Binary codes with covering radius one from a linear programming point of view: some new lower bounds

by

Laurent Habsieger

Mailing address:
Laboratoire d'Algorithmique Arithmétique
CNRS UMR 9936
Université Bordeaux 1
351 cours de la Libération
33405 Talence Cedex
FRANCE

Email: habsiege@ceremab.u-bordeaux.fr

Abstract: We study binary codes with covering radius one via their characteristic functions. The covering condition is expressed as a system of linear inequalities. The excesses then have a natural interpretation that makes congruence properties clear. We present new congruences and give several improvements on the lower bounds for $K(n,1)$ given by Zhang [9,10]. We study more specifically the cases $n \equiv 5 \mod 6$ and $n \equiv 2,4 \mod 6$, and get new lower bounds such as $K(11,1) \geq 178$ and $K(20,1) \geq 52455$.

Résumé: Nous étudions les codes binaires de recouvrement dont le rayon de recouvrement vaut 1, à l'aide de leur fonction caractéristique. La condition de recouvrement s'exprime comme un système d'inéquations linéaires. Les excès de recouvrement ont alors une interprétation naturelle qui rend les propriétés de congruence claires. Nous présentons de nouvelles congruences et améliorons quelques minorations de $K(n,1)$ données par Zhang [9,10]. Nous étudions plus particulièrement les cas $n \equiv 5 \mod 6$ et $n \equiv 2,4 \mod 6$, et obtenons de nouvelles minorations, comme $K(11,1) \geq 178$ ou $K(20,1) \geq 52455$.

1. Introduction

Let $\mathbb{F}_2$ be the finite field with two elements and n be some positive integer. Let us put $H = (\mathbb{F}_2)^n$ and define the Hamming distance between two elements $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ of H by

$$\mathrm{d}(x, y) = |\{i \in \{1, \ldots, n\} : x_i \neq y_i\}| .$$

For $x \in H$ and $r \in \mathbb{Z}$, the sphere of center x and radius r is denoted $S_r(x)$ and is defined by

$$S_r(x) = \{y \in H : \mathrm{d}(x, y) = r\} .$$

Note that $|S_r(x)| = \binom{n}{r}$.

A binary code with covering radius one is a subset C of H such that the following covering condition holds:

$$\forall x \in H, \ \exists y \in C : \mathrm{d}(x, y) \leq 1 . \tag{1}$$

The problem of determining $K(n, 1)$, the minimal cardinality of C, has been widely studied in the last decade [1-10]. The methods used in these papers are various and range from congruence properties [1,4-8] to pair covering by k-uples [9,10], and from embedded error-correcting codes [2] to recurrence relations [3].

We first introduce a formalism that gives an algebraic interpretation to the theory of excesses [1-2,4-8]. This enables us to produce numerous congruence properties. Later sections will be devoted to the study of special cases: Section 3 deals with the case $n \equiv 5 \mod 6$, Section 4 with the cases $n \equiv 1, 3 \mod 6$ and Section 5 with the cases $n \equiv 2, 4 \mod 6$. We will end this paper by giving an updated version of the lower bounds for $K(n, 1)$ and by indicating how these bounds might be improved further.

2. Generalities

Let F be a real function defined on H. For $i \in \mathbb{Z}$, let us introduce the function F_i defined by

$$F_i(x) = \sum_{y \in S_i(x)} F(y) .$$

Note that $F_i = 0$ if $i \notin \{0, \ldots, n\}$, $F_0 = F$ and $\sum_{0 \leq i \leq n} F_i = |F|$, where

$$|F| = \sum_{x \in H} F(x) .$$

It is also clear, by definition, that

$$|F_i| = \binom{n}{i} |F| . \tag{2}$$

We shall make extensive use of the following Lemma.

Lemma 1. *For $i, j \in \mathbb{Z}$, we have*

$$(F_i)_j = \sum_{\substack{j-i \le k \le i+j \\ k \equiv i+j \mod 2}} \binom{k}{\frac{k+j-i}{2}} \binom{n-k}{\frac{i+j-k}{2}} F_k(x).$$

Proof. By definition (and by using the isometric property of the translations and permutations for the Hamming distance) we get

$$\begin{aligned}(F_i)_j(x) &= \sum_{\mathrm{d}(x,y)=j} \sum_{\mathrm{d}(y,z)=i} F(z) = \sum_{k \in \mathbf{N}} \sum_{\mathrm{d}(x,z)=k} F(z) |\{y \in H : \mathrm{d}(x,y) = j \text{ et } \mathrm{d}(y,z) = i\}| \\ &= \sum_{k \in \mathbf{N}} |\{y \in H : \mathrm{d}(y,0) = j \text{ et } \mathrm{d}(y,z_k) = i\}| F_k(x),\end{aligned}$$

where z_k is the vector beginning with k 1's and ending with $n-k$ 0's. The coefficient of $F_k(x)$ is 0 if $i+j+k$ is odd. If $i+j+k$ is even, it is equal to the number of ways for choosing $\frac{k+j-i}{2}$ 1's among the k first coordinates and $\frac{i+j-k}{2}$ 1's among the $n-k$ last coordinates. This gives the desired result. □

Let us apply this formalism to codes and let N denote the characteristic function of C:

$$N(x) = \begin{cases} 1 & \text{if } x \in C, \\ 0 & \text{if } x \notin C. \end{cases}$$

Then the covering condition (1) becomes

$$\forall x \in H, \ (N_0 + N_1)(x) \ge 1.$$

Let us put $\delta = N_0 + N_1 - 1$, so that δ is a function defined on H that takes nonnegative integer values. It is closely related to the theory of excesses [1-2,4-8], since $\delta(x)$ just equals the excess on the singleton $\{x\}$. Moreover, by formula (2), we have

$$|\delta| = (n+1)|C| - 2^n. \tag{3}$$

Since δ is a nonnegative function, (3) implies the sphere covering bound $|C| \ge \frac{2^n}{n+1}$. Lemma 1 gives the general form for δ_i:

$$\delta_i = (n+1-i)N_{i-1} + N_i + (i+1)N_{i+1} - \binom{n}{i}. \tag{4}$$

This last formula enables us to produce numerous congruence properties for the δ function. We start with a general property.

Lemma 2. *For any odd prime number p dividing $n+1$,*

$$\sum_{i=0}^{p-1} \delta_i \equiv p - 1 \mod p.$$

Proof. By summing (4), we get

$$\sum_{i=0}^{p-1} \delta_i = (n+1) \sum_{i=0}^{p-2} N_i + p(N_{p-1} + N_p) - \sum_{i=0}^{p-1} \binom{n}{i}.$$

Since $n \equiv -1 \mod p$, we have

$$\sum_{i=0}^{p-1} \binom{n}{i} \equiv \sum_{i=0}^{p-1} (-1)^i \equiv -1 \mod p,$$

and the Lemma follows. □

In a similar way, we can get congruence properties for other sums of δ_i. We list below the congruences for $p \in \{2,3,4,5\}$.

$$\begin{cases} \delta_0 + \delta_1 \equiv N+1 \mod 2 & \text{if } n \equiv 0 \mod 2 \\ \delta_0 + \delta_1 \equiv 0 \mod 2 & \text{if } n \equiv 1 \mod 2 \end{cases}$$

$$\begin{cases} \delta_1 + \delta_2 \equiv 0 \mod 3 & \text{if } n \equiv 0 \mod 3 \\ 2\delta_0 + \delta_1 + \delta_2 \equiv 0 \mod 3 & \text{if } n \equiv 1 \mod 3 \\ \delta_0 + \delta_1 + \delta_2 \equiv 2 \mod 3 & \text{if } n \equiv 2 \mod 3 \end{cases}$$

$$\begin{cases} \delta_2 + \delta_3 \equiv 0 \mod 4 & \text{if } n \equiv 1 \mod 4 \\ \delta_0 + \delta_1 + \delta_2 + \delta_3 \equiv 0 \mod 4 & \text{if } n \equiv 3 \mod 4 \end{cases}$$

$$\begin{cases} 4\delta_1 + 4\delta_2 + \delta_3 + \delta_4 \equiv 0 \mod 5 & \text{if } n \equiv 0 \mod 5 \\ 3\delta_0 + 2\delta_1 + 2\delta_2 + \delta_3 + \delta_4 \equiv 0 \mod 5 & \text{if } n \equiv 1 \mod 5 \\ \delta_3 + \delta_4 \equiv 0 \mod 5 & \text{if } n \equiv 2 \mod 5 \\ \delta_0 + 3\delta_1 + 3\delta_2 + \delta_3 + \delta_4 \equiv 0 \mod 5 & \text{if } n \equiv 3 \mod 5 \\ \delta_0 + \delta_1 + \delta_2 + \delta_3 + \delta_4 \equiv 4 \mod 5 & \text{if } n \equiv 4 \mod 5 \end{cases}$$

Let us now examine more closely the numerical implications of these congruences.

3. The case $n \equiv 5 \mod 6$

If $n \equiv 5 \mod 6$, we have the two congruences

$$\begin{cases} \delta_0 + \delta_1 \equiv 0 \mod 2, \\ \delta_0 + \delta_1 + \delta_2 \equiv 2 \mod 3, \end{cases}$$

which implies that

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

Moreover we have $5(\delta_0 + \delta_1) + 2\delta_2 \geq 10$, unless $(\delta_0, \delta_1, \delta_2) = (0,0,2)$. Let us put

$$T = \{x \in H \ : \ \delta(x) = \delta_1(x) = 0 \text{ and } \delta_2(x) = 2\}.$$

We have the inequality

$$\sum_{x \in H} (5(\delta_0 + \delta_1) + 2\delta_2)(x) \geq 10 \cdot 2^n - 6|T|,$$

and we would like to prove that $|T|$ is not too large. We will need the following Lemmas.

Lemma 3.

$$\forall x \in T,\ \exists! y \in S_2(x)\ :\ \delta(y) > 0\,.$$

Moreover $\delta(y) = 2$.

Lemma 4. *For any* $x \in Z_2$, *the following inequalities hold*

$$\begin{cases} |S_2(x) \cap T| \leq \binom{n}{2} - (2n-3) & \text{if } x \in C, \\ |S_2(x) \cap T| \leq \binom{n}{2} - 3(n-2) & \text{if } x \notin C. \end{cases}$$

Lemma 5. *For* $n \geq 11$, *we have*

$$|T| - 4|Z_2 \cap C| + 2|S| \leq \left(\binom{n}{2} - 2n - 1\right)\frac{|\delta|}{2}\,.$$

Lemma 6. *The following estimates hold:*

$$\begin{cases} (5(\delta_0+\delta_1)+2\delta_2)(x) \geq 10 & \text{for } x \in H \setminus T, \\ (5(\delta_0+\delta_1)+2\delta_2)(x) = 4 & \text{for } x \in T, \\ (5(\delta_0+\delta_1)+2\delta_2)(x) \geq 34 & \text{for } x \in (Z_2 \cap C) \setminus S, \\ (5(\delta_0+\delta_1)+2\delta_2)(x) \geq 22 & \text{for } x \in S. \end{cases}$$

The proofs of these Lemmas are omitted since this paper is just an extended abstract. We can now prove the main result of this section.

Theorem 7. *For* $n \equiv 5 \,mod\, 6$, $n \geq 11$, *we have*

$$|C| \geq \left(1 + \frac{10}{5\binom{n}{2} - n + 2}\right)\frac{2^n}{n+1}\,.$$

Proof. By Lemma 6, we have

$$\sum_{x \in H}(5(\delta_0+\delta_1)+2\delta_2)(x) \geq 10\,.\,2^n - 6|T| + 24|Z_2 \cap C| - 12|S|\,.$$

By Lemma 5, we get

$$\sum_{x \in H}(5(\delta_0+\delta_1)+2\delta_2)(x) \geq 10\,.\,2^n - 6\left(\binom{n}{2} - 2n - 1\right)\frac{|\delta|}{2}\,.$$

By (3), this gives the inequality

$$\left(5(1+n) + 2\binom{n}{2}\right)|\delta| \geq 10\,.\,2^n - 3\left(\binom{n}{2} - 2n - 1\right)|\delta|\,,$$

from which we deduce that

$$|\delta| \geq \frac{10\,.\,2^n}{5\binom{n}{2} - n + 2}\,.$$

We then just have to apply (3) to get the desired result. □

Let us give some of the corresponding lower bounds for $K(n,1)$.

Corollary 8.

$$K(11,1) \geq 178$$
$$K(17,1) \geq 7392$$

These bounds are all better than the ones given in Zhang's table [9,10], which were respectively 176 and 7378. Van Wee [8] and Honkala [5] gave the bounds $K(11,1) \geq 177$ (both authors), $K(17,1) \geq 7391$ (Van Wee) and $K(17,1) \geq 7399$ (Honkala). Theorem 1 thus improves on the first lower bound.

4. The cases $n \equiv 1,3 \mod 6$

We start with a Lemma that extends the approach given at the beginning of the last section. As in the last section, its proof is omitted.

Lemma 9. *Let $p \geq 5$ be a prime number. Let us assume there exist three congruence properties of the following type:*

$$\sum_{i=0}^{p-4} \alpha_i \delta_i + \delta_{p-3} \equiv 0 \mod p-2, \tag{5}$$

$$\sum_{i=0}^{p-3} \beta_i \delta_i + \delta_{p-2} \equiv 0 \mod p-1, \tag{6}$$

$$\sum_{i=0}^{p-1} \delta_i \equiv p-1 \mod p, \tag{7}$$

where the α_i's and the β_i's are rational numbers. Then the following property holds:

$$\forall x \in H, \quad \delta_0(x) = \cdots = \delta_{p-2}(x) = 0 \Longrightarrow \delta_{p-1}(x) \geq 2p-1.$$

It is probably true that a necessary and sufficient condition for the existence of (5-7) is that p divides $n+1$. Since the applications of this Lemma require explicit congruence properties, we shall not try to prove this characterization.

Let us first apply this Lemma with $p = 5$.

Theorem 10. *For $n \equiv 19,39 \mod 60$, we have*

$$|C| \geq \left(1 + \frac{36}{9\left(n+1+\binom{n+1}{3}\right) + 4\binom{n}{4}}\right) \frac{2^n}{n+1}.$$

For $n \equiv 9,49 \mod 60$, we have

$$|C| \geq \left(1 + \frac{36}{18(n+1) + 9\binom{n+1}{3} + 4\binom{n}{4}}\right) \frac{2^n}{n+1}.$$

Proof. When n is congruent to 19 or 39 modulo 60, the following congruence properties hold

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

By Lemma 9, we know that either $\delta_0 + \delta_1 + \delta_2 + \delta_3 \geq 4$ or $\delta_4 \geq 9$. Thus it is always true that

$$9(\delta_0 + \delta_1 + \delta_2 + \delta_3) + 4\delta_4 \geq 36.$$

Using (2-3) again gives the desired result.

When n is congruent to 29 or 49 modulo 60, the following congruence properties hold

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

By Lemma 9, we know that either $2(\delta_0 + \delta_1) + \delta_2 + \delta_3 \geq 4$ or $\delta_4 \geq 9$. Thus it is always true that

$$18(\delta_0 + \delta_1) + 9(\delta_2 + \delta_3) + 4\delta_4 \geq 36.$$

Using (2-3) again gives the desired result. □

Let us give some of the corresponding explicit lower bounds for $K(n, 1)$.

Corollary 11.

$$K(9, 1) \geq 53$$
$$K(19, 1) \geq 26251$$

The only improvement to the tables in [3,9-10] is $K(19, 1) \geq 26251$. The bound given in [3,9-10] (and found in [2]) was 26216, and Habsieger obtained in [3] the small improvement 26218.

Let us now apply Lemma 9 with $p = 7$. The only interesting cases mentioned in the tables are $n = 13$ and $n = 27$. This method does not give a good result for $n = 13$, i.e $K(13, 1) \geq 587$, while Cohen, Lobstein and Sloane's bound [2] is 598. So we will focus on the case $n = 27$, where the only improvement to the sphere covering bound was given by Habsieger [3] ($K(27, 1) \geq 4793495$).

Theorem 12. $K(27, 1) \geq 4793611$.

Proof. The following congruence properties hold

$$\begin{cases} \delta_0 + \delta_1 \equiv 0 \mod 2, \\ \delta_0 + \delta_1 + \delta_2 \equiv 0 \mod 3, \\ \delta_0 + \delta_1 + \delta_2 + \delta_3 \equiv 0 \mod 4, \\ \delta_3 + \delta_4 \equiv 0 \mod 5, \\ \delta_4 + \delta_5 \equiv 0 \mod 6, \\ \delta_0 + \delta_1 + \delta_2 + \delta_3 + \delta_4 + \delta_5 + \delta_6 \equiv 6 \mod 7, \end{cases}$$

By Lemma 9, we know that either $3(\delta_0+\delta_1+\delta_2+\delta_3)+2(\delta_4+\delta_5)\geq 12$ or $\delta_6\geq 13$. Thus it is always true that

$$39(\delta_0+\delta_1+\delta_2+\delta_3)+26(\delta_4+\delta_5)+12\delta_6\geq 156\,.$$

Using (2-3) again gives

$$|C|\geq\left(1+\frac{156}{39(28+\binom{28}{3})+26\binom{28}{5}+12\binom{27}{6}}\right)\frac{2^{27}}{28}=\left(1+\frac{1}{39976}\right)\frac{2^{27}}{28}\,,$$

and the Theorem follows. □

5. The cases $n\equiv 2,4 \mod 6$

Let us introduce a new function ϕ defined for any $x\in H$ by

$$\phi(x)=\frac{n}{2}(N_0(x)+N_1(x))+N_2(x)+N_3(x)-\frac{(n+1)(n+2)}{6}\,.$$

The next Lemma shows the importance of this function.

Lemma 13. *The function ϕ satisfies to the two following properties:*

$$\forall x\in H\,,\ \phi(x)\geq 0\,, \tag{8}$$

$$|\phi|=\frac{(n+1)(n+2)}{6}(n|C|-2^n)\,. \tag{9}$$

Proof. Let us first assume that $n\equiv 2 \mod 6$. The two following congruence properties hold

$$\begin{cases}\delta_0+\delta_1+N_0\equiv 1 \mod 2\,,\\ \delta_0+\delta_1+\delta_2\equiv 2 \mod 3\,.\end{cases}$$

The first congruence shows that $\delta_0+\delta_1+N_0\geq 1$. Put $f=\delta_0+\delta_1+N_0-1$. By Lemma 1 and (4), we have

$$0\leq f_0+f_1=\delta_0+\delta_1+n\delta_0+2\delta_2+N_0+N_1-1-n=(n+2)\delta_0+2(\delta_1+\delta_2)-n\,,$$

which implies that $(\frac{n}{2}+1)\delta_0+\delta_1+\delta_2\geq\frac{n}{2}$. If $\delta_0=0$, this gives $\delta_1+\delta_2\geq\frac{n}{2}$, and even $\delta_1+\delta_2\geq\frac{n}{2}+1$, since $\delta_0+\delta_1+\delta_2\equiv 2 \mod 3$. If $\delta_0\geq 1$, we still have $\delta_0+\delta_1+\delta_2\geq 2$ and therefore $\frac{n}{2}\delta_0+\delta_1+\delta_2\geq 2+\frac{n}{2}-1$. Thus, we always have

$$\frac{n}{2}\delta_0+\delta_1+\delta_2\geq\frac{n}{2}+1\,.$$

Now (4) tells us that

$$\frac{n}{2}\delta_0+\delta_1+\delta_2-\frac{n}{2}-1=\frac{3n}{2}(N_0+N_1-1)+3(N_2+N_3)-\binom{n}{2}-\frac{n}{2}-1=3\phi\,,$$

and (8) is half-proved.

Let us now assume that $n \equiv 4 \mod 6$. The two following congruence properties hold

$$\begin{cases} \delta_0 + \delta_1 + N_0 \equiv 1 \mod 2, \\ 2\delta_0 + \delta_1 + \delta_2 \equiv 0 \mod 3. \end{cases}$$

The proof then proceeds as before and we still have $(\frac{n}{2}+1)\delta_0 + \delta_1 + \delta_2 \geq \frac{n}{2}$. If $\delta_0 = 0$, we obtain $\delta_1 + \delta_2 \geq \frac{n}{2}$, and even $\delta_1 + \delta_2 \geq \frac{n}{2} + 1$, since $2\delta_0 + \delta_1 + \delta_2 \equiv 0 \mod 3$. If $\delta_0 \geq 1$, we still have $2\delta_0 + \delta_1 + \delta_2 \geq 3$ and therefore $\frac{n}{2}\delta_0 + \delta_1 + \delta_2 \geq 3 + \frac{n}{2} - 2$. Thus, we always have

$$\frac{n}{2}\delta_0 + \delta_1 + \delta_2 \geq \frac{n}{2} + 1,$$

and in the same way, we get $\phi \geq 0$.

To prove (9), we apply (2) to the definition of ϕ:

$$|\phi| = \left(\frac{n}{2}(1+n) + \binom{n}{2} + \binom{n}{3}\right)|C| - \frac{(n+1)(n+2)}{6}2^n = \frac{(n+1)(n+2)}{6}(n|C| - 2^n).$$

□

This Lemma readily gives Van Wee's bound [7]: $|C| \geq \frac{2^n}{n}$. However Van Wee's bound applies whenever n is even, whereas this Lemma does not cover the case $n \equiv 0 \mod 6$. In terms of δ, Van Wee's proof may be summarized as follows:

$$\begin{aligned} 2^n - |C| &\leq \sum_{x \in H \setminus C} (\delta_0 + \delta_1)(x) && \text{by the congruence property } \delta_0 + \delta_1 \equiv N + 1 \mod 2, \\ &= \sum_{y \in H} \delta(y)(n - \delta(y)) && \text{by using the definition of } \delta_1 \text{ and permuting sums,} \\ &\leq (n-1)|\delta| && \text{since we can assume that } \delta(y) > 0 \text{ in the previous sum,} \\ &= (n^2-1)|C| && \text{by (3).} \end{aligned}$$

Let us now use this Lemma to improve on Van Wee's bound.

Theorem 14. *For $n \equiv 20, 40 \mod 60$ we have*

$$|C| \geq \left(1 + \frac{8}{\frac{(n+1)(n+2)}{6}\left(\binom{n+1}{2} + 6\right)}\right)\frac{2^n}{n}.$$

For $n \equiv 10, 50 \mod 60$ we have

$$|C| \geq \left(1 + \frac{8}{\frac{(n+1)(n+2)}{6}\left(\binom{n+1}{2} + 1\right)}\right)\frac{2^n}{n}.$$

Proof. In both cases we can apply Lemma 13. We then use Lemma 1 to compute ϕ_1 and ϕ_2 and we find

$$\left(\frac{n}{2}+6\right)\phi+\phi_1+\phi_2 = 10\left(\binom{\frac{n}{2}+1}{2}(N_0+N_1)+\frac{n}{2}(N_2+N_3)+N_4+N_5\right) - \frac{(n+1)(n+2)}{3}\left(\frac{n}{2}\left(\frac{n}{2}+1\right)+3\right).$$

Thus, if 10 divides n, we obtain the congruence property

$$\left(\frac{n}{2}+6\right)\phi+\phi_1+\phi_2 \equiv 8 \mod 10.$$

When $n \equiv 20, 40 \mod 60$, this gives the inequality $6\phi+\phi_1+\phi_2 \geq 8$. We now use (2) and (9) to get

$$\frac{(n+1)(n+2)}{6}\left(6+\binom{n+1}{2}\right)(n|C|-2^n) \geq 8.2^n,$$

and the first part of the Theorem is proved.

When $n \equiv 10, 50 \mod 60$, we have the inequality $\phi+\phi_1+\phi_2 \geq 8$ and we find similarly

$$\frac{(n+1)(n+2)}{6}\left(1+\binom{n+1}{2}\right)(n|C|-2^n) \geq 8.2^n,$$

which completes the proof of the Theorem. □

Let us give some of the corresponding explicit lower bounds for $K(n,1)$.

Corollary 15.

$$K(10,1) \geq 104$$
$$K(20,1) \geq 52455$$

These bounds improve on Van Wee's bounds [7]. However, when $n = 10$, the best bound is Zhang's one [9] ($K(10,1) \geq 105$). When $n = 20$, we can use the same method to increase our lower bound by one unit. Both our results improve on Van Wee's bound [7] ($K(20,1) \geq 52429$).

Theorem 16. $K(20,1) \geq 52456$

Let us now study the special cases $n = 14$ and $n = 28$. Since the proofs of the next two Theorems are basically the same, we give only the first one.

Theorem 17. $K(14,1) \geq 1172$

Proof. We use Lemma 1 to get the identity

$$9\phi+\phi_1+\phi_2+2(\phi_3+\phi_4) = 70(14(N_0+N_1)+9(N_2+N_3)+4(N_4+N_5)+N_6+N_7-1626)+60,$$

which leads to the inequality

$$14(N_0+N_1)+9(N_2+N_3)+4(N_4+N_5)+N_6+N_7 \geq 1626.$$

Let us put $\psi = 14(N_0 + N_1) + 9(N_2 + N_3) + 4(N_4 + N_5) + N_6 + N_7 - 1626$. By applying Lemma 1 again, we obtain

$$\frac{9}{10}(3\phi + \phi_1 + \phi_2) + 4\psi + \psi_1 + \psi_2$$
$$= 36(35(N_0 + N_1) + 20(N_2 + N_3) + 10(N_4 + N_5) + 4(N_6 + N_7) + N_8 + N_9 - 5032) + 30\,,$$

which gives

$$35(N_0 + N_1) + 20(N_2 + N_3) + 10(N_4 + N_5) + 4(N_6 + N_7) + N_8 + N_9 \geq 5032\,.$$

We then apply (2) to get

$$|C| \geq \frac{5032 \cdot 2^{14}}{35\binom{15}{1} + 20\binom{15}{3} + 10\binom{15}{5} + 4\binom{15}{7} + \binom{15}{9}} = 1171.083\cdots\,,$$

and the Theorem follows. □

Theorem 18. $K(28, 1) \geq 9587064$

6. Concluding remarks

Let us first give an updated version of Zhang's Table I [9-10]. We consider only those values of $n \leq 33$ for which $K(n, 1)$ is still unknown.

n	Lower bound for $K(n,1)$	Reference
9	55	[3]
10	105	[9]
11	178	Theorem 7
12	342	[7]
13	598	[2]
14	1172	Theorem 17
17	7399	[5]
18	14564	[7]
19	26251	Theorem 10
20	52455	Theorem 14
21	95330	[3]
22	190651	[7]
23	352336	Theorem 7
24	699051	[7]
25	1290562	[3]
26	2581111	[7]
27	4793611	Theorem 12
28	9587064	Theorem 18
29	17985042	Theorem 7
30	35791395	[7]
33	252645140	[3]

There is some hope of improving a number of the lemmas given in this paper. In Section 3, one might well think that $Z_2 \setminus C$ should be much bigger than $Z_2 \cap C$. By Lemma 4, an effective comparison between $|Z_2 \cap C|$ and $|Z_2|$ would give a smaller estimate for $|T|$. In Section 4, the inequality $\delta_{p-1}(x) \geq 2p-1$ can probably be sharpened. One might even get a lower bound which is quadratic in p.

References

[1] W. Chen and I. S. Honkala, Lower bounds for q-ary covering codes, *IEEE Trans. Inform. Theory* **36** (1990), 664-671.

[2] 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.

[3] L. Habsieger, Lower bounds for q-ary coverings by spheres of radius one, *J. Combin. Theory Ser. A* **67** (1994), 199-222.

[4] I. S. Honkala, Modified bounds for binary covering codes, *IEEE Trans. Inform. Theory* **37** (1991), 351-365.

[5] I. S. Honkala, A lower bound on binary codes with covering radius one, preprint.

[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, Bounds on packings and coverings by spheres in q-ary and mixed Hamming spaces, *J. Combin. Theory Ser. A* **57** (1991), 117-129.

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

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

[10] Z. Zhang, Linear inequalities for covering codes: Part II-Triple covering inequalities, *IEEE Trans. Inform. Theory* **38** (1992), 1648-1662.