Combinatorial lower bounds on binary codes with covering radius one

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

Abstract

We give a short survey of the best known lower bounds on $K(n,1)$, the minimum cardinality of a binary code of length n and covering radius 1. Then we prove new lower bounds on $K(n,1)$, e.g.

$$K(n,1) \geq \frac{(5n^2-13n+66)2^n}{(5n^2-13n+46)(n+1)} \text{ when } n \equiv 5 \pmod 6,$$

which lead to several numerical improvements.

1 Introduction and survey of known results

A binary code $C \subseteq \mathbf{F}_2^n$ has covering radius R if R is the smallest integer such that every word in $\mathbf{F}_2^n$ is withing Hamming distance R from at least one codeword. The problem of determining $K(n,R)$, the smallest cardinality of a binary code of length n and covering radius R has been widely studied in recent years. In this paper we study lower bounds for this function. The most interesting case is $R=1$, which is easier than the larger values of R and has been studied in a number of papers, like [1], [6], [8], [7], [2], [5], [4] and [3].

Let $B_s(x) = \{y \in \mathbf{F}_2^n \mid d(y,x) \leq s\}$ and denote its cardinality by $V(n,s)$. Trivially,

$$K(n,1) \geq \frac{2^n}{n+1}. \tag{1}$$

Some lower bounds use the function $A(n,3)$, the largest possible cardinality of a binary code of length n and minimum distance 3. Cohen, Lobstein and Sloane [1] showed that for $n \geq 2$

$$K(n,1) \geq \frac{2^n - 2A(n,3)}{n-1}. \tag{2}$$

ARS COMBINATORIA 50(1998), pp. 149-159

Most of the bounds are based on the concept of *excess* introduced in [6]. From now on we assume that C is a given code of length n and covering radius 1.

As in [6], define

$$E_C(x) = |B_1(x) \cap C| - 1$$

and more generally for an arbitrary subset $V \subseteq \mathbf{F}_2^n$

$$E_C(V) = \sum_{x \in V} E_C(x), \tag{3}$$

or equivalently

$$E_C(V) = \sum_{c \in C} |B_1(c) \cap V| - |V|. \tag{4}$$

In particular,

$$E_C(\mathbf{F}_2^n) = |C|(n+1) - 2^n. \tag{5}$$

Because C is fixed we usually drop the subscript C. As usual, we denote

$$Z_i = \{x \in \mathbf{F}_2^n | E(x) = i\}$$

and

$$Z = \{x \in \mathbf{F}_2^n | E(x) > 0\}.$$

Then we can equivalently write

$$E(V) = \sum_{i>0} i|Z_i \cap V|.$$

Using the fact that for given x, every sphere $B_1(c)$, $c \in C$ intersects $B_1(x)$ in exactly $n+1$, 2 or 0 points, van Wee [6] showed that if n is even, then (4) implies that for every $x \notin C$

$$E(B_1(x)) \equiv 1 \pmod 2, \tag{6}$$

and

$$K(n,1) \geq \frac{2^n}{n} \text{ if } n \text{ is even.} \tag{7}$$

Similarly, by considering the excess on spheres of radius two he showed that

$$K(n,1) \geq \frac{(V(n,2)+2)2^n}{V(n,2)(n+1)} \text{ if } n \equiv 2 \pmod 3 . \tag{8}$$

Because for even values of n we can use (7) which is always at least as good as (8), we only need (8) when $n \equiv 5 \pmod 6$.

By considering simultaneously the excesses on spheres of radius one and two it was proved by van Wee [7] that

$$K(n,1) \geq \frac{(V(n,2)+5)2^n - 3(A(n,3)-1)(n+1)}{V(n,2)(n+1)} \tag{9}$$

for every $n \equiv 5 \pmod 6$. This gives at least as good a lower bound as (8) for all n. Honkala [4] showed that we further obtain

$$K(n,1) \geq \frac{(V(n,2)+5)2^{n+1} - 9A(n,3)(n+1)}{(2V(n,2)-3)(n+1)} \tag{10}$$

for every n with $n \equiv 5 \pmod 6$.

Other lower bounds on $K(n,1)$ have been calculated by Zhang [8] and Habsieger [2].

By considering the excess on spheres of radius s, Honkala [5] showed that if $n+1$ is divisible by an odd prime $s+1$, then

$$E(B_s(x)) \equiv -1 \pmod{s+1} \tag{11}$$

and

$$K(n,1) \geq \frac{(V(n,s)+s)2^n}{V(n,s)(n+1)}.$$

Recently, Habsieger [3] showed that one can obtain further improvements by considering the excess on the sets $S_i(x) = \{y \in \mathbf{F}_2^n | d(y,x) = i\}$. We denote

$$\delta_i(x) := E(S_i(x)).$$

By (5),

$$\sum_{x \in \mathbf{F}_2^n} \delta_i(x) = \binom{n}{i} \sum_{x \in \mathbf{F}_2^n} E(x) = \binom{n}{i}(|C|(n+1) - 2^n). \tag{12}$$

Habsieger showed that

$$K(n,1) \geq \frac{(5n^2-7n+24)2^n}{(5n^2-7n+4)(n+1)} \text{ when } n \equiv 5 \pmod 6, \tag{13}$$

and

$$K(n,1) \geq \frac{(4V(n,4)+5V(n,3)+36)2^n}{(4V(n,4)+5V(n,3))(n+1)} \text{ when } n \equiv 19, 39 \pmod{60}. \tag{14}$$

Several other improvements on $K(n,1)$ for specific values of n were also proved; likewise other similar general formulas not giving any further improvements in the range $n \leq 33$.

In this paper we further improve the results in [3] by using the same approach and suitable combinatorial counting arguments. In particular, we show that

$$K(n,1) \geq \frac{(5n^2-13n+66)2^n}{(5n^2-13n+46)(n+1)} \text{ when } n \equiv 5 \pmod 6, n \geq 11,$$

which gives at least as good a lower bound as (13) for all $n \geq 11$. We obtain the numerical results

$$K(23,1) \geq 352448, K(29,1) \geq 17988086.$$

We also improve on (14) slightly and show that

$$K(n,1) \geq \frac{(2V(n,4)+5V(n,3)+28)2^n}{(2V(n,4)+5V(n,3))(n+1)} \text{ when } n \equiv 19, 39 \pmod{60} \tag{15}$$

which always gives at least as good a lower bound as (14). This bound implies that $K(27,1) \geq 4793641$. We furthermore show that $K(19,1) \geq 26261$.

2 The case $n \equiv 5 \pmod 6$

We now show how a combinatorial argument can be used to sharpen [3, Theorem 7]. Assume that $n \equiv 5 \pmod 6$ and that $n \geq 11$.

By [6],

$$\delta_0(x) + \delta_1(x) \equiv 0 \pmod 2 \tag{16}$$

and

$$\delta_0(x) + \delta_1(x) + \delta_2(x) \equiv 2 \pmod 3 \tag{17}$$

for all $x \in \mathbf{F}_2^n$. Indeed, the proof used to obtain (6) immediately gives (16), when n is odd. The congruence (17) is obtained in the same way by considering $E(B_2(x))$.

Therefore as in [3],

$$5\delta_0(x) + 5\delta_1(x) + 2\delta_2(x) \equiv 4 \pmod 6.$$

Consequently, the left-hand side is at least 10, except if x belongs to the set

$$T := \{x \in \mathbf{F}_2^n | \delta_0(x) = \delta_1(x) = 0, \delta_2(x) = 2\}.$$

Therefore (12) implies that

$$\sum_{x \in \mathbf{F}_2^n} (5\delta_0(x)+5\delta_1(x)+2\delta_2(x)) = (5+4n+n^2)(|C|(1+n)-2^n) \geq 10 \cdot 2^n - 6|T|. \tag{18}$$

We need one more fact from [3] (see already [7]), namely that

$$|B_2(x) \cap Z| = 1 \text{ whenever } x \in T. \tag{19}$$

Indeed, if $x \in T$, and there are two different points $y_1, y_2 \in S_2(x) \cap Z_1$, we can choose a word $y \in S_1(x)$ such that $d(y, y_1) = 1$ and $d(y, y_2) = 3$, but then $\delta_0(y) + \delta_1(y) = 1$, contradicting (16).

We now estimate the size of the set T.

Lemma 1

$$|T| \leq \frac{1}{2}\binom{n-3}{2}(|C|(n+1) - 2^n).$$

Proof. Assume first that $x \in Z_2 \backslash C$ and that the three codewords covering x are $x+e_1$, $x+e_2$, $x+e_3$, where e_i is the word of weight one with its single 1 in the ith coordinate. Then x, $x+e_1+e_2$, $x+e_1+e_3$, $x+e_2+e_3 \in Z$. Hence a word $x+e_i+e_j$ with $i \leq 3$, $j \neq i$ cannot belong to T because $|S_2(x) \cap Z| \geq 3$. Therefore $|S_2(x) \cap T| \leq \binom{n-3}{2}$ as shown in [3].

Assume then that $x \in Z_2 \cap C$. The word x is covered by exactly two codewords $c_1, c_2 \in C$ other than x itself. Denote by y the other word that both c_1 and c_2 cover. (We should actually denote $c_1(x)$ etc. but we assume that the word x is fixed to simplify our notations.) If any other point in $B_2(x)$ belongs to Z then by (19), $|S_2(x) \cap T| \leq \binom{n-3}{2}$. We therefore consider the words in the set

$$L := \{x \in Z_2 \cap C \mid |B_2(x) \cap Z| = 4\}.$$

Assume that $x \in L$. If $E(y) = 1$ then $y \notin C$, and also $E(c_1) = E(c_2) = 1$ (any other codeword covering c_1, for instance, would itself belong to Z, which is a contradiction since $x \in L$). Denote by L_1 the set of such points x and let $L_2 = L \setminus L_1$. Assume now that $x \in L_2$, i.e., $E(y) \geq 2$. If y is covered by any codeword $c \in C$ such that $x + c$ has weight three, then we again find a fifth point in $B_2(x) \cap Z$, a contradiction. Hence $E(y) \leq 2$. Hence $E(y) = 2$ and $y \in C$, and our assumption $x \in L$ implies that $E(c_1) = E(c_2) = 2$. Clearly, for any two different points $x_1, x_2 \in L_2$ the sets $B_2(x_1) \cap Z$ and $B_2(x_2) \cap Z$ are either the same or disjoint.

We next show that if $x \in L_2$ then

$$|(S_2(x) \cup S_2(c_1) \cup S_2(c_2) \cup S_2(y)) \cap T| \leq 4\binom{n-3}{2}. \tag{20}$$

Without loss of generality, x is the all zero-word 0^n, $c_1 = e_1$, $c_2 = e_2$ and $y = e_1 + e_2$. If $a = a_1 a_2 \ldots a_n$ and $a \in (S_2(x) \cup S_2(c_1) \cup S_2(c_2) \cup S_2(y)) \cap T$, then $wt(a_3 a_4 \ldots a_n) = 2$, otherwise one of the words $x, c_1, c_2, y \in Z$ has distance 1 to a, a contradiction. Hence $|(S_2(x) \cup S_2(c_1) \cup S_2(c_2) \cup S_2(y)) \cap T| \leq 4\binom{n-2}{2}$. The claim (20) now follows when we show that for every i, $3 \leq i \leq n$ there are at least eight different words $a = a_1a_2 \ldots a_n$ such that $wt(a_3a_4 \ldots a_n) = 2$, $a_i = 1$ and $a \notin T$. (Then the total number of such points for all i together is at least $4(n-2)$ because each such point is counted twice, and $4\binom{n-2}{2} - 4(n-2) < 4\binom{n-3}{2}$.) By symmetry, it suffices to prove the claim for $i = 3$. Choose $z = e_1 + e_3$. The words $x, c_1, y \in C$ belong to $B_2(z)$. By the congruence $\delta_0(z) + \delta_1(z) + \delta_2(z) \equiv 2 \pmod 3$, there is a word $b \in Z \cap B_2(z)$ of weight three or four. If b has weight three, b is of the form 111000... or 101..., and using (19) we see that there are at least $n - 3 \geq 8$ words a of the required type that begin with 011... in the former case or with 101... in the latter case. If b has weight four and is of the form 111... then there are again $n-3$ words a of the required type that begin with 111... . Assume therefore that b has weight four and is of the form 101..., say $b =$ 10111000.... Then we find six words a of the required type, namely 10110..., 10101..., 11110..., 11101..., 00110..., 00101..., But we can apply the same argument to the word $z' = e_2 + e_3$. The same argument separately for z' proves the claim except in the case when also the word $b' \in Z \cap B_2(z')$ has weight four and begins with 011... . But then the two arguments together provide us with eight suitable words a.

We now claim that

$$|T| \leq |Z_2 \setminus L_1|\binom{n-3}{2} + |L_1|\binom{n-2}{2}. \tag{21}$$

We go through the points of Z_2 as follows. Take any point x in L_2 and consider the four points $B_2(x) \cap Z$ (which all belong to $Z_2 \cap C$). Then take any of the remaining points in L_2, say x' (now $x' \notin B_2(x) \cap Z$), consider $B_2(x') \cap Z$, and so on, until there are no points of L_2 left (now we have already gone through a number of other points in $Z_2 \cap C$ as well), and then consider the remaining points of $Z_2 \setminus L_1$. Finally, for all $x \in L_1$ we know that $|S_2(x) \cap T| \leq \binom{n-2}{2}$ proving (21).

For each point in L_1 there are two words of Z_1 within distance one. Furthermore, we have seen that the distance between any two points in L_1 is at least three, and therefore

$$E(\mathbf{F}_2^n) \geq 2|Z_2 \setminus L_1| + 4|L_1|. \tag{22}$$

Substituting (22) in (21) we obtain

$$\begin{aligned} |T| &\leq |Z_2 \setminus L_1|\binom{n-3}{2} + |L_1|\binom{n-2}{2} \\ &\leq \frac{1}{2}\binom{n-3}{2}E(\mathbf{F}_2^n) + |L_1|(\binom{n-2}{2} - 2\binom{n-3}{2}) \end{aligned}$$

$$\leq \frac{1}{2}\binom{n-3}{2}E(\mathbf{F}_2^n)$$

when $n \geq 11$ and the claim follows from (5).□

Substituting the result of the previous lemma to (18) we immediately obtain the following theorem.

Theorem 2 *If $n \geq 11$ and $n \equiv 5 \pmod 6$, then*

$$K(n,1) \geq \frac{(5n^2 - 13n + 66)2^n}{(5n^2 - 13n + 46)(n+1)}.$$

We get the following numerical improvements:

$$\begin{aligned} K(23,1) &\geq 352448 \\ K(29,1) &\geq 17988086. \end{aligned}$$

The best previously known lower bounds were 352336 and 17985042 [3].

3 The General Case

The improvements presented in this section are based on the following lemma.

Lemma 3 *Let $p \geq 5$ be a prime. Suppose that a binary $m \times n$ matrix A has the following properties:*

- *the number of 1's in every row equals $p-1$,*
- *the number of 1's in every column is divisible by $p-1$,*
- *the number of 1's in common in any two columns is divisible by $p-2$,*
- *$m+1$ is divisible by p.*

Then $m \geq 3p-1$ for all n.

Before proving this lemma, we show how it is connected with our original covering radius problem.

Assume that we have a binary code C of length n and covering radius 1 such that for all $y \in \mathbf{F}_2^n$ we have the congruences (cf. [3, Lemma 9])

$$\delta_0(y) + \delta_1(y) + \ldots + \delta_{p-2}(y) + \delta_{p-1}(y) \equiv p-1 \pmod p, \qquad (23)$$

$$\alpha_0\delta_0(y) + \alpha_1\delta_1(y) + \ldots + \alpha_{p-3}\delta_{p-3}(y) + \delta_{p-2}(y) \equiv 0 \pmod{p-1} \quad (24)$$

and

$$\beta_0\delta_0(y) + \beta_1\delta_1(y) + \ldots + \beta_{p-4}\delta_{p-4}(y) + \delta_{p-3}(y) \equiv 0 \pmod{p-2}, \quad (25)$$

where the coefficients α_i, β_i are integers.

Lemma 4 *If (23), (24) and (25) hold for all $y \in \mathbf{F}_2^n$, and there is a word x such that $\delta_0(x) = \delta_1(x) = \ldots = \delta_{p-2}(x) = 0$, then for $m = \delta_{p-1}(x)$ there is a binary $m \times n$ matrix A that satisfies the properties of Lemma 3.*

Proof. By translating the code C if necessary we can assume that x is the all-zero word. We now form the matrix A by writing each word in $B_{p-1}(x) \cap Z_i$ as a row of the matrix i times for all i. The number of rows becomes $m = E(B_{p-1}(x))$. In particular, p divides $m+1$ by (23). Our assumption $\delta_0(x) = \delta_1(x) = \ldots = \delta_{p-2}(x) = 0$ guarantees that no point in $B_{p-2}(x)$ belongs to Z and therefore $m = \delta_{p-1}(x)$. Furthermore, each row has $p-1$ 1's, and the number of 1's in the ith column is simply the excess $E(S_{p-2}(e_i))$, where e_i again denotes the binary word of weight one with its single 1 in the ith coordinate. By (24), $E(S_{p-2}(e_i)) = \delta_{p-2}(e_i)$ is divisible by $p-1$. Similarly, the number of 1's in common in two different columns i and j equals $\delta_{p-3}(e_i + e_j)$, which is divisible by $p-2$ by (25).□

We now discuss how the results presented in [3, Section 4] can be improved. If $n \equiv 19$ or $39 \pmod{60}$, then — using the fact that

$$\delta_i(x) = (n+1-i)A_{i-1}(x) + A_i(x) + (i+1)A_{i+1}(x) - \binom{n}{i}$$

where $A_i(x)$ denotes the number of codewords at distance i from x — it has been shown in [3] that for all $x \in \mathbf{F}_2^n$,

$$\begin{cases} 2n\delta_0(x) + \delta_1(x) + \delta_2(x) \equiv 0 \pmod{3}, \\ \delta_0(x) + \delta_1(x) + \delta_2(x) + \delta_3(x) \equiv 0 \pmod{4}, \\ \delta_0(x) + \delta_1(x) + \delta_2(x) + \delta_3(x) + \delta_4(x) \equiv 4 \pmod{5}. \end{cases}$$

(the third one of course follows from (11)). Therefore $\delta_0(x)+\delta_1(x)+\delta_2(x)+\delta_3(x) \geq 4$ or $\delta_4(x) \geq 14$ by Lemmas 4 and 3 (for $p = 5$). Consequently,

$$7(\delta_0(x) + \delta_1(x) + \delta_2(x) + \delta_3(x)) + 2\delta_4(x) \geq 28.$$

Adding over all x we get by (12),

$$\left(7\binom{n}{0} + 7\binom{n}{1} + 7\binom{n}{2} + 7\binom{n}{3} + 2\binom{n}{4}\right)(|C|(n+1) - 2^n) \geq 28 \cdot 2^n,$$

and obtain the following theorem.

Theorem 5 *If* $n \equiv 19$ *or* $39 \pmod{60}$, *then*

$$K(n,1) \geq \frac{(2V(n,4) + 5V(n,3) + 28)2^n}{(2V(n,4) + 5V(n,3))(n+1)}.$$

Corollary 6 $K(19,1) \geq 26261$.

A similar obvious modification leads to the following improvement of [3, Theorem 12]:

Theorem 7 $K(27,1) \geq 4793641$.

The best previous lower bounds were $K(19,1) \geq 26251$ and $K(27,1) \geq 4793611$ [3].

It remains to prove Lemma 3.

Proof of Lemma 3. Trivially, $m \geq 2p-1$: otherwise $m = p-1$ but then the first row must simply be repeated $p-1$ times in the matrix, contradicting the third condition. So assume that there is a matrix $A = (a_{ij})$ with $m = 2p-1$.

We first show that any two columns have either 0 or $p-2$ 1's in common. Clearly, any two columns cannot have $3p-6$ or more 1's in common: because the number of 1's in a column is divisible by $p-1$, and $3p-6 = 3(p-1)-3$, either of these columns has at least $3p-3$ 1's, a contradiction since $3p-3 > 2p-1$. So, assume that two columns, say the first and the second columns, have $2p-4$ 1's in common. Because the number of 1's in a column is divisible by $p-1$, there are at least two more 1's in the first column and two more 1's in the second column, and altogether at least $(2p-4)+2+2 = 2p$ rows, a contradiction.

Next we show that any two columns where the number of 1's is positive have at least one 1 in common. Assume that the first two columns have no 1 in common and that they both have $p-1$ 1's (obviously neither of them can have more). The first column has 1's in common with some other column, say the third; in fact they have exactly $p-2$ 1's common. There are now two possible cases illustrated in the figure.

$$\begin{array}{r}p-1\left\{\begin{array}{cccc}1&0&1&*\\1&0&1&*\\\vdots&&&\\1&0&1&*\\1&0&0&*\end{array}\right.\\p-1\left\{\begin{array}{cccc}0&1&0&1\\0&1&0&1\\\vdots&&&\\0&1&0&1\\0&1&0&0\end{array}\right.\end{array}\qquad\qquad\begin{array}{r}p-1\left\{\begin{array}{ccc}1&0&1\\1&0&1\\\vdots&&\\1&0&1\\1&0&0\end{array}\right.\\p-1\left\{\begin{array}{ccc}0&1&1\\0&1&1\\\vdots&&\\0&1&1\\0&1&0\end{array}\right.\end{array}$$

Case 1 Case 2

Case 1: If the third column has no 1's in common with the second column, take any column, say the fourth, which has. Again, the second and fourth columns have exactly $p-2$ 1's in common. The number of 1's in common in the first and fourth columns is 0 or $p-2$, i.e., exactly 0 or $p-2$ of the stars * in the figure are 1's. However, since the number of 1's in the fourth column is divisible by $p-1$, and there is one more row left, all the stars must be 0's and in the last row the fourth column has 1. Therefore the last row must begin $0011\ldots$. But then the number of 1's in common in the third and fourth columns is not divisible by $p-2$, a contradiction.

Case 2: If the second and third columns have 1's in common (necessarily $p-2$ of them), then in the first $2p-2$ rows there are $2p-4$ 1's in the third column. Since the number of 1's in the third column is divisible by $p-1$ there have to be at least two more rows, a contradiction.

Let now L be the number of columns that are not identically zero. We have shown that any two such columns have exactly $p-2$ 1's in common. Counting the number of triples (i,j,k) such that $a_{ij}=a_{ik}=1$ and $j<k$ in two different ways we get

$$\binom{L}{2}(p-2)=(2p-1)\binom{p-1}{2}. \tag{26}$$

At most one column has $2(p-1)$ 1's, because otherwise the number of rows is at least $2(p-1)+2(p-1)-(p-2)=3p-2>2p-1$. The total number of 1's in the matrix A is therefore $L(p-1)$ or $(L+1)(p-1)$. On the other hand, each of the $2p-1$ rows has $p-1$ 1's, and thus $L=2p-2$ or $L=2p-1$, contradicting (26).□

Acknowledgment

The author would like to thank Laurent Habsieger for sending a preprint of [3] and for useful comments. The author would also like to acknowledge the high class referee work.

References

[1] 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.

[2] L. Habsieger, "Lower bounds for q-ary coverings by spheres of radius one," *J. Combin. Theory Ser. A* **67** (1994) 199-122.

[3] L. Habsieger, "Binary codes with covering radius one: some new lower bounds," *Discrete Mathematics,* submitted.

[4] I. S. Honkala, "A lower bound on binary codes with covering radius one," *Proc. of the French-Israeli Workshop in Algebraic Coding, Lecture Notes in Computer Science* **781**, Springer, Berlin (1994), 34–37.

[5] I. S. Honkala, "A new lower bound on codes with covering radius one," *Proc. of ISITA'94*, Sydney, (1994), 39–41.

[6] G. J. M. van Wee, "Improved sphere bounds on the covering radius of codes," *IEEE Trans. Inform. Theory* **34** (1988), 237–245.

[7] G. J. M. van Wee, "Some new lower bounds for binary and ternary covering codes," *IEEE Trans. Inform. Theory* **39** (1993), 1422–1424.

[8] Z. Zhang, "Linear inequalities for covering codes: Part I — Pair covering inequalities," *IEEE Trans. Inform. Theory* **37** (1991), 573–582.

[9] Z. Zhang and C. Lo, "Linear inequalities for covering codes: Part II — Triple covering inequalities," *IEEE Trans. Inform. Theory* **38** (1992), 1648–1662.