hence if $|B_r(x)\cap C_1|=t$ then $|B_r(x)\cap C_2|\geqslant\mu-t$.

On the other hand, if $C=C_1\cup C_2$ is any partition of a μ-fold r-covering C then, for all $i=1,2,\ldots,\mu$ and for all $x\in\mathbb{F}_2^n$, we have $d^i(x,C_1)\leqslant r$ or $d^{\mu+1-i}(x,C_2)\leqslant r$. This very important fact will be used repeatedly in Section 3. For example, if we know that $d^{\mu}(x,C_1)\leqslant r+1$ and $d^{\mu}(x,C_2)\leqslant r+1$ for $x\in\mathbb{F}_2^n$, then C is a subnormal μ-fold r-covering.

As usual (see [4]), we denote $C_a^{(i)}=\{c\in C\mid c(i)=a\}$, where $c(i)$ denotes the ith coordinate of $c\in\mathbb{F}_2^n$.

Definition 2.2. Suppose C is an (n,M) code. We say that C has μ-fold norm N if there is an index i such that

$$d^j(x,C_0^{(i)})+d^{\mu+1-j}(x,C_1^{(i)})\leqslant N \quad \text{for all } j=1,2,\ldots,\mu \text{ and } x\in\mathbb{F}_2^n. \tag{2}$$

If C has μ-fold norm $2r+1$ we say that C is a normal μ-fold r-covering. If C is a normal μ-fold $\mathrm{CR}^{\mu}(C)$-covering then C is called μ-fold normal.

As usual, we also say that a partition $C_1\cup C_2$ in (1) (resp. a coordinate i in (2)) is *acceptable* if it can be used to show that C has a given μ-fold subnorm (resp. norm) or that C is a subnormal (resp. normal) μ-fold r-covering.

Clearly, if C is a (sub)normal μ-fold r-covering then it is also a (sub)normal μ'-fold r'-covering for every $\mu'\leqslant\mu$ and $r'\geqslant r$. If a code C has at least two codewords then it is 1-fold (sub)normal if and only if it is (sub)normal in the usual sense [4, 3, 5].

By definition, a μ-fold (sub)normal code has at least 2μ codewords. For example, the code $\mathbb{F}_2^{2r}$ is a μ-fold r-covering for

$$\mu=\sum_{i=0}^{r}\binom{2r}{i}>M/2,$$

where $M=2^{2r}$ is the cardinality of this code. Therefore, this code is not μ-fold (sub)normal. In Section 3 we show for $r\leqslant 2$ that if an $[n,k]$ code C is a μ-fold r-covering and $n\geqslant 2r+1$, then C is μ-fold normal.

Example 2.3. If the codes $C_i\subseteq\mathbb{F}_2^n$ $(i=1,2,\ldots,k)$ are subnormal μ_i-fold r-coverings (normal μ_i-fold r-coverings with respect to the first coordinate) and $C_i\cap C_j=\emptyset$ when $i\neq j$, then their union $\bigcup C_i$ is a subnormal $(\mu_1+\mu_2+\cdots+\mu_k)$-fold r-covering (normal $(\mu_1+\mu_2+\cdots+\mu_k)$-fold r-covering with respect to the first coordinate).

Example 2.4. If the codes C_i $(i=1,2)$ are μ_i-fold r_i-coverings then their direct sum $C_1 \oplus C_2 = \{(a,b) \mid a \in C_1,\ b \in C_2\}$ is a $\mu_1\mu_2$-fold (r_1+r_2)-covering. In the following theorem we see how using the ADS we can save one coordinate compared to the direct sum.

Theorem 2.5. *Suppose that an (n_A, M_A) code A is a subnormal μ_A-fold r_A-covering with $A = A_1 \cup A_2$ acceptable, and that an (n_B, M_B) code B is a normal μ_B-fold r_B-covering with the first coordinate acceptable. Then the ADS of A and B,*

$$A \dot{\oplus} B = \{(a,b) \mid a \in A_1,\ (0,b) \in B\} \cup \{(a,b) \mid a \in A_2,\ (1,b) \in B\}$$

is an $(n_A + n_B - 1, M)$ code which is a subnormal $\mu_A\mu_B$-fold (r_A+r_B)-covering, where $M = |A_1| \cdot B_0^{(1)}| + |A_2| \cdot |B_1^{(1)}|$. If A is a normal μ_A-fold r_A-covering with the last coordinate acceptable and we choose $A_1 = A_0^{(n_A)}$ and $A_2 = A_1^{(n_A)}$, then $A \dot{\oplus} B$ is a normal $\mu_A\mu_B$-fold (r_A+r_B)-covering.

Proof. Denote $C = A \dot{\oplus} B$, and $C_1 = \{(a,b) \mid a \in A_1,\ (0,b) \in B\}$ and $C_2 = \{(a,b) \mid a \in A_2,\ (1,b) \in B\}$. Let $x \in \mathbb{F}_2^{n_A}$ and $y \in \mathbb{F}_2^{n_B-1}$ be arbitrary. By Definitions 2.1 and 2.2 we can find different words $a_1^1, a_2^1, \ldots, a_{\mu_A}^1 \in A_1$, $a_1^2, a_2^2, \ldots, a_{\mu_A}^2 \in A_2$ and $(0,b_1^0), (0,b_2^0), \ldots, (0,b_{\mu_B}^0) \in B_0^{(1)}$, $(1,b_1^1), (1,b_2^1), \ldots, (1,b_{\mu_B}^1) \in B_1^{(1)}$ such that

$$d(a_i^1, x) + d(a_i^2, x) \leqslant 2r_A + 1$$

and

$$d((0,b_j^0),(0,y)) + d((1,b_j^1),(0,y)) \leqslant 2r_B + 1.$$

Consequently, if we choose

$$c_{i,j}^1 = (a_i^1, b_j^0) \in C_1 \quad \text{and} \quad c_{i,j}^2 = (a_i^2, b_j^1) \in C_2,$$

then we have

$$\begin{aligned} &d(c_{i,j}^1,(x,y)) + d(c_{i,j}^2,(x,y)) \\ &\quad \leqslant d(a_i^1,x) + d((0,b_j^0),(0,y)) + d(a_i^2,x) + d((1,b_j^1),(0,y)) - 1 \\ &\quad \leqslant (d(a_i^1,x) + d(a_i^2,x)) + (d((0,b_j^0),(0,y)) + d((1,b_j^1),0,y))) - 1 \\ &\quad \leqslant 2r_A + 1 + 2r_B + 1 - 1 = 2(r_A + r_B) + 1, \end{aligned}$$

proving our first claim. The second claim follows immediately from the first. □

Remark. Clearly, if A and B in the previous theorem are linear, and A_1 is a linear subspace of A of dimension $\dim A - 1$ (in particular if A is a normal μ_A-fold r_A-covering with the last coordinate acceptable and $A_1 = A_0^{(n_A)}$ and $A_2 = A_1^{(n_A)}$), then $A \dot{\oplus} B$ is also linear.

Corollary 2.6. *Assume that an $[n_A, k_A]$ code A is a normal μ_A-fold r_A-covering with the last coordinate acceptable and an $[n_B, k_B]$ code B is a normal μ_B-fold r_B-covering with the*

first coordinate acceptable. Then there is an $[n_A+n_B-1, k_A+k_B-1]$ *code* $A \oplus B$ *that is a normal* $\mu_A\mu_B$*-fold* (r_A+r_B)*-covering.*

3. Normality results for binary linear codes

It is known that all binary linear $[n,k]$ codes with covering radius 3 or less are 1-fold normal (if $k>0$) (see [3, 11]). In this section we show that for $r=1$ and 2 all binary linear μ-fold r-coverings of length at least $2r+1$ are μ-fold normal. The proof is done in several steps. The case $r=1$ is easy and is discussed in Theorem 3.2. The case $r=2$ is divided into two parts: in Lemmas 3.4–3.6 we prove the result when the minimum distance of the code is one, and in Lemma 3.7 and Theorem 3.8 we prove it when the minimum distance is two.

In Theorem 3.3 we study 2-fold coverings and show that if C is a linear 2-fold r-covering of length n, $r<n$, and C has minimum distance one, then C is 2-fold normal.

Lemma 3.1. *Suppose* C *is a* μ*-fold* r*-covering with* $\mu \geqslant 2$ *and with minimum distance* d*. Then* $d \leqslant r$*.*

Proof. Any codeword of C must be r-covered by another codeword of C, and hence $d \leqslant r$ as claimed. □

From now on C will be a linear code of length n. If $x \in \mathbb{F}_2^n$ then the support of x is the set $\{i \mid x(i)=1\}$. In this section we will identify codewords with their supports. For example, $\{1,2\}$ will denote the word $(1,1,0,0,\ldots) \in \mathbb{F}_2^n$. If $x, y \in \mathbb{F}_2^n$ we will denote that $x \subseteq y$ if the support of x is a subset of the support of y.

Theorem 3.2. *If an* $[n,k]$ *code* C *is a* μ*-fold 1-covering and* $n \geqslant 3$*, then* C *is* μ*-fold normal.*

Proof. If $\mu=1$, then C had covering radius 0 or 1 and is normal by [3], i.e. 1-fold normal. Assume $\mu \geqslant 2$. Then $\mathrm{CR}^{\mu}(C)=1$.

If $C=\mathbb{F}_2^n$ then C is a normal μ-fold 1-covering with respect to every coordinate. Indeed, it suffices to consider $x=0^n$ (the all-zero word) in (2), and we have $x, \{2\}, \{3\}, \ldots, \{n\}, \{2,3\} \in C_0^{(1)}$ and $\{1\}, \{1,2\}, \{1,3\}, \ldots, \{1,n\}, \{1,2,3\} \in C_1^{(1)}$.

Suppose therefore that $C \neq \mathbb{F}_2^n$. Without loss of generality, $\{n\} \notin C$ and $\{1\} \in C$. We show that the first coordinate is acceptable.

Case 1: Suppose $x \in C$; w.l.o.g. again $x=0^n$. The point x is 1-covered by some $\mu-1$ codewords $x, \{i_1\}, \{i_2\}, \ldots, \{i_{\mu-2}\} \in C_0^{(1)}$ and by $\{1\} \in C_1^{(1)}$; hence $d^1(x, C_0^{(1)})=0$ and $d^{\mu-1}(x, C_0^{(1)})=1$. Furthermore, because $\mu \geqslant 2$, $\{n\}$ is covered by a word $\{n,i\}$, where $i \neq 1$ (because of the linearity of C, $i=1$ would imply $\{n\} \in C$, a contradiction). Hence $d^{\mu}(x, C_0^{(1)}) \leqslant 2$. Because $\{1\} \in C$ and C is linear, we have $d^i(x, C_1^{(1)}) \leqslant d^i(x, C_0^{(1)})+1$, and (2) follows for x.

Case 2: Suppose $x \notin C$; w.l.o.g. $x = \{n\}$. The point x is covered by μ codewords $0^n, \{n, j_1\}, \{n, j_2\}, \ldots, \{n, j_{\mu-1}\} \in C_0^{(1)}$; hence $d^\mu(x, C_0^{(1)}) \leqslant 1$ and $d^\mu(x, C_1^{(1)}) \leqslant 2$, proving (2) for x. □

Theorem 3.3. *If an $[n, k]$ code C is a 2-fold r-covering with minimum distance 1 and $r < n$, then C is 2-fold normal.*

Proof. We can assume $r = \mathrm{CR}^\mu(C)$. Because the minimum distance of C is 1 we can assume that $\{1\} \in C$. We show that the first coordinate of C is acceptable. Suppose $x \in \mathbb{F}_2^n$ and $d(x, C) = \min_{c \in C} d(x, c) = i$. Because C is linear we can assume that x has weight i and that $x(1) = 0$ (by adding a suitable codeword to x if necessary). Because $r < n$, we can choose $y \in \mathbb{F}_2^n$ of weight r such that $x \subseteq y$ and $y(1) = 0$. Then y is r-covered by a codeword $c \in C$, $c \neq 0^n$, $c \neq \{1\}$. By adding the word $\{1\}$ to c if necessary, we can assume that $c \in C_0^{(1)}$ and $d(x, c) \leqslant d(x, y) + d(y, c) \leqslant r - i + r = 2r - i$. Then $0^n, c \in C_0^{(1)}$, $\{1\}, \{1\} + c \in C_1^{(1)}$, $d^1(x, C_0^{(1)}) + d^2(x, C_1^{(1)}) \leqslant d(x, 0^n) + d(x, \{1\} + c) \leqslant i + 2r + 1 - i = 2r + 1$ and $d^2(x, C_0^{(1)}) + d^1(x, C_1^{(1)}) \leqslant d(x, c) + d(x, \{1\}) \leqslant 2r - i + i + 1 = 2r + 1$. □

Lemma 3.4. *Assume that an $[n, k]$ code C is a μ-fold 2-covering and $n \geqslant 5$, and that $\{1\} \in C$. If $x \in \mathbb{F}_2^n$, $\mathrm{wt}(x) = 1$ and $d(x, C) = 1$, then $|C_0^{(1)} \cap B_3(x)| \geqslant \mu$.*

Proof. The proof consists of five steps.

Step 1: Denote by t ($t \geqslant 1$) the number of words of weight 1 in C. Then w.l.o.g. these t words are $\{1\}, \{2\}, \ldots, \{t\}$ and $C = \mathbb{F}_2^t \oplus C'$, where $C' \subseteq \mathbb{F}_2^{n-t}$. Without loss of generality further $x = \{t+1\}$. Denote

$$\mathscr{S} = \{c \in C \mid \{t+1\} \subseteq c \subseteq \{t+1, \ldots, n\},\ \mathrm{wt}(c) = 2\},$$

$$\mathscr{U} = \{c \in C \mid \{t+1\} \subseteq c \subseteq \{t+1, \ldots, n\},\ \mathrm{wt}(c) = 3\},$$

and

$$s = |\mathscr{S}|, \qquad u = |\mathscr{U}|.$$

Then x is 2-covered by exactly $F := 1 + t + u + (1+t)s$ codewords of C. Indeed if we denote $\mathscr{T} = \{\{1\}, \{2\}, \ldots, \{t\}\} \subseteq \mathbb{F}_2^n$, then x is covered by 0^n and by the words in $\mathscr{T}, \mathscr{U}, \mathscr{S}$ and $\mathscr{T} + \mathscr{S} = \{a + b \mid a \in \mathscr{T},\ b \in \mathscr{S}\}$. Only $1 + s$ of these F words belong to $C_1^{(1)}$ and therefore $|C_0^{(1)} \cap B_2(x)| = F - 1 - s$. If there is a codeword $z \subseteq \{t+1, \ldots, n\}$ of C of weight 2 such that $z \notin \mathscr{S}$ and z is not a sum of two words in $\mathscr{S}$, then z itself and the words in $z + \mathscr{S} = \{z + b \mid b \in \mathscr{S}\}$ clearly belong to $C_0^{(1)} \cap B_3(x)$ and hence $|C_0^{(1)} \cap B_3(x)| \geqslant F - 1 - s + 1 + s = F \geqslant \mu$ and we are done. We can therefore in the rest of the proof assume that

$$\begin{aligned} &\text{if } z \in C,\ \mathrm{wt}(z) = 2,\ z \subseteq \{t+1, \ldots, n\} \text{ and } z \notin \mathscr{S} \\ &\quad \text{then } z \text{ is the sum of two words in } \mathscr{S}. \end{aligned} \tag{3}$$

Step 2: If $n - t \leqslant 1$ then $C = \mathbb{F}_2^t \oplus \{0\}$ (because $d(x, C) = 1$) and $\{t+1\}$ is 2-covered by exactly $t+1$ words in C. Now $n \geqslant 5$ implies that $t \geqslant 4$ and $|C_0^{(1)} \cap B_3(x)| \geqslant 1 + (t-1) + \binom{t-1}{2} \geqslant t + 1$. Hence we can asume $n - t \geqslant 2$.

Step 3: Assume now that there is an index j, $t+1<j\leqslant n$, such that $\{t+1,j\}\notin C$ (and hence $\{j\}$ is not 2-covered by any $c\in C$ of weight 2 such that $c\subseteq\{t+1,\dots,n\}$ by (3)) and that for all h, $t+1<h\leqslant n$, we have $\{t+1,j,h\}\notin C$. We consider the words in C that 2-cover $\{t+1,j\}$. By our assumptions the only words in C of weight 2 or less that 2-cover $\{t+1,j\}$ are 0^n, the words in $\mathscr{S}$, and all the other, say M, words $c\in C$ that 2-cover $\{t+1,j\}$ have weight 4 and satisfy $c(1)=\cdots=c(t)=0$. Hence $M+s+1\geqslant\mu$ and, consequently, $M\geqslant\mu-s-1\geqslant\mu-F+1+s$ because $F\geqslant 2s+2$. These words together with the $F-1-s$ previously found words show that $|C_0^{(1)}\cap B_3(x)|\geqslant\mu$.

Step 4: By step 3 and (3) we can assume that the s words in $\mathscr{S}$ are $\{t+1,t+2\}$, $\{t+1,t+3\},\dots,\{t+1,t+s+1\}$ and the u words in $\mathscr{U}$ are $\{t+1,t+s+2,t+s+3\}$, $\{t+1,t+s+4,t+s+5\},\dots,\{t+1,n-1,n\}$. Indeed, because there are no words of weight 1 in C' it is clear that $d(\mathscr{S},\mathscr{U})=\min\{d(a,b)\mid a\in\mathscr{S},\ b\in\mathscr{U}\}\geqslant 3$, and if two words in $\mathscr{U}$ were only Hamming distance 2 apart then their sum would be a sum of two words in $\mathscr{S}$ by (3), contradicting $d(\mathscr{S},\mathscr{U})\geqslant 3$.

Assume that $u\geqslant 1$ and $\{t+1,n-1,n\}\in\mathscr{U}$. The word $\{n\}$ is 2-covered only by 0^n, the words in $\mathscr{T}$, by $\{t+1,n-1,n\}$ and the s words $\{t+1,n-1,n\}+\mathscr{S}$ and by some K words $c\in C$ of weight 3 for which $c\cap\{t+1,n-1,n\}=\{n\}$ (there are no words $c\subseteq\{t+1,\dots,n\}$, for which $c\cap\{t+1,n-1,n\}=\{t+1,n\}$ by the assumption at the beginning of step 4). Therefore $1+t+1+s+K\geqslant\mu$. If $u\geqslant 2$ then $F\geqslant 2s+t+3$ and $K\geqslant\mu-s-t-2=\mu-(2s+t+3)+1+s\geqslant\mu-F+1+s$. All these K codewords c satisfy $c(1)=0$ because $\{n\}$ is not covered by any codewords $a\in C$ of weight 1 or 2 such that $a\subseteq\{t+1,\dots,n\}$ (by (3)). These codewords added to $\{t+1,n-1,n\}$ together with the $F-1-s$ words of C found in step 1 again show that $|C_0^{(1)}\cap B_3(x)|\geqslant\mu$.

Step 5: By step 4 we can assume that $u\leqslant 1$. If $s\geqslant 3$ then the $F-1-s$ words found in step 1 and the words in $\mathscr{S}+\mathscr{S}\backslash\{0^n\}$ and $\mathscr{S}+\mathscr{S}+\mathscr{S}\backslash\mathscr{S}$ prove our claim because $\binom{s}{2}+\binom{s}{3}\geqslant 1+s$. Hence we may also assume $s\leqslant 2$. Now step 3 (or what is said at the beginning of step 4) implies that $n-t\leqslant 5$. Now there are only the following possibilities (w.l.o.g.): (1) $n-t=2$ and C' is generated by 11; (2) $n-t=3$, C' generated by the words 110, 101 ($t=2$ implies $\mu\leqslant 7$; $t\geqslant 3$ is clear); (3) $n-t=3$, C' generated by 111; (4) $n-t=4$, C' generated by 1110, 1001 ($t=1$ implies $\mu\leqslant 3$; $t=2$ implies $\mu\leqslant 5$; $t\geqslant 3$ is clear); (5) $n-t=5$, C' generated by 11100, 10010, 10001 ($t=1$ implies $\mu\leqslant 5$; $t=2$ implies $\mu\leqslant 7$; $t\geqslant 3$ is clear). It is easy to check our claim in each of these cases using the assumption $n\geqslant 5$. □

Lemma 3.5. *Assume that an* $[n,k]$ *code* C *is a* μ*-fold 2-covering,* $k<n$, $n\geqslant 5$ *and that* $\{1\}\in C$. *Then*

$$|C_0^{(1)}\cap B_3(0^n)|\geqslant\mu-1.$$

Proof. Because $C\neq\mathbb{F}_2^n$ we can again assume that $\{1\},\{2\},\dots,\{t\}\in C$ and $\{t+1\},\dots,\{n\}\notin C$ and use the same notation as in step 1 of the proof of the previous lemma. If $u\geqslant 1$ (resp. $s\geqslant 3$) then the $F-1-s$ words in $C_0^{(1)}\cap B_2(x)$ (we again denote $x=\{t+1\}$) found in step 1 together with the words in $u+\mathscr{S}$ for any $u\in\mathscr{U}$ (resp.

$\mathscr{S}+\mathscr{S}$) prove our claim. We can therefore assume $u=0$ and $s\leqslant 2$. If $s=0$ we are already done. Using again the points in $\mathscr{S}+\mathscr{S}$ we see that $|C_0^{(1)}\cap B_3(0^n)|\geqslant F-1-s+s-1\geqslant F-2$. If $F>\mu$ we are done. On the other hand, if $F=\mu$, $s=1$ or 2 and $n-t\geqslant 4$, then there is a point $\{n\}$ not 2-covered by any word in $\mathscr{S}$ and therefore there is a word $c\in C$, $c\subseteq\{t+1,\ldots,n\}$ of weight 2 or 3 that 2-covers $\{n\}$, and we are done. If $n-t\leqslant 3$, $u=0$, $s=1$ or 2, $F=\mu$ and $n\geqslant 5$, it is again easy to check the remaining cases. □

Lemma 3.6. *Assume that an $[n,k]$ code C is a μ-fold 2-covering with minimum distance 1 and $n\geqslant 5$. Then C is a normal μ-fold 2-covering.*

Proof. Without loss of generality, $\{1\}\in C$. Let $x\in\mathbb{F}_2^n$ be arbitrary. We show that (2) holds for $i=1$, $N=5$. We know that $d(x,C)\leqslant 2$. Because C is linear, we can assume that $\mathrm{wt}(x)\leqslant 2$ and $x(1)=0$.

If $C=\mathbb{F}_2^n$ then it is easy to check that $\mu\leqslant 1+n+\binom{n}{2}$, $|C_0^{(1)}\cap B_3(0^n)|\geqslant\binom{n}{2}+n$, $|C_0^{(1)}\cap B_4(0^n)|\geqslant\binom{n}{2}+n+1$, $|C_1^{(1)}\cap B_3(0^n)|\geqslant\binom{n}{2}+1$, $|C_1^{(1)}\cap B_4(0^n)|\geqslant\binom{n}{2}+n$ and $|C_1^{(1)}\cap B_5(0^n)|\geqslant\binom{n}{2}+n+1$, which shows that the normality condition (2) holds for $x=0^n$. We can therefore assume that $C\neq\mathbb{F}_2^n$ and that there is a word $y\in\mathbb{F}_2^n$ such that $d(y,C)=1$. We use the same notations as in Lemmas 3.4 and 3.5 and assume that $\{1\},\ldots,\{t\}\in C$, $\{t+1\},\ldots,\{n\}\notin C$ for some t, $1\leqslant t<n$.

If $x=0^n$ then $d^1(x,C_0^{(1)})=0$, $d^1(x,C_0^{(1)})=1$, $d^{\mu-1}(x,C_0^{(1)})\leqslant 3$ by Lemma 3.5, and $d^\mu(x,C_0^{(1)})\leqslant d^\mu(\{t+1\},C_0^{(1)})+1\leqslant 4$ by Lemma 3.4. Similarly, $d^1(x,C_1^{(1)})=1$, $d^{\mu-t}(x,C_1^{(1)})\leqslant 3$ (because clearly $|B_2(\{1\})\cap C_1^{(1)}|\geqslant\mu-t$), $d^{\mu-1}(x,C_1^{(1)})\leqslant d^{\mu-1}(x,C_0^{(1)})+1\leqslant 4$ by Lemma 3.5, and finally $d^\mu(x,C_1^{(1)})\leqslant d^\mu(\{t+1\},C_0^{(1)})+2\leqslant 5$ by Lemma 3.4, This shows that (2) holds for $x=0^n$.

Similarly, if $x=\{t+1\}$, we have $d^{s+1}(x,C_0^{(1)})\leqslant 1$ (by the definition of s in Lemma 3.4), $d^\mu(x,C_0^{(1)})\leqslant 3$ by Lemma 3.4, $d^{\mu-1-s}(x,C_1^{(1)})\leqslant 3$ (because $|C_0^{(1)}\cap B_2(x)|\geqslant\mu-1-s$ by the proof of Lemma 3.4) and $d^\mu(x,C_1^{(1)})\leqslant d^\mu(x,C_0^{(1)})+1\leqslant 4$ by Lemma 3.4. Therefore (2) holds for x.

It remains to check that (2) holds if $d(x,C)=2$ and x has weight 2. Without loss of generality, $x=\{t+1,t+2\}$. Because $d(x,C)=2$ and $x(1)=0$, we know that x cannot be 2-covered by any $c\in C$ with $c(1)=1$. Hence $d^\mu(x,C_0^{(1)})\leqslant 2$ and $d^\mu(x,C_1^{(1)})\leqslant d^\mu(x,C_0^{(1)})+1\leqslant 3$, completing the proof of Lemma 3.6. □

Lemma 3.7. *Assume that an $[n,k]$ code C is a μ-fold 2-covering with minimum distance 2 and $n\geqslant 5$, $\mu\geqslant 2$, and that $\{1,2\}\in C$. If $d(x,C)=1$ then (2) holds for x when $i=1$ and $N=5$.*

Proof. Because C is linear we can w.l.o.g. assume that $\mathrm{wt}(x)=1$ and that $x(1)=0$. Denote by s (resp. u) the number of codewords of C of weight 2 (resp. 3) that 2-cover x. Denote the corresponding sets by $\mathscr{S}$ and $\mathscr{U}$, respectively. Then x is covered by the all-zero word 0^n and these $s+u$ words and by no others.

Case 1: Assume first that $x=\{2\}$. Then $d^1(x, C_1^{(1)})=1$, $d^s(x, C_0^{(1)})=1$, $d^{\mu-1}(x, C_0^{(1)})\leqslant 2$ (all the words in $B_2(x)\cap C$ except $\{1, 2\}$ belong to $C_0^{(1)}$). We next show that $d^{\mu-s}(x, C_1^{(1)})\leqslant 3$. Namely, the word $\{1,2\}$ is 2-covered by 0^n and by itself, by some words $c\in C$ of weight 3 or 4 for which necessarily $c(1)=1$ and by the words $\{1,j\}, \{2,j\}$ for some $s-1$ indices $j\neq 1, 2$, thus proving our claim.

Finally, we show that $d^{\mu}(x, C_1^{(1)})\leqslant 4$, which then also implies that $d^{\mu}(x, C_0^{(1)})\leqslant 4$ (add $\{1,2\}$ to the words in $B_4(x)\cap C_1^{(1)}$). Because every codeword $c\in C$, $c\neq 0^n$, that 2-covers $\{1\}$ satisfies $c(1)=1$ we have $|B_4(x)\cap C_1^{(1)}|\geqslant \mu-1$. We show that there is at least one more codeword in $B_4(x)\cap C_1^{(1)}$. If $\{j_1, j_2\}\in C$ for some $j_1>j_2>2$, then $\{1, 2, j_1, j_2\}\in C$ and we are done. We can assume that no such codeword $\{j_1, j_2\}$ exists. In particular, $s\leqslant 2$. Assume $s=2$, and that the other word of weight two 2-covering $\{2\}$ is $\{2, 3\}$. Then there are only three codewords of weight 2 in C, and hence $\mu\leqslant |B_2(0^n)\cap C|=4$. If $\mu=2$ the claim follows because $\{1,2\}, \{1,3\}\in B_4(x)\cap C_1^{(1)}$; if $\mu=3$ (resp. 4) then $\{n\}$ is 2-covered by a word c (resp. by two words c_1, c_2) of weight 3 in $C_0^{(1)}$ and $\{1,2\}, \{1,3\}$ and $\{1,2\}+c$ (resp. $\{1,2\}+c_1, \{1,2\}+c_2$) belong to $B_4(x)\cap C_1^{(1)}$. Finally, if $s=1$, then $\mu=2$ and the same argument as before (consider $\{n\}$) proves our claim.

Case 2: Assume that $x=\{n\}$ and that $\{1, n\}\notin C$. We have $d^{\mu-s-1}(x, C_1^{(1)})\leqslant 3$ because all the words in $B_2(\{1, n\})\cap C$ belong to $B_3(x)\cap C_1^{(1)}$ except 0^n and the s words of weight 2 that 2-cover x. Clearly, $d^{s+1}(x, C_0^{(1)})=1$.

We next show that $d^{\mu}(x, C_0^{(1)})\leqslant 3$. Denote $\mathscr{U}_i=\mathscr{U}\cap C_i^{(1)}$, $i=0, 1$. Clearly, $\{0^n\}\cup\mathscr{S}\cup\mathscr{U}_0\cup(\mathscr{U}_1+\mathscr{U}_1)\subseteq B_3(x)\cap C_0^{(1)}$; hence $|B_3(x)\cap C_0^{(1)}|\geqslant \mu-1$. Furthermore, if $|\mathscr{U}_1|\geqslant 3$ we are done. Assume therefore that $|\mathscr{U}_1|\leqslant 2$. If $s\geqslant 2$ then there are two indices j_1, j_2 such that $\{j_1, n\}, \{j_2, n\}\in C$ and hence $\{j_1, j_2\}\in C$, thus proving our claim ($\{j_1, j_2\}\notin \mathscr{U}_1+\mathscr{U}_1$ because the minimum distance of C is two). If $|\mathscr{U}_1|=2$ and $s=1$, then there are some codewords $\{1, j_1, n\}, \{1, j_2, n\}, \{j_3, n\}\in C$ and their sum belongs to $B_3(x)\cap C_0^{(1)}$. Hence we can assume that (1) $|\mathscr{U}_1|\leqslant 1$ and $s\leqslant 1$, or (2) $|\mathscr{U}_1|=2$ and $s=0$. First suppose (1). If there are indices j_1, j_2, $1\neq j_1\neq n$, $1\neq j_2\neq n$, such that $\{j_1, j_2\}\in C$ we are done. In particular, we can assume that $\{1,2\}$ is the only codeword of weight 2 that does not belong to $\mathscr{S}$. If $s=0$ (resp. $s=1$) then $\mu\leqslant 2$ (resp. $\mu\leqslant 3$). If $\mu<2$ (resp. $\mu<3$) we are already done; if $\mu=2$ (resp. $\mu=3$) then there is a word $c\in\mathscr{U}$, $c\in C_0^{(1)}$ or $c+\{1,2\}\in C_0^{(1)}$ which, together with 0^n (resp. 0^n and the word in $\mathscr{S}$), prove our claim. Then suppose (2) instead of (1). If the two words in $\mathscr{U}_1$ are $\{1, j_i, n\}$, $i=1, 2$, then their sum $\{j_1, j_2\}\in C$ has weight 2 and $j_1, j_2\geqslant 3$. If there is any other $c\in C$ of weight 2 satisfying $c(1)=0$ we are again done. In particular, we can again assume that the only $c\in C$ of weight 2 for which $c(1)=1$ is the word $\{1,2\}$. Hence 0^n is 2-covered by only three codewords of C and $\mu\leqslant 3$. Now the claim follows from $\{0^n\}\cup(\{1,2\}+\mathscr{U}_1)\subseteq B_3(x)\cap C_0^{(1)}$.

Finally, we show that $d^{\mu}(x, C_1^{(1)})\leqslant 4$. The word $\{1\}$ is 2-covered by $\mu-1$ codewords $c_1=\{1,2\}, c_2, \ldots, c_{\mu-1}\in C_1^{(1)}$ of weight 2 or 3. We show that there is at least one more codeword in $B_4(x)\cap C_1^{(1)}$. If $\{j, n\}\in C$ for some j, then $\{1, n\}\notin C$ implies that $j\geqslant 3$ and $\{1,2\}+\{j, n\}$ will do. Assume that no such j exists. If there is no word $\{1, k, n\}$ in C, $1<k<n$, then none of the words c_i 2-covers $\{n\}$ and there is a word $c_0=\{j_1, j_2, n\}\in C$, $3\leqslant j_1<j_2<n$ (if $j_1=2$, adding c_1 would yield a codeword of the form $\{1, k, n\}$), and

c_0+c_1 will do. Hence we assume that there does exist a word $\{1,k,n\}\in C$ (then $k\geqslant 3$, otherwise $\{n\}$ would be a codeword). If $\{1,h\}\in C$ for some $h\geqslant 3$, then $h\neq k$ because the minimum distance of C is 2, and $\{1,k,n\}+\{1,h\}+\{1,2\}$ will do. Assume therefore that no such h exists. If $\mu=2$ we are already done, because $\{1,2\},\{1,k,n\}\in B_4(x)\cap C_1^{(1)}$; hence consider the case $\mu\geqslant 3$. Then the word 0^n has to be covered by another codeword of C of weight 2, say $\{k_1,k_2\}$, and $3\leqslant k_1<k_2<n$. If there exists such a word for which $k_1\neq k\neq k_2$ then $\{1,k,n\}+\{k_1,k_2\}$ will do. If for every such word $k_1=k$ or $k_2=k$ then there exists only one such word, and consequently there are only two words of weight 2 in C. Then $\mu=3$ and we are done because $\{1,2\},\{1,k,n\}$, $\{1,k,n\}+\{k_1,k_2\}\in B_4(x)\cap C_1^{(1)}$. □

Theorem 3.8. *If an $[n,k]$ code C is a μ-fold 2-covering with $n\geqslant 5$, then C is μ-fold normal.*

Proof. If $\mu=1$ then C is 1-fold normal by [3]. Hence assume $\mu\geqslant 2$. If C is a μ-fold 1-covering then the result follows from Theorem 3.2. We can assume $\mathrm{CR}^{\mu}(C)=2$. If the minimum distance of C is 1, then the result follows from Lemma 3.6. We can therefore assume that the minimum distance of C equals 2 and that $\{1,2\}\in C$. We show that the first coordinate is acceptable by showing that (2) holds for all $x\in\mathbb{F}_2^n$ when $i=1$ and $N=5$. If $d(x,C)=1$ this has already been shown in the previous lemma. It remains to consider the cases $x\in C$ and $d(x,C)=2$.

Case 1: Assume $d(x,C)=2$. By adding a suitable codeword to x if necessary, we can assume that $\mathrm{wt}(x)=2$ and that $x(1)=0$. It is easy to check that every $c\in C$ that 2-covers the point $y=x+\{1\}$ satisfies $c(1)=1$. Indeed, this is immediate if $\mathrm{wt}(c)\geqslant 4$, and if $\mathrm{wt}(c)=2$ or 3 and $c(1)=0$ then $x\subseteq c$, contradicting our assumption $d(x,C)=2$. Therefore $d^{\mu}(x,C_1^{(1)})\leqslant 3$. Adding $\{1,2\}$ to these (at least) μ words in $B_2(y)$ shows that $d^{\mu}(x.C_0^{(1)})\leqslant 3$, completing the proof of case 1.

Case 2: Assume $x\in C$; w.l.o.g. $x=0^n$. Every codeword $c\in C$, $c\neq 0^n$, that 2-covers $\{1\}$ belongs to $C_1^{(1)}$. Therefore $d^{\mu-1}(x,C_1^{(1)})\leqslant 3$. It suffces to show that $d^{\mu}(x,C_0^{(1)})\leqslant 3$, which then implies $d^{\mu}(x,C_1^{(1)})\leqslant 5$ because $\{1,2\}\in C$. Every codeword $c\in C$ that 2-covers $\{2\}$ satisfies $c(1)=0$ except $\{1,2\}$. Therefore $|B_3(x)\cap C_0^{(1)}|\geqslant \mu-1$. If there exists a word $\{j_1,j_2\}\in C$, $2<j_1<j_2$, or a word $\{j_1,j_2,j_3\}\in C$, $2<j_1<j_2<j_3$, we are done. Assume that no such codewords exist. Suppose there is another word of weight 2, the word $\{2,3\}$ say, that 2-covers $\{2\}$. Because $\{4\}$ must be 2-covered by a codeword in $C\backslash\{0^n\}$, we can assume that $\{2,4\}\in C$ or $\{2,4,j\}\in C$ for some $j>4$ (we can add $\{1,2\}$ if necessary), but then adding $\{2,3\}$ to this codeword proves our claim. Hence we can assume that the only codeword of C of weight 2 is $\{1,2\}$, and thus $\mu=2$. Then there exists a word $c\in C$ of weight 3 that 2-covers $\{n\}$ and c or $\{1,2\}+c$ together with 0^n prove our claim. □

Acknowledgment

The author would like to thank the referees for useful comments.

References

[1] R.F. Clayton, Multiple packings and coverings in algebraic coding theory, Ph.D. Thesis, Univ. of California, Los Angeles, 1987.

[2] G.D. Cohen, M.R. Karpovsky, H.F. Mattson Jr and J.R. Schatz, Covering radius — survey and recent results, IEEE Trans. Inform. Theory 31 (1985) 328–343.

[3] G.D. Cohen, A.C. Lobstein and N.J.A. Sloane, Further results on the covering radius of codes, IEEE Trans. Inform. Theory 32 (1986) 680–694.

[4] R.L. Graham and N.J.A. Sloane, On the covering radius of codes, IEEE Trans. Inform. Theory 31 (1985) 385–401.

[5] I.S. Honkala, Lower bounds for covering codes, IEEE Trans. Inform. Theory 34 (1988) 326–329.

[6] I.S. Honkala, Modified bounds for covering codes, IEEE Trans. Inform. Theory 37 (1991) 351–365.

[7] I.S. Honkala, All binary codes with covering radius one are subnormal, Discrete Math. 94 (1991) 229–232.

[8] I.S. Honkala, On (k, t)-subnormal covering codes, IEEE Trans. Inform. Theory 37 (1991) 1203–1206.

[9] I.S. Honkala, On $(q, 1)$-subnormal q-ary covering codes, Discrete Appl. Math. to appear.

[10] I.S. Honkala and H.O. Hämäläinen, Bounds for abnormal binary codes with covering radius one, IEEE Trans. Inform. Theory 37 (1991) 372–375.

[11] X. Hou, Some results on the norm of codes, IEEE Trans. Inform. Theory 36 (1990) 683–685.

[12] X. Hou, Binary linear quasi-perfect codes are normal, IEEE Trans. Inform. Theory 37 (1991) 378–379.

[13] K.E. Kilby and N.J.A. Sloane, On the covering radius problem for codes I. Bounds on normalized covering radius, SIAM J. Algebraic Discrete Methods 8 (1987) 604–618.

[14] K.E. Kilby and N.J.A. Sloane, On the covering radius problem for codes II. Codes of low dimension; normal and abnormal codes, SIAM J. Algebraic Discrete Methods 8 (1987) 619–627.

[15] J.H. van Lint, Recent results on covering problems, in: T. Mora, ed., Applied Algebra, Algebraic Algorithms and Error-Correcting Codes: Proc. 6th Internat. Conf. AAECC-6, Rome, Italy, 1988 (Springer, Berlin, 1989) 7–21.

[16] A.C. Lobstein and G.J.M. van Wee, On normal and subnormal q-ary codes, IEEE Trans. Inform. Theory 35 (1989) 1291–1295; 36 (1990) 1498.

[17] P.R.J. Östegård, Upper bounds for q-ary covering codes, IEEE Trans. Inform. Theory 37 (1991) 660–664.

[18] P.R.J. Östergård, Further results on (k, t)-subnormal covering codes, IEEE Trans. Inform. Theory 38 (1992) 206–210.

[19] N.J.A. Sloane, A new approach to the covering radius of codes, J. Combin. Theory 42 Ser. A (1986) 61–86.

[20] G.J.M. van Wee, More binary covering codes are normal, IEEE Trans. Inform. Theory 36 (1990) 1466–1470.

[21] G.J.M. van Wee, G.D. Cohen and S.N. Litsyn, A note on perfect multiple coverings of the Hamming space, IEEE Trans. Inform. Theory 37 (1991) 678–682.