Some new lower bounds for ternary covering codes

Laurent Habsieger[1]

Submitted: February 23, 1995; Accepted: January 22, 1996

To Dominique Foata, on the occasion of his sixtieth birthday

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

e-mail: habsiege@ceremab.u-bordeaux.fr

Abstract: In [5], we studied binary codes with covering radius one via their characteristic functions. This gave us an easy way of obtaining congruence properties and of deriving interesting linear inequalities. In this paper we extend this approach to ternary covering codes. We improve on lower bounds for ternary 1-covering codes, the so-called football pool problem, when 3 does not divide $n-1$. We also give new lower bounds for some covering codes with a covering radius greater than one.

[1] partially supported by the EC grant CHRX-CT93-0400 and the "PRC maths-info"

1. Introduction

Let $\mathbb{F}_3$ be the finite field with three elements and n be some positive integer. Let us put $H = (\mathbb{F}_3)^n$ 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 $S_r(x) = \emptyset$ if $r \notin \{0, \ldots, n\}$, and

$$|S_r(x)| = 2^r \binom{n}{r}, \tag{1}$$

if $r \in \{0, \ldots, n\}$. The ball of center x and radius r is denoted $B_r(x)$ and is defined by $B_r(x) = \{y \in H \ : \ \mathrm{d}(x,y) \leq r\}$. We have $|B_R(x)| = \sum_{r=0}^{R} 2^r \binom{n}{r}$.

Let R be a positive integer. A ternary code with covering radius R is a subset C of H such that the following covering condition holds:

$$\forall x \in H \, , \ \exists y \in C \ : \ \mathrm{d}(x,y) \leq R \, . \tag{2}$$

The problem of determining $K_3(n,R)$ the minimal cardinality of C has been widely studied in the last decade (see [2] for a complete bibliography).

In [5] we gave an algebraic interpretation of the geometric theory of excesses for binary covering codes. In this article we adapt this point of view to ternary covering codes. We first introduce in Section 2 the formalism that will be used throughout the paper. In Section 3, we present general characteristics of our approach when the covering radius equals one, the so-called football pool problem. We then apply it to the cases $n \equiv 2 \mod 3$ and $n \equiv 0 \mod 3$, in Section 4. In Section 5 we deal with the case of a covering radius which is greater than one, and give general properties. We use them in Section 6 to get new lower bounds for some covering codes, with a covering radius greater than one.

2. Preliminary lemmas

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 and by (1), that

$$|F_i| = 2^i \binom{n}{i} |F| \, . \tag{3}$$

We shall make extensive use of the following lemma.

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

$$(F_i)_j = \sum_{k\in\mathbb{N}} \left(\sum_{m=0}^{i} \binom{k}{i-m} \binom{n-k}{m} \binom{i-m}{i+j-k-2m} 2^m \right) F_k \,.$$

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

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

where z_k is the vector of H starting with k 1's and ending with $n-k$ 0's. Let us find the shape of an element $y \in H$ such that $\mathrm{d}(y,0)=j$ and $\mathrm{d}(y,z_k)=i$. Let m denote the number of nonzero coordinates among the $n-k$ last coordinates, and let α_l be the number of l's among the k first coordinates, for $l = 0, 1, 2$. Since we are dealing with ternary codes, we must have $\alpha_0+\alpha_1+\alpha_2 = k$. Moreover the conditions $\mathrm{d}(x,0)=j$ and $\mathrm{d}(y,z_k)=i$ may be stated as $\alpha_1+\alpha_2 = j-m$ and $\alpha_0+\alpha_2 = i-m$. Thus $(\alpha_0, \alpha_1, \alpha_2)$ satisfies to the system

$$\begin{cases} \alpha_0+\alpha_1+\alpha_2 = k \\ \alpha_1+\alpha_2 = j-m \\ \alpha_0+\alpha_2 = i-m \end{cases}$$

We find this way $(\alpha_0, \alpha_1, \alpha_2) = (k+m-j, k+m-i, i+j-k-2m)$. The number of such codewords is

$$\frac{(\alpha_0+\alpha_1+\alpha_2)!}{\alpha_0!\alpha_1!\alpha_2!} = \frac{k!}{(k+m-j)!(k+m-i)!(i+j-k-2m)!}\,.$$

Since the number of codewords of length $n-k$ with m nonzero coordinates is $\binom{n-k}{m}2^m$, we get

$$\begin{aligned}&|\{y \in H \ : \ \mathrm{d}(x,0)=j \text{ and } \mathrm{d}(y,z_k)=i\}| \\ &\qquad = \sum_{m=0}^{i} \frac{k!}{(k+m-j)!(k+m-i)!(i+j-k-2m)!} \binom{n-k}{m} 2^m\,,\end{aligned}$$

and the lemma follows. □

Let us apply this lemma to an easy case.

Lemma 2. *For $j \in \mathbb{Z}$, we have*

$$(F_0+F_1)_j = 2(n-j+1)F_{j-1} + (j+1)(F_j+F_{j+1})\,.$$

Proof. We use Lemma 1 with $i = 0, 1$ to obtain

$$\begin{aligned}(F_0 + F_1)_j &= F_j + \sum_{k\in\mathbb{N}} F_k \sum_{m=0}^{1} \binom{k}{1-m}\binom{n-k}{m}\binom{1-m}{1+j-k-2m} 2^m \\ &= F_j + \sum_{k\in\mathbb{N}} F_k \left(k\binom{1}{j-k+1} + 2(n-k)\binom{0}{j-k-1}\right) \\ &= F_j + (j+1)F_{j+1} + jF_j + 2(n-j+1)F_{j-1}\,,\end{aligned}$$

and the result is proved. □

Let R be a positive integer and C be a R-covering code of H, i. e. a subset of H that satisfies (2). Let A denote its characteristic function. Then the covering condition (2) becomes:

$$\forall x \in H\,,\ (A_0 + \cdots + A_R)(x) \geq 1\,.$$

As in [5], put $\delta = A_0 + \cdots + A_R - 1$, so that δ is a function defined on H that takes nonnegative integer values. As usual, we put $Z = \{x \in H \ :\ \delta(x) > 0\}$. The function δ is closely related to the theory of excesses, since $\delta(x)$ just equals the excess on $\{x\}$. Moreover, by (3), we have

$$|\delta| = \left(\sum_{r=0}^{R} 2^r \binom{n}{r}\right) |C| - 3^n\,. \tag{4}$$

Let us first study the case $R = 1$.

3. General lemmas for covering radius one

In this case Lemma 2 gives the general form for the δ_i's:

$$\delta_i = 2(n+1-i)A_{i-1} + (i+1)(A_i + A_{i+1}) - 2^i\binom{n}{i}\,. \tag{5}$$

For instance we have

$$\begin{cases} \delta_1 = 2nA_0 + 2(A_1 + A_2) - 2n\,, \\ \delta_2 = 2(n-1)A_1 + 3(A_2 + A_3) - 2n(n-1)\,, \end{cases}$$

which already shows that δ_1 is always even. We shall now give several other properties of the delta function.

Lemma 3. *For any element x in H such that $\delta(x)$ is odd, we have the inequality*

$$\left(\frac{\delta_1}{2} + \delta_2\right)(x) \geq n\,.$$

Proof. Let y be in $S_1(x)$. Let $\bar{y}$ denote the unique element of $S_1(x) \cap S_1(y)$. Since $\delta_1(y)$ is even, we have

$$0 \equiv \delta_1(y) \equiv 1 + \delta(\bar{y}) + \sum_{z\in S_2(x)\cap S_1(y)} \delta(z) \mod 2\,,$$

which implies that

$$\delta(\bar{y}) + \sum_{z \in S_2(x) \cap S_1(y)} \delta(z) \geq 1\,.$$

Summing over y gives the property

$$\begin{aligned} 2n &\leq \sum_{y \in S_1(x)} \delta(\bar{y}) + \sum_{y \in S_1(x)} \sum_{z \in S_2(x) \cap S_1(y)} \delta(z) \\ &= \delta_1(x) + \sum_{z \in S_2(x)} \sum_{y \in S_1(x) \cap S_1(z)} \delta(z) = \delta_1(x) + \sum_{z \in S_2(x)} 2\delta(z) \\ &= \delta_1(x) + 2\delta_2(x)\,, \end{aligned}$$

and the lemma is proved. □

Lemma 4.

$$\frac{\delta_1}{2} + \delta_2 \geq \binom{A_1}{2}\,.$$

Proof. We shall use the notations of the preceeding proof. Let us put

$$E_1 = \{\{x_1, x_2\} \subset S_1(x) \cap C \ :\ x_2 = \bar{x}_1\} \text{ and } E_2 = \{\{x_1, x_2\} \subset S_1(x) \cap C \ :\ x_2 \neq \bar{x}_1\}\,.$$

For $\{x_1, x_2\} \in E_1$, the points x, x_1 and x_2 are collinear. This implies that $\delta(y) \geq 1$ for $y \in \{x, x_1, x_2\}$, which shows that

$$\frac{\delta(x_1) + \delta(x_2)}{2} \geq 1\,.$$

For $\{x_1, x_2\} \in E_2$, the point $x_1 + x_2 - x$ belongs to $S_2(x) \cap S_1(x_1) \cap S_1(x_2)$, which shows that $\delta(x_1 + x_2 - x) \geq 1$.

Combining these results gives the inequalities

$$\begin{aligned} \binom{A_1(x)}{2} = \sum_{\{x_1,x_2\} \subset S_1(x) \cap C} 1 &\leq \sum_{\{x_1,x_2\} \in E_1} \frac{\delta(x_1) + \delta(x_2)}{2} + \sum_{\{x_1,x_2\} \in E_2} \delta(x_1 + x_2 - x) \\ &\leq \frac{\delta_1(x)}{2} + \delta_2(x)\,, \end{aligned}$$

and the lemma is proved. □

Lemma 5. *For any element x of H such that $\delta(x)$ is even and $\delta_2(x) = 1$, we have $\delta_1(x) \geq 2$.*

Proof. The proof proceeds as in the previous lemma and we use again the notations of Lemma 3. If $\delta_2(x)$ equals 1, there exists $y \in S_2(x)$ such that $\delta(y) = 1$. For $z \in S_1(x) \cap S_1(y)$, we have $\delta_1(z) = \delta(x) + \delta(\bar{z}) + 1 \equiv 1 + \delta(\bar{z}) \equiv 0 \mod 2$, which shows that $\delta_1(x) \geq \delta(\bar{z}) \geq 1$. Since $\delta_1(x)$ is even, the lemma is proved. □

Lemma 6. *For any element x of C, we have $\delta_1(x) \geq 2\delta(x)$.*

Proof. For x in C, we have $\delta(x) = A_1(x)$ and $\delta_1(x) = 2(A_1(x) + A_2(x))$, which makes the lemma obvious. □

We shall also need the quantity $A_3(n,3)$, the maximum cardinality of a subset of H such that any two distinct elements of this subset have distance at least 3. This quantity also equals the maximum number of disjoint spheres of radius one in H. Let us put

$$C_0 = \{c \in C \ : \ \mathrm{d}(c, C \setminus \{c\}) \geq 3\} = \{c \in C \ : \ A_1(c) = A_2(c) = 0\}.$$

By definition we have the estimate

$$|C_0| \leq A_3(n,3). \tag{6}$$

4. Applications to the football pool problem

In this section, we shall first study the case $n \equiv 0 \mod 3$, then the case $n \equiv 2 \mod 3$, and we shall end with an updated table of the best lower bounds of which the author is aware.

Let n be a positive multiple of 3. We introduce the nonnegative function

$$\varphi = 2\delta + 3\frac{\delta_1}{2} + \delta_2 .$$

By (5), we also have $\varphi = (3n+2)A_0 + (2n+3)A_1 + 6A_2 + 3A_3 - 2n^2 - n - 2$, which shows that

$$\varphi \equiv 1 - A_0 \mod 3. \tag{7}$$

We shall use this property to prove the following crucial lemma.

Lemma 7. *For x in $H \setminus C$, we have $\varphi(x) \geq 4$.*

Proof. For x in $H \setminus C$, we already know by (7) that $\varphi \equiv 1 \mod 3$. If $\varphi(x)$ equals 1, we must have, by definition, $\delta(x) = \delta_1(x) = 0$ and $\delta_2(x) = 1$, which is impossible by Lemma 5. Therefore $\varphi(x)$ is greater than one, and one concludes by using (7). □

We need one more lemma before estimating the size of $|C|$.

Lemma 8. *For y in Z, we have $2A_0 + \frac{3}{2}A_1 + A_2 \geq \frac{7}{2}$.*

Proof. For $y \in (H \setminus C) \cap Z$, the conditions $\delta(y) \geq 1$ and $\delta_1(y) \geq 0$ imply the lower bounds $A_1(y) \geq 2$ and $(A_1 + A_2)(y) \geq n$, which show that $(2A_0 + \frac{3}{2}A_1 + A_2)(y) \geq n + 1 \geq \frac{7}{2}$.

For $y \in C \cap Z$, the condition $\delta(y) \geq 1$ implies that $A_1(y) \geq 1$. We therefore have $2A_0 + \frac{3}{2}A_1 + A_2 \geq 2 + \frac{3}{2} = \frac{7}{2}$ and the proof of the lemma is complete. □

Let us now use these results to obtain a lower bound for $|C|$.

Theorem 9. *Let n be a positive integer, with $n \equiv 0 \mod 3$. Then we have*

$$K_3(n,1) \geq \frac{(4n^2 + 2n + 5)3^n}{(2n+1)(4n^2 + 2n - 3) + 8}.$$

Proof. Let us put $S = \sum_{x\in H\setminus C} \varphi(x)$. By definitions, we obtain

$$\begin{aligned} S &= \sum_{x\in H\setminus C} \left(2\delta + 3\frac{\delta_1}{2} + \delta_2\right)(x) \\ &= \sum_{y\in H} \delta(y)\left(2|S_0(y)\cap(H\setminus C)| + \frac{3}{2}|S_1(y)\cap(H\setminus C)| + |S_2(y)\cap(H\setminus C)|\right) \\ &= \sum_{y\in Z} \delta(y)\left(2n^2+n+2-\left(2A_0+\frac{3}{2}A_1+A_2\right)(y)\right). \end{aligned}$$

We then use Lemma 8 and formula (4) to get

$$S \le \left(2n^2+n+2-\frac{7}{2}\right)|\delta| = \left(2n^2+n-\frac{3}{2}\right)((2n+1)|C|-3^n).$$

Since Lemma 7 ensures us that $S \ge 4|H\setminus C| = 4(3^n - |C|)$, we have

$$8(3^n-|C|) \le 2S \le (4n^2+2n-3)((2n+1)|C|-3^n),$$

and the theorem follows. $\square$

This theorem gives the following improvements. We indicate in parenthesis the former best previous bound, according to [2].

$$\begin{aligned} K_3(9,1) &\ge 1060 \qquad (1048) \\ K_3(12,1) &\ge 21531 \qquad (21395) \end{aligned}$$

Theorem 9 can be refined by a much closer analysis of the size of $\varphi(x)$, according to the possible values of $A_1(x)$. We can prove the following inequality

$$(4n^2+2n-3)|\delta| \ge 8(3^n-|C|) + 2(n-3)|(H\setminus C)\cap Z|,$$

which extends the last inequality in the proof of Theorem 9. However, it does not seem easy to get a non-trivial estimate for $|(H\setminus C)\cap Z|$. Indeed, when $n \not\equiv 0 \mod 3$, for instance $n = 4, 5$, we can have $Z \subset C$ for an optimal covering code C.

Let us now study the case $n \equiv 2 \mod 3$.

Let n be a positive integer with $n \equiv 2 \mod 3$. In this case we introduce the nonnegative function

$$\varphi = \delta + \frac{3}{2}\delta_1 + \delta_2.$$

By (5) we have $\varphi = (3n+1)A_0 + 2(n+1)A_1 + 6A_2 + 3A_3 - 2n^2 - n - 1$, which shows that

$$\varphi \equiv 1 + A_0 \mod 3. \tag{8}$$

We shall need the following crucial lemma.

Lemma 10. *We have*

$$\varphi(x) \geq \begin{cases} 4 & \textit{if } x \in H \setminus C, \\ 2 & \textit{if } x \in C_0, \\ 5 & \textit{if } x \in C \setminus C_0. \end{cases}$$

Proof. For x in $H \setminus C$, we have $\varphi(x) \equiv 1 \mod 3$, by (8). If $\varphi(x)$ equals 1, either $(\delta(x), \delta_1(x), \delta_2(x)) = (1,0,0)$ or $(\delta(x), \delta_1(x), \delta_2(x)) = (0,0,1)$. The first case is impossible by Lemma 3, as is the second by Lemma 5. Therefore we have $\varphi(x) \geq 4$.

For x in C, we have $\varphi(x) \equiv 2 \mod 3$, by (8). This shows that $\varphi(x) \geq 2$. Moreover, for $x \in C \setminus C_0$, we know that $(\delta + \delta_1)(x)$ is a positive integer. By Lemma 6, we cannot have both $\delta(x) > 0$ and $\delta_1(x) = 0$. This implies that, for $x \in C \setminus C_0$, $\delta_1(x) > 0$ and thus $\varphi(x) \geq 3$. By (8) this proves that $\varphi(x) \geq 5$ for any $x \in C \setminus C_0$. □

Let us apply this lemma to get a lower bound for $|C|$.

Theorem 11. *Let n be a positive integer, with $n \equiv 2 \mod 3$. Then we have*

$$K_3(n,1) \geq \frac{(2n^2+n+5)3^n - 3A_3(n,3)}{(2n+1)(2n^2+n+1)-1}.$$

Proof. We compute $|\varphi|$:

$$\begin{aligned} |\varphi| &= \sum_{x \in H \setminus C} \varphi(x) + \sum_{x \in C \setminus C_0} \varphi(x) + \sum_{x \in C_0} \varphi(x) \\ &\geq 4(3^n - |C|) + 2|C_0| + 5(|C| - |C_0|) \qquad \text{by Lemma 10,} \\ &\geq 4.3^n + |C| - 3A_3(n,3) \qquad \text{by (6).} \end{aligned}$$

Moreover we have

$$|\varphi| = (2n(n-1) + 3n + 1)|\delta| = (2n^2+n+1)((2n+1)|C| - 3^n),$$

by (3-4) and the definition of φ. A straightforward calculation then completes the proof of the theorem. □

This theorem, together with the upper bounds for $A_3(n,3)$ to be found in [7], gives the following improvements. We indicate in parenthesis the former best lower bound for $K_3(n,1)$, according to [1,2,6].

$$\begin{aligned} K_3(8,1) &\geq 397 \qquad (393) \\ K_3(11,1) &\geq 7822 \qquad (7767) \\ K_3(14,1) &\geq 166526 \qquad (165775) \end{aligned}$$

We give below an updated list of the best lower bounds for $K_3(n,1)$ when $n \leq 14$. We consider only those values of n for which $K_3(n,1)$ is still unknown. The bound $K_3(6,1) \geq 63$ was stated without proof in [9] ; we proved in [3] the lower bound $K_3(6,1) \geq 60$.

n	Lower bound for $K_3(n,1)$	Reference
6	63	[9]
7	153	[4]
8	397	Theorem 11
9	1060	Theorem 9
10	2818	[3]
11	7822	Theorem 11
12	21531	Theorem 9
14	166526	Theorem 11

5. General results for covering radii greater than one

Let R be an integer greater than one. Let us recall that $\delta = A_0 + \cdots + A_R - 1$. Lemma 1 gives

$$\begin{aligned}\delta_1 &= 2n(A_0 + \cdots + A_{R-1} - 1) + 2RA_R + (R+1)A_{R+1}\,,\\ \delta_2 &= 2n(n-1)(A_0 + \cdots + A_{R-2} - 1) + 2(R-1)(2n-R)A_{R-1}\\ &\qquad + 2R(n-1)A_R + 3\binom{R+1}{2}A_{R+1} + \binom{R+2}{2}A_{R+2}\,.\end{aligned}$$

This shows that

$$\begin{aligned}2\delta + \delta_1 &= 2(n+1)(A_0 + \cdots + A_{R-1} - 1) + (R+1)(2A_R + A_{R+1})\\ &\equiv 2(n+1)(A_0 + \cdots + A_{R-1} - 1) \mod (R+1)\,.\end{aligned}$$

Let us put $\epsilon = (R+1)\lceil 2(n+1)/(R+1)\rceil - 2(n+1)$, where $\lceil t\rceil$ denotes the least integer greater than or equal to t. We then have $\epsilon \in \{0, \ldots, R\}$ and

$$2\delta + \delta_1 \equiv \epsilon(1 - A_0 - \cdots - A_{R-1}) \mod (R+1)\,. \tag{9}$$

Let us put

$$T = \{x \in H \ :\ A_0(x) = \cdots = A_{R-1}(x) = 0\} = \{x \in H \ :\ B_{R-1}(x) \cap C = \emptyset\}\,.$$

We have

$$|T| = \sum_{x\in T}(1 - A_0 - \cdots - A_{R-1}) \geq \sum_{x\in H}(1 - A_0 - \cdots - A_{R-1}) = 3^n - \left(\sum_{r=0}^{R-1} 2^r\binom{n}{r}\right)|C|\,, \tag{10}$$

by (3). Moreover, for $x \in T$, we have $(2\delta+\delta_1)(x) \equiv \epsilon \mod (R+1)$ and thus $(2\delta+\delta_1)(x) \geq \epsilon$, since ϵ belongs to $\{0, \ldots, R\}$. For $x \in H \setminus T$, we know that

$$\epsilon(1 - A_0 - \cdots - A_{R-1})(x) \leq 0 \leq (2\delta + \delta_1)(x)\,.$$

Therefore we have

$$2\delta + \delta_1 \geq \epsilon(1 - A_0 - \cdots - A_{R-1})\,, \tag{11}$$

which gives a lower bound for $|C|$. When ϵ is greater than one, we shall study the properties (9) and (11) on spheres of radius one. When ϵ equals one, the inequality (11) can be refined, as will be shown in the next section. Before doing so, we shall need to estimate the number of elements of T in spheres or balls. The next lemma gives lower bounds for the number of elements in spheres which are not in T and is analogous to Lemma 2 in [1].

Lemma 12. *For $n \geq (R+1)/2$, we have*

$$|S_1(y) \cap (H \setminus T)| \geq \begin{cases} R & \text{if } y \in H,\\ R+1 & \text{if } y \in Z.\end{cases}$$

Proof. Let y be in H. There exists c in $C \cap B_R(y)$.

Then we have

$$|S_1(y) \cap (H \setminus T)| \geq |S_1(y) \cap B_{R-1}(c)| = \begin{cases} R & \text{if } \mathrm{d}(y,c) = R, \\ 2(R-1) & \text{if } \mathrm{d}(y,c) = R-1, \\ 2n & \text{if } \mathrm{d}(y,c) \leq R-2, \end{cases}$$

which shows that $|S_1(y) \cap (H \setminus T)| \geq R$. If $y \in Z$, there exists another element d in $C \cap B_R(y)$. If $\mathrm{d}(y,d) = \mathrm{d}(y,c) = R$ or $\mathrm{d}(y,d) = \mathrm{d}(y,c) + 1 = R$, there is a coordinate of d which is different from the same coordinate for y and c. This provides an element in $S_1(y) \cap (B_{R-1}(d) \setminus B_{R-1}(c))$. If $\mathrm{d}(y,d) \leq R-2$, we already know that $|S_1(y) \cap B_{R-1}(c)| \geq 2n \geq R+1$. Thus, in every case we have $|S_1(y) \cap (H \setminus T)| \geq R+1$ for $y \in Z$. $\square$

6. Applications with $R \geq 2$

Let us start with $R = 2$ and $n \equiv 3 \mod 6$. In this case, we have

$$\begin{aligned} \delta &= A_0 + A_1 + A_2 - 1\,, \\ \delta_1 &= 2n(A_0 + A_1 - 1) + 4A_2 + 3A_3\,, \\ \delta_2 &= 2n(n-1)(A_0 - 1) + 4(n-1)(A_1 + A_2) + 9A_3 + 6A_4\,, \end{aligned}$$

which gives the congruence $\delta_1 + 2\delta \equiv 1 - A_0 - A_1 \mod 3$. Here we have $\epsilon = 1$.

Theorem 14. *Let n be a positive integer with $n \equiv 3 \mod 6$. Then we have*

$$K_3(n,2) \geq \frac{(2n^2+1)3^n}{(2n^2-n-2)(2n^2+1) + (n+3)(2n+1)}\,.$$

Proof. Let n be a positive integer with $n \equiv 3 \mod 6$. Let us introduce the nonnegative function φ defined by

$$\varphi = \frac{1}{3}(\delta + 2\delta_1 + 2(A_0 + A_1 - 1)) = \left(4\frac{n}{3} + 1\right)(A_0 + A_1 - 1) + 3A_2 + 2A_3\,.$$

We get

$$\begin{aligned} \varphi_1 &= \frac{1}{3}(4(n-1)(A_0-1) + 4(n+1)\delta + 3\delta_1 + 4\delta_2) \\ &= 2n\left(4\frac{n}{3} + 1\right)(A_0 - 1) + \left(26\frac{n}{3} - 4\right)A_1 + 20\frac{n}{3}A_2 + 15A_3 + 8A_4\,. \end{aligned}$$

From these expressions we deduce

$$\frac{5}{2}\delta + \frac{1}{2}\varphi + \varphi_1 = \left(8\frac{n}{3}(n+1) + 3\right)(A_0 - 1) + \left(28\frac{n}{3} - 1\right)A_1 + \left(20\frac{n}{3} + 4\right)A_2 + 16A_3 + 8A_4\,,$$

which gives the congruence

$$\frac{5}{2}\delta + \frac{1}{2}\varphi + \varphi_1 \equiv 5(1 - A_0 - A_1) \mod 8\,.$$

We therefore have $\frac{5}{2}\delta + \frac{1}{2}\varphi + \varphi_1 \geq 5(1 - A_0 - A_1)$, which can be expressed as

$$\delta_2 + \delta_1 + (n+3)\delta \geq (n+3)(1 - A_0) - 4A_1 \, .$$

Let us study what happens on T.

For $x \in T \cap (H \setminus Z)$, we know that $\delta_2 + \delta_1 \geq n+3$. For $x \in T \cap Z$, we have $A_2(x) \geq 2$. Let z_1, z_2 be in $S_2(x) \cap C$. From the property $S_1(z_1) \cap S_1(z_2) \cap S_2(x) \neq \emptyset$, we deduce that $\delta_2(x) > 0$, for any element x in T. This in turn implies that $(\delta_2 + \delta_1)(x) \geq 6$, by using the congruence property $\delta_2 + \delta_1 \equiv 0 \mod 6$. Therefore, for any x in T, we get

$$\delta_2 + \delta_1 + (n-3)\delta \geq n + 3 \, .$$

Summing over T gives

$$\begin{aligned} (n+3)|T| &\leq \sum_{x \in T} (\delta_2 + \delta_1 + (n-3)\delta)(x) \\ &= \sum_{y \in Z} \delta(y) \left(|S_2(y) \cap T| + |S_1(y) \cap T| + (n-3)|S_0(y) \cap T| \right) . \end{aligned}$$

Let us introduce the function F defined on H by $F(x) = |S_1(x) \cap (H \setminus T)| - 2$. By Lemma 12, we know that F is nonnegative. From Lemma 1 we obtain

$$2|S_2(y) \cap (H \setminus T)| + |S_1(y) \cap (H \setminus T)| + 2n|S_0(y) \cap (H \setminus T)| = F_1 + 4n \geq 4n \, .$$

By Lemma 12, we also know that $|S_1(y) \cap (H \setminus T)| \geq 3$ for any y in Z. Combining these two last inequalities gives, for any y in Z,

$$\begin{aligned} &2\left(|S_2(y) \cap (H \setminus T)| + |S_1(y) \cap (H \setminus T)| + (n-3)|S_0(y) \cap (H \setminus T)| \right) \\ &\qquad \geq 4n + 3 - 6|S_0(y) \cap (H \setminus T)| \geq 4n - 3 \, , \end{aligned}$$

which implies that

$$(n+3)|T| \leq \sum_{y \in Z} \delta(y)(|S_2(y)| + |S_1(y)| + (n-3)|S_0(y)| - (2n-1)) = (2n^2 - n - 2)|\delta| \, .$$

From (4) and (10), we obtain

$$(n+3)(3^n - (2n+1)|C|) \leq (2n^2 - n - 2)((2n^2+1)|C| - 3^n) \, ,$$

and the theorem follows. $\square$

This theorem provides the lower bound $K_3(9,2) \geq 130$, which improves on the lower bound 128 given in [2].

Let us give a first special case, which improves on the bound $K_3(14,2) \geq 12193$ given in [6].

Theorem 15. $K_3(14, 2) \geq 12204$.

Proof. In this case, Lemma 1 provides the formulas

$$\begin{aligned}
\delta &= A_0 + A_1 + A_2 - 1\,,\\
\delta_1 &= 28A_0 + 28A_1 + 4A_2 + 3A_3 - 28\,,\\
\delta_2 &= 364A_0 + 52A_1 + 52A_2 + 9A_3 + 6A_4 - 364\,,\\
\delta_3 &= 312A_1 + 72A_2 + 73A_3 + 16A_4 + 10A_5 - 2912\,,
\end{aligned}$$

which imply the properties

$$\begin{aligned}
3\delta_3 + 2\delta_2 + \frac{\delta_1}{3} + \frac{26}{3}\delta &= 746A_0 + 1058A_1 + 330A_2 + 240A_3 + 60A_4 + 30A_5 - 9482\\
&\equiv 28 - 4A_0 - 22A_1 \mod 30\,.
\end{aligned}$$

This shows that, for any element x in T, we have

$$(3\delta_3 + 2\delta_2 + \frac{1}{3}\delta_1 + \frac{26}{3}\delta)(x) \geq 28\,. \tag{12}$$

Let us introduce the function F defined on H by $F(x) = |S_1(x) \cap (H \setminus T)| - 2$. By Lemma 12, we know that F is nonnegative. From Lemma 1 we obtain, for any $y \in Z$,

$$\begin{aligned}
&2|S_2(y) \cap (H \setminus T)| + |S_1(y) \cap (H \setminus T)| + 28|S_0(y) \cap (H \setminus T)| = F_1 + 56 \geq 56\\
&3|S_3(y) \cap (H \setminus T)| + 2|S_2(y) \cap (H \setminus T)| + 26|S_1(y) \cap (H \setminus T)| = F_2 + 728 \geq 728\,.
\end{aligned}$$

We deduce from these inequalities that

$$3|S_3(y)\cap(H\setminus T)|+2|S_2(y)\cap(H\setminus T)|+\frac{1}{3}|S_1(y)\cap(H\setminus T)|+\frac{26}{3}|S_0(y)\cap(H\setminus T)| \geq 18\,, \tag{13}$$

the equality holding if and only if the quadruple $(|S_3(y)\cap(H\setminus T)|, |S_2(y)\cap(H\setminus T)|, |S_1(y)\cap(H \setminus T)|, |S_0(y) \cap (H \setminus T)|)$ equals $(0, 0, 28, 1)$. We now sum the inequality (12) over T and we use (13) to obtain

$$\begin{aligned}
S &= \sum_{x\in T}(3\delta_3 + 2\delta_2 + \frac{1}{3}\delta_1 + \frac{26}{3}\delta)(x)\\
&= \sum_{y\in Z}\delta(y)\left(3|S_3(y) \cap T| + 2|S_2(y) \cap T| + \frac{1}{3}|S_1(y) \cap T| + \frac{26}{3}|S_0(y) \cap T|\right)\\
&\leq \sum_{y\in Z}\delta(y)\left(3|S_3(y)| + 2|S_2(y)| + \frac{1}{3}|S_1(y)| + \frac{26}{3}|S_0(y)| - 18\right)\\
&= 9464|\delta| = 28 \times (338|\delta|)\,,
\end{aligned}$$

and $S \geq 28|T| \geq 28(3^{14} - 29|C|)$. In this way we find

$$|C| \geq \frac{(338 + 1)3^{14}}{338 \times 393 + 29} = 12203.747\ldots\,,$$

and the theorem is proved. □

Let us prove another partial result, for $R = 3$ and $n = 13$. In this case we have the following lower bound, which improves on the lower bound 609 given in [2].

Theorem 16. $K_3(13,3) \geq 611$.

Proof. In this case, Lemma 1 provides the formulas

$$\begin{aligned}
\delta &= A_0 + A_1 + A_2 + A_3 - 1\,,\\
\delta_1 &= 26A_0 + 26A_1 + 26A_2 + 6A_3 + 4A_4 - 26\,,\\
\delta_2 &= 312A_0 + 312A_1 + 92A_2 + 72A_3 + 18A_4 + 10A_5 - 312\,,\\
\delta_3 &= 2288A_0 + 528A_1 + 440A_2 + 200A_3 + 136A_4 + 40A_5 + 20A_6 - 2288\,,
\end{aligned}$$

which imply the properties

$$\begin{aligned}
\delta_3 + \delta_1 + 14\delta &= 2328A_0 + 568A_1 + 480A_2 + 220A_3 + 140A_4 + 40A_5 + 20A_6 - 2328\\
&\equiv 12(1 - A_0 - A_1) \mod 20\,.
\end{aligned}$$

Let us put $T' = \{x \in H \,:\, A_0(x) = A_1(x) = 0\}$, so that $|T'| \geq 3^{13} - 27|C|$, by analogy with (10). Moreover, for any element x of T', we have the congruence $(\delta_3 + \delta_1 + 14\delta)(x) \equiv 12 \mod 20$. This shows the weaker congruence $(\delta_3 + \delta_1 + 4\delta)(x) \equiv 2 \mod 10$. Therefore we get either $(\delta_3 + \delta_1 + 4\delta)(x) = 2$ or $(\delta_3 + \delta_1 + 4\delta)(x) \geq 12$. The first case is impossible, since it implies $\delta(x) = 0$ and contradicts the congruence $(\delta_3 + \delta_1 + 14\delta)(x) \equiv 12 \mod 20$. Thus we have proved that, for any element x of T', the inequality $(\delta_3 + \delta_1 + 4\delta)(x) \geq 12$ holds. Summing this last inequality over T' gives

$$(2288 + 26 + 4)|\delta| \geq 12|T'| \geq 12(3^{13} - 27|C|)\,,$$

which in turn provides the lower bound

$$|C| \geq \frac{(2318 + 12)3^{13}}{2318 \times 2627 + 12 \times 27} = 610.0081\ldots\,,$$

and the theorem follows. $\square$

Let us improve the bound $K_3(14,4) \geq 254$ given by Lo and Zhang [6].

Theorem 17. $K_3(14,4) \geq 255$.

Proof. In this case we have

$$\begin{aligned}
\delta &= A_0 + A_1 + A_2 + A_3 + A_4 - 1\,,\\
\delta_1 &= 28(A_0 + A_1 + A_2 + A_3 - 1) + 8A_4 + 5A_5\,,\\
\delta_2 &= 364(A_0 + A_1 + A_2 - 1) + 144A_3 + 104A_4 + 30A_5 + 15A_6\,,
\end{aligned}$$

which gives the properties

$$\begin{aligned}
\delta_2 + \delta &= 365(A_0 + A_1 + A_2 - 1) + 145A_3 + 105A_4 + 30A_5 + 15A_6\\
&\equiv 10(1 - A_0 - A_1 - A_2) - 5A_3 \mod 15\,.
\end{aligned}$$

We now introduce the nonnegative function

$$\begin{aligned}
\varphi &= \frac{\delta_2 + \delta + 10(A_0 + A_1 + A_2 - 1) + 5A_3}{15}\\
&= 25(A_0 + A_1 + A_2 - 1) + 10A_3 + 7A_4 + 2A_5 + A_6\,.
\end{aligned}$$

Lemma 1 gives us

$$\varphi_1 = 700(A_0 + A_1 - 1) + 340A_2 + 259A_3 + 108A_4 + 63A_5 + 18A_6 + 7A_7\,,$$

from which we deduce the congruence property

$$5\varphi_1 + 15\varphi + \delta_1 + 12\delta \equiv 5(1 - A_0 - A_1 + 3A_2 + 3A_3) \mod 35\,.$$

If $3(A_2 + A_3) - A_0 - A_1$ is less than or equal to 5, we get $5(1 - A_0 - A_1 + 3A_2 + 3A_3) < 35$ and therefore

$$5\varphi_1 + 15\varphi + \delta_1 + 12\delta \geq 5(1 - A_0 - A_1 + 3A_2 + 3A_3)\,. \tag{14}$$

If $3(A_2 + A_3) - A_0 - A_1$ is greater than 5, we get $A_2 + A_3 \geq 2$ from which we deduce $\delta_1 + 12\delta \geq 40(A_2 + A_3 - 1) \geq 5 + 15(A_2 + A_3)$ and (14) is still true. Expressed in terms of the A_i's, the inequality (14) becomes

$$A_7 + 3A_6 + 10A_5 + 19A_4 + 42A_3 + 60A_2 + 112(A_0 + A_1 - 1) \geq 0\,.$$

Summing this last inequality over H provides the following lower bound

$$|C| \geq \frac{112}{2108208} 3^{14} = 254.098\ldots\,,$$

and the theorem follows. □

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, S. N. Litsyn, A.C. Lobstein and H. F. Mattson, Covering radius 1985–1994, preprint.

[3] L. Habsieger, Lower bounds for q-ary covering codes, *J. Combin. Theory Ser. A* **67** (1994), 199–222.

[4] L. Habsieger, A new lower bound for the football pool problem for 7 matches, preprint.

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

[6] C. Lo and Z. Zhang, New lower bounds for $K_3(n, R)$ from linear inequalities, *IEEE Trans. Inform. Theory*, submitted.

[7] R. J. M. Vaessens, E" H. L. Aarts and J. H. van Lint, Genetic algorithms in coding theory-A table for $A_3(n, d)$,*Discrete Applied Mathematics* **45** (1993), 71–87.

[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] G. J. M. Weber, On the football pool problem for 6 matches: a new upper bound, *J. Combin. Theory Ser. A* **35** (1983), 106–108.