Lower bounds for quaternary covering codes

WOLFGANG HAAS

December 2, 2006

Abstract

Let $K_q(n, R)$ denote the least cardinality of a q-ary code of length n, such that every q-ary word of length n differs from at least one word in the code in at most R places. We use a method of Blass and Litsyn to derive the bounds $K_4(5,2) \geq 14$ and $K_4(6,2) \geq 32$.

1 Introduction

Let $K_q(n, R)$ denote the least number of a collection (a code) of q-ary words of length n, such that every q-ary word of length n differs from at least one word in the collection in at most R places. The set of q-ary words of length n we denote by $\mathbf{F}_q^n$. W.l.o.g. we may assume $\mathbf{F}_q = \{0, 1, ..., q-1\}$. Let $d(,)$ stand for the Hamming distance on $\mathbf{F}_q^n$, i.e. the number of coordinates, in which two words from $\mathbf{F}_q^n$ differ.

For a monograph on covering codes see [4]. An updated table of bounds on $K_q(n, R)$ is published in internet by Kéri [5].

In a recent paper Blass and Litsyn [1] developed a method to derive lower bounds for $K_q(n, R)$ by showing directly, that for every q-ary code of length n with size small enough, there always exists a word with Hamming distance at least $R+1$ from every codeword. It depends on elementary estimations of the generalized function $N_q(d_1, d_2, ..., d_M)$, which denotes the least N, such that whenever $\mathbf{x}_1, ..., \mathbf{x}_M \in \mathbf{F}_q^N$ there exists $\mathbf{x} \in \mathbf{F}_q^N$ such that $d(\mathbf{x}, \mathbf{x}_i) \geq d_i$ for $1 \leq i \leq M$. In this note we use the method of Blass and Litsyn to derive $K_4(5,2) \geq 14$ and $K_4(6,2) \geq 32$ improving on the previously best known bounds $K_4(5,2) \geq 12$ and $K_4(6,2) \geq 28$ due to Chen and Honkala [3]. The best known upper bounds are $K_4(5,2) \leq 16$ and $K_4(6,2) \leq 52$ (Östergård [6], [7]).

2 Notations and properties

Let $B_q(\mathbf{x}, R)$ denote the q-ary Hamming ball with radius R centered at $\mathbf{x} \in \mathbf{F}_q^n$, and $V_q(n, R)$ its cardinality, i.e.

$$V_q(n,R) = \sum_{0 \le i \le R} \binom{n}{i} (q-1)^i.$$

We say, that $\mathbf{x}$ r-covers $\mathbf{y}$, if $d(\mathbf{x},\mathbf{y}) \le r$. Let $A_q(n,d)$ denote the maximal cardinality of a q-ary code of length n and minimal Hamming distance at least d.

We use $N_q(d_1^{n_1}, d_2^{n_2}, ..., d_M^{n_M})$ as an abbreviation for

$$N_q(\underbrace{d_1, ..., d_1}_{n_1}, \underbrace{d_2, ..., d_2}_{n_2}, ..., \underbrace{d_M, ..., d_M}_{n_M}).$$

Apparently

$$N_q((R+1)^{m-1}) \le n \Leftrightarrow K_q(n,R) \ge m. \tag{1}$$

When we want to show $N_q(d_1, d_2, ..., d_M) \le N$ we always assume, that arbitrary $\mathbf{x}_1, ..., \mathbf{x}_M \in \mathbf{F}_q^N$ are given. Let $a_i \in \mathbf{F}_q$ then denote the first symbol from $\mathbf{x}_i$ for $1 \le i \le M$. We say the symbols $a_1, ..., a_M$ form the first column of the code.

Property 1 (Blass, Litsyn [1]). If

$$\sum_{1 \le i \le M} V_q(N, d_i - 1) < q^N,$$

then

$$N_q(d_1, d_2, ..., d_M) \le N.$$

Property 2. If

$$m((q-1)N - 1) + 2A_q(N,3) + n < q^N, \tag{2}$$

then

$$N_q(2^m, 1^n) \le N. \tag{3}$$

Proof. Assume $\mathbf{x}_1, ..., \mathbf{x}_m, \mathbf{x}_{m+1}, ..., \mathbf{x}_{m+n} \in \mathbf{F}_q^N$. Let $C_0 \subset C = \{\mathbf{x}_1, ..., \mathbf{x}_m\}$ be a maximal set of minimal Hamming distance at least three. Whenever

$\mathbf{x} \in C - C_0$, then $B_q(\mathbf{x}, 1)$ contains at most $V_q(N, 1) - 2$ elements not already contained in $\bigcup_{\mathbf{y} \in C_0} B_q(\mathbf{y}, 1)$. This implies

$$\begin{aligned}
& \left| \bigcup_{1 \leq i \leq m} B_q(\mathbf{x}_i, 1) \cup \bigcup_{m < i \leq m+n} B_q(\mathbf{x}_i, 0) \right| \\
\leq\ & |C_0| V_q(N, 1) + (|C| - |C_0|)(V_q(N, 1) - 2) + n \\
=\ & |C|(V_q(N, 1) - 2) + 2|C_0| + n \\
\leq\ & m((q-1)N - 1) + 2A_q(N, 3) + n \\
<\ & q^N = |\mathbf{F}_q^N|
\end{aligned}$$

by (2), and (3) follows.

3 Proof of $K_4(5, 2) \geq 14$

From now on we assume $q = 4$ and $a, a_i \in \mathbf{F}_4 = \{0, 1, 2, 3\}$.

a) $N_4(3^2, 2^{11}) \leq 4$.

If a symbol different from a_1, a_2 occurs at most four times in the first column of the code then the result follows from $N_4(2^6, 1^7) \leq 3$ (property 2, use $A_4(3, 3) = 4$ [2]). Otherwise $a_1 \neq a_2$ and at least one of the symbols a_1 and a_2 occurs exactly once in the first column. Then the result follows from $N_4(3, 2, 1^{11}) \leq 3$ (property 1).

b) $N_4(3^{13}) \leq 5$.

If in a column of the code one symbol occurs at most twice then the result follows from a). Otherwise w.l.o.g. let 0 be the symbol which occurs exactly four times in every column of the code. Since the four codewords beginning with 0 may be assumed not all to be equal (by $K_4(5, 2) \geq 12$ [3]), we may assume (after some exchanging of rows and columns of the words), that the first codeword begins with $a_1 0$, where $a_1 \neq 0$. Now there must be a symbol $a^* \neq 0$, which does not occur in the second column of the three codewords beginning with a_1. Since a_1 and a^* occur exactly three times in every column of the code, the result follows from $N_4(2^6, 1^7) \leq 3$ (property 2).

The bound $K_4(5, 2) \geq 14$ now follows from (1) and b).

4 Proof of $K_4(6, 2) \geq 32$

a) $N_4(3, 2^{15}, 1^{15}) \leq 4$.

W.l.o.g. $\mathbf{x}_1 = \mathbf{0}$, the all-zero word. Let $A_i \subset \mathbf{F}_4^4$ $(0 \leq i \leq 4)$ denote the set of words containing the symbol 0 exactly i times. Let $A_{\geq 1} = \mathbf{F}_4^4 - A_0$. For $i = 0, 1$ let u_i (resp. v_i) denote the number of indices j among $\{2, ..., 16\}$

(resp. $\{17, ..., 31\}$) such that $\mathbf{x}_j \in A_0$ if $i = 0$ and $\mathbf{x}_j \in A_{\geq 1}$ if $i = 1$. Every word from A_0 (resp. $A_{\geq 1}$) 1-covers at most 9 (resp. 3) words from A_0 and every word from A_0 (resp. $A_{\geq 1}$) 1-covers at most 4 (resp. 7) words from A_1. a) now follows if we can show

$$A_0 \cup A_1 \not\subset \bigcup_{2 \leq j \leq 16} B_4(\mathbf{x}_j, 1) \cup \bigcup_{17 \leq j \leq 31} B_4(\mathbf{x}_j, 0)$$

since $B_4(\mathbf{x}_1, 2) = A_2 \cup A_3 \cup A_4$. Assuming the contrary, by the previous paragraph we would have

$$9u_0 + 3u_1 + v_0 \geq |A_0| = 81 \tag{4}$$

and

$$4u_0 + 7u_1 + v_1 \geq |A_1| = 108. \tag{5}$$

Addition of (4) and (5) together with $u_0 + u_1 = 15$, $v_0 + v_1 = 15$ yields $3u_0 + 165 = 3u_0 + 10(u_0 + u_1) + (v_0 + v_1) = 13u_0 + 10u_1 + (v_0 + v_1) \geq 189$ and thus $u_0 \geq 8$, but then $4u_0 + 7u_1 + v_1 \leq 4u_0 + 7(15 - u_0) + 15 = 120 - 3u_0 \leq 96$, contradicting (5).

Let $N_4^{(s)}(d_1, ..., d_{31})$ denote the corresponding value of N, when in all columns every symbol occurs at least s times.

b) $N_4^{(7)}(3^7, 2^{24}) \leq 5$.

In each column every symbol occurs at most ten times. If a symbol does not occur among $a_1, ..., a_7$ then the result follows by $N_4(2^{17}, 1^{14}) \leq 4$ (property 1). Otherwise there exists a symbol which occurs exactly once among $a_1, ..., a_7$. Now the result follows from a).

c) $N_4^{(6)}(3^6, 2^{25}) \leq 5$.

In each column every symbol occurs at most thirteen times. If a symbol does not occur among $a_1, ..., a_6$ then the result follows by $N_4(2^{19}, 1^{12}) \leq 4$ (property 2, use $A_4(4, 3) = 16$ [2]). Otherwise there exist at least two different symbols among $a_1, ..., a_6$ which occur exactly once among $a_1, ..., a_6$. At least one of them occurs at most ten (indeed nine) times in the first column. Now the result follows by a).

d) $N_4(3^{31}) \leq 6$.

If a symbol occurs at most five times in a column, the result follows by $N_4(3^5, 2^{26}) \leq 5$ (property 1). Otherwise, if in a column a symbol occurs exactly six times, the result follows by c). And if every symbol occurs at least seven times in every column, the result follows by b).

The bound $K_4(6, 2) \geq 32$ follows from (1) and d).

Wolfgang Haas
Albert-Ludwigs-Universität
Mathematisches Institut
Eckerst. 1
79104 Freiburg
Germany

References

[1] U. BLASS, S. LITSYN, *Several new lower bounds for football pool systems*, Ars Combinatoria **50** (1998), 297-302.

[2] A. BROUWER, *Table of general quaternary codes*, http://www.win.tue.nl/~aeb/codes/quaternary-1.html.

[3] W. CHEN, I.S. HONKALA, *Lower bounds for q-ary covering codes*, IEEE Trans. Inform. Theory **36** (1990), 664-671.

[4] G. COHEN, I.S. HONKALA, S. LITSYN, A. LOBSTEIN, *Covering Codes*, North Holland Mathematical Library, vol 54, 1997, Elsevier.

[5] G. KÉRI, *Tables for Covering Codes*, http://www.sztaki.hu/~keri/codes/.

[6] P.R.J. ÖSTERGÅRD, *Upper bounds for q-ary covering codes*, IEEE Trans. Inform. Theory **37** (1991), 660-664 and **37** (1991), 1738.

[7] P.R.J. ÖSTERGÅRD, *New constructions for q-ary covering codes*, Ars Combinatoria **52** (1999), 51-63.