Lower bounds for $q$-ary codes of covering radius one

Wolfgang Haas

Albert-Ludwigs-Universitaet, Mathematisches Institut, Eckerstr. 1, 79104 Freiburg, Germany

Received 28 September 1998; revised 7 April 1999; accepted 19 July 1999

Abstract

Let $k_q(n)$ denote the minimal cardinality of a $q$-ary code $C$ of length $n$ and covering radius one. The numbers of elements of $C$ that lie in a fixed $k$-dimensional subspace of $\{0,\ldots,q-1\}^n$ satisfy a certain system of linear inequalities. By employing a technique for dealing with ‘large’ values of $k$ (i.e. unbounded with increasing $n$) we are able to derive lower bounds for $k_q(n)$. The method works especially well in cases where the sphere covering bound has not been substantially improved, for example if $q=3$ and $n \equiv 1 \pmod{3}$. As an application we show that the difference between $k_q(n)$ and the sphere covering bound approaches infinity with increasing $n$ if $q$ is fixed and $(q-1)n+1$ does not divide $q^n$. Moreover, we present improvements of already known lower bounds for $k_q(n)$ such as $k_3(10) \geq 2835$. © 2000 Published by Elsevier Science B.V. All rights reserved.

1. Introduction

Let $q$ be an integer greater than one and let $A$ be the set $\{0,1,\ldots,q-1\}$. The Hamming distance between two elements $x=(x_1,\ldots,x_n)$ and $y=(y_1,\ldots,y_n)$ in $A^n$ is defined by

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

Let $\mathcal{C}_q(n)$ denote the set of the subsets of $A^n$ with covering radius one, i.e.

$$\mathcal{C}_q(n) = \{ C \subset A^n: \forall x \in A^n \ \exists y \in C \text{ with } d(x,y) \leq 1 \}$$

and let us define

$$k_q(n) = \min_{C \in \mathcal{C}_q(n)} |C|.$$

Then we have the known sphere covering bound

$$k_q(n) \geq \sigma_q(n) = \left\lceil \frac{q^n}{(q-1)n+1} \right\rceil,$$

where $\lceil s \rceil$ denotes the least integer greater than or equal to $s$. It is well known [6] that if $q$ is a prime power and $(q-1)n+1$ divides $q^n$, the equality holds in (1).
In most other cases the inequality in (1) can be improved (see for instance [1–7]). So Habsieger [2] proved, that \(k_q(n) > \sigma_q(n)\) if \((q - 1)n + 1\) does not divide \(q^n\) and \((q,n) \not\in \{(2,2),(2,4)\}\). This gives rise to the question whether
\[
k_q(n) - \sigma_q(n) \to \infty \quad \text{for } n \to \infty
\] (2)
This was proved by van Wee [7] in the cases \(q = 2, n \not\equiv 1,3 \pmod{6}\) and \(q = 3, n \not\equiv 1 \pmod{3}\). The method depends on certain congruence properties of the counting excess function on some subsets of \(A^n\). In the cases \(q = 2, n \equiv 1,3 \pmod{6}\) and \(q = 3, n \equiv 1 \pmod{3}\) the necessary congruence properties are not satisfied and therefore the method does not work.

To deal with these cases we go back to the well-known system of linear inequalities which is satisfied by the number of elements of \(C \subseteq \mathcal{C}_q(n)\) that lie in a fixed \(k\)-dimensional subspace of \(A^n\) (see [2]). We restate this system in Section 2.

In Section 3 we prove (Theorem 2) that the solutions of such systems are ‘large on average’ if \(k\) is ‘favourable’ (depending on the occurring parameters). The effectivity of Theorem 2 grows with increasing \(k\).

In Section 4 we show that the covering inequalities from Section 2 always possess ‘favourable’ values of \(k\) which are unbounded with increasing \(n\). An application of Theorem 2 now proves (2) in all cases. More precisely we prove:

**Theorem 1.** Let \(q\) be an integer greater than one. Then there is a constant \(c > 1\) depending only on \(q\), such that if \(n > n_0(q)\) and \((q - 1)n + 1\) does not divide \(q^n\) we have
\[
k_q(n) - \sigma_q(n) > c^n.
\] (3)

In Section 5 we use Theorem 2 to derive a general lower bound for \(k_q(n)\) and improve a few already known lower bounds listed in [1]. For instance, we show \(k_2(21) \geq 95360\) and \(k_3(10) \geq 2835\). The notation of this paper is partially taken from Habsieger [2].

2. The covering inequalities

Let \(C \in \mathcal{C}_q(n)\). For \(\sigma \in A^k, 1 \leq k \leq n\) we define
\[
n_\sigma = |\{x \in C: x = (x_1, \ldots, x_n) \text{ with } (x_1, \ldots, x_k) = \sigma\}|,
\]
\[
N(\sigma) = \{\mu \in A^k: d(\mu, \sigma) = 1\}.
\] (4)
In the following, we shall make frequent use of \(|N(\sigma)| = (q - 1)k\) for each \(\sigma \in A^k\).

**Lemma 1** (Habsieger [2]). If \(C \in \mathcal{C}_q(n)\) we have for each \(\sigma \in A^k\)
\[
[(q - 1)(n - k) + 1]n_\sigma + \sum_{\mu \in N(\sigma)} n_\mu \geq q^{n-k}.
\] (5)
Proof. For $\sigma \in A^k$ let

\[ A_\sigma = \{ x \in A^n : x = (x_1, \ldots, x_\sigma) \text{ with } (x_1, \ldots, x_k) = \sigma \}. \]

It is required, that $C$ covers each of the $q^n-k$ elements from $A_\sigma$, $\sigma \in A^k$. This can be done only by elements of $C \cap A_\sigma$ and by the elements of $C \cap A_\mu$ with $\mu \in N(\sigma)$. Since each of the $n_\sigma$ elements of $C \cap A_\sigma$ covers exactly $(q-1)(n-k)+1$ elements of $A_\sigma$ and each of the $n_\mu$ elements of $C \cap A_\mu$ covers exactly one element of $A_\mu$, (5) follows.

3. The main tool

Theorem 2. Let $q,k,l,r,h$ be positive integers with $q \geq 2$. Assume the non-negative integers $x_\sigma$, $\sigma \in A^k$ satisfy

\[ lx_\sigma + \sum_{\mu \in N(\sigma)} x_\mu \geq h \text{ for each } \sigma \in A^k. \]  \hspace{1cm} (6)

If

\[ h \geq l(r - 1) + (q - 1)k(r + 1) - (q - 2) \]  \hspace{1cm} (7)

and

\[ l \geq (q - 1)k \]  \hspace{1cm} (8)

holds, then we have

\[ \sum_{\sigma \in A^k} x_\sigma \geq rq^k. \]  \hspace{1cm} (9)

Proof. Assume the assumptions of Theorem 2 are satisfied, but

\[ \sum_{\sigma \in A^k} x_\sigma \leq rq^k - 1 \]  \hspace{1cm} (10)

holds. We set $B = \{ \sigma \in A^k : x_\sigma < r \}$, $N = |B|$ and use the abbreviation $Z = \sum_{\sigma \in B} (r - 1 - x_\sigma)$.

We define $y_\sigma$ for $\sigma \in A^k$ by

\[ y_\sigma = \begin{cases} x_\sigma - r & \text{if } x_\sigma \geq r, \\ 0 & \text{otherwise}. \end{cases} \]  \hspace{1cm} (11)

Of course $y_\sigma \geq 0$ for each $\sigma \in A^k$. Furthermore, for each $\sigma \in A^k$ we have

\[ \sum_{\mu \in N(\sigma)} y_\mu = \sum_{\mu \in N(\sigma)} (x_\mu - r) + \sum_{\mu \in N(\sigma) \cap B} (r - x_\mu) \]
\[ \geq \sum_{\mu \in N(\sigma)} x_\mu - r(q - 1)k + \sum_{\mu \in N(\sigma) \cap B} 1 \]
\[ \geq h - lx_\sigma - r(q - 1)k + \sum_{\mu \in N(\sigma) \cap B} 1 \text{ by (6)} \]
\[ \geq (q - 1)(k - 1) + 1 + l(r - 1 - x_\sigma) + \sum_{\mu \in N(\sigma) \cap B} 1 \text{ by (7)}. \]  \hspace{1cm} (12)
Therefore, we have

\[
\sum_{\sigma \in B} \sum_{\mu \in N(\sigma)} y_{\mu} \geq N[(q - 1)(k - 1) + 1] + lZ + \sum_{\sigma \in B} \sum_{\mu \in N(\sigma) \setminus B} 1. \tag{13}
\]

On the other side by (11), we have

\[
\sum_{\mu \in A^k} y_{\mu} = \sum_{\mu \in A^k} (x_{\mu} - r) + \sum_{\mu \in A^k, x_{\mu} < r} (r - x_{\mu}) \\
\leq rq^k - 1 - rq^k + \sum_{\sigma \in B} (r - x_{\sigma}) \text{ by (10)} \\
= N - 1 + Z.
\]

Therefore,

\[
\sum_{\sigma \in B} \sum_{\mu \in N(\sigma)} y_{\mu} = \sum_{\mu \in A^k} y_{\mu} \sum_{\sigma \in N(\mu)} 1 \\
= (q - 1)k \sum_{\mu \in A^k} y_{\mu} - \sum_{\mu \in A^k} y_{\mu} \sum_{\mu \in N(\mu) \setminus B} 1 \\
\leq (N - 1)(q - 1)k + lZ - \sum_{\mu \in A^k} y_{\mu} \sum_{\sigma \in N(\mu) \setminus B} 1 \text{ by (8)}. \tag{14}
\]

About the sums occurring on the right-hand side of (13) and (14) we show:

**Lemma 2.**

\[
\sum_{\sigma \in B} \sum_{\mu \in N(\sigma) \setminus B} 1 + \sum_{\mu \in A^k} y_{\mu} \sum_{\sigma \in N(\mu) \setminus B} 1 \geq N(q - 2).
\]

We first finish the proof of Theorem 2 and give the proof of Lemma 2 afterwards.

From (13) and (14) we have

\[
N[(q - 1)(k - 1) + 1] + \sum_{\sigma \in B} \sum_{\mu \in N(\sigma) \setminus B} 1 \leq (N - 1)(q - 1)k - \sum_{\mu \in A^k} y_{\mu} \sum_{\sigma \in N(\mu) \setminus B} 1.
\]

If we add the sum on the right-hand side and use Lemma 2 we get \(N(q - 1)k \leq (N - 1)(q - 1)k\), a contradiction because of \(q \geq 2\) and \(k \geq 1\). This ends the proof of Theorem 2. □

**Proof of Lemma 2.** For \(\sigma \in A^k\) and \(1 \leq j \leq k\) define

\[
K(\sigma, j) = \{\mu \in A^k: \mu \text{ and } \sigma \text{ differ at most in the } j\text{th coordinate}\},
\]

\[
\mathcal{K} = \{K(\sigma, j): \sigma \in A^k, 1 \leq j \leq k\}.
\]
We first show

for each $\sigma \in B$ there is an integer $j_\sigma$ with $1 \leq j_\sigma \leq k$ and

$$\sum_{\mu \in K(\sigma, j_\sigma)} y_\mu \geq |K(\sigma, j_\sigma) \cap B|,$$

(15)

By (12) we have for $\sigma \in B$

$$\sum_{1 \leq j \leq k} \sum_{\mu \in K(\sigma, j)} y_\mu = \sum_{1 \leq j \leq k} \sum_{\mu \in K(\sigma, j) \cap B} y_\mu = \sum_{\mu \in N(\sigma)} 1 = \sum_{1 \leq j \leq k} \sum_{\mu \in K(\sigma, j) \cap B} 1 = \sum_{1 \leq j \leq k} (|K(\sigma, j) \cap B| - 1).$$

Therefore for at least one index $1 \leq j_\sigma \leq k$ we have

$$\sum_{\mu \in K(\sigma, j_\sigma)} y_\mu > |K(\sigma, j_\sigma) \cap B| - 1$$

and (15) follows.

We are now able to prove Lemma 2. We define $\mathcal{K}^* \subset \mathcal{K}$ by

$$\mathcal{K}^* = \left\{ K(\sigma, j) \in \mathcal{K} : \sum_{\mu \in K(\sigma, j)} y_\mu \geq |K(\sigma, j) \cap B| \right\}.$$  

(16)

We assume $|\mathcal{K}^*| = t$ and $\mathcal{K}^* = \{K(\sigma_i, j_i) : 1 \leq i \leq t\}$ and set

$$s_i = |K(\sigma_i, j_i) \cap B| \text{ for } 1 \leq i \leq t.$$

By (15) and by the definition of the $K(\sigma_i, j_i)$ we have

$$\sum_{1 \leq i \leq t} s_i \geq N.$$  

(17)

Apparently,

$$\sum_{\sigma \in B} \sum_{\mu \in N(\sigma) \cap B} y_\mu \sum_{\mu \in \mathcal{K}} 1 \geq \sum_{1 \leq i \leq t} \left\{ \sum_{\sigma \in \mathcal{K}(\sigma_i, j_i) \cap B} \sum_{\mu \in K(\sigma_i, j_i) \cap B} 1 + \sum_{\mu \in K(\sigma_i, j_i) \cap B} y_\mu \sum_{\sigma \in \mathcal{K}(\sigma_i, j_i) \cap B} 1 \right\}.$$  

(18)
To evaluate the inner sums in (18) we note
\[ \sum_{\sigma \in K(i, j)} \sum_{\mu \in K(i, j) \setminus B} 1 = s_i(s_i - 1) \]
and
\[ \sum_{\mu \in K(i, j)} y_{\mu} \sum_{\sigma \in K(i, j) \setminus B} 1 \geq \sum_{\mu \in K(i, j)} y_{\mu}(q - s_i - 1) \geq s_i(q - s_i - 1) \]
(remember that the \( K(i, j) \)'s are elements from \( \mathcal{H}^* \) defined in (16)). The last two statements inserted in (18) yield
\[ \sum_{\sigma \in B} \sum_{\mu \in N(\sigma) \setminus B} 1 + \sum_{\mu \in A^k} \sum_{\sigma \in N(\mu) \setminus B} 1 \geq \sum_{1 \leq j \leq t} [s_j(s_i - 1) + s_j(q - s_i - 1)] = (q - 2) \sum_{1 \leq i \leq t} s_i \geq N(q - 2) \text{ by (17)}, \]
completing the proof of Lemma 2 and therefore the proof of Theorem 2. □

**Remark.** Theorem 2 is the best possible in the sense that conclusion (9) is not necessarily valid if one decreases the right-hand side of assumption (7). To see this, fix a \( \sigma_0 \in A^k \) and define the integers \( x_\sigma, \sigma \in A^k \) by
\[
\begin{cases}
  r + (q - 1)k - 1 & \text{if } \sigma = \sigma_0, \\
  r - 1 & \text{if } \sigma \in N(\sigma_0), \\
  r & \text{otherwise}.
\end{cases}
\]
It is easy to check that these numbers satisfy (6) with \( h = l(r - 1) + (q - 1)k(r + 1) - (q - 2) - 1 \), if (8) is satisfied and \( q \geq 3 \) or \( q = 2 \) and \( l \geq k + 1 \) (a small strengthening of (8)), but we have \( \sum_{\sigma \in A^k} x_\sigma = rq^k - 1 \).

4. **Proof of Theorem 1**

The proof starts with a lemma about certain rationals ‘not near’ to an integer. As convenient, \( ||\xi|| \) denotes the distance of \( \xi \) to a nearest integer and log means the natural logarithm.

**Lemma 3.** Let \( q, n, s \) be integers with \( q \geq 2, n \geq 2 \) and \( 3 \log n + 1 \leq s \leq n \). If \( (q - 1)n + 1 \) does not divide \( q^n \), then there exists a natural number \( k \) in the interval \([s - 3 \log n, s]\) such that the inequality
\[ \left|\frac{q^{n-k}}{(q - 1)n + 1}\right| \geq \frac{1}{2q} \quad (19) \]
holds.
Proof. Let $d$ be a nearest integer to $q^{n-s}/((q - 1)n + 1)$ and write $q^{n-s}/((q - 1)n + 1) = d + \theta$ with $|\theta| \leq \frac{1}{2}$. We have $\theta \neq 0$ because $(q - 1)n + 1$ does not divide $q^n$. Furthermore, $q^{n-s} = d((q - 1)n + 1) + \theta((q - 1)n + 1)$ and therefore $\theta((q - 1)n + 1)$ is an integer $r \neq 0$. It follows $q^{n-s} = d + \frac{r}{(q - 1)n + 1}$ with $r \leq 1$. We have $\frac{r}{(q - 1)n + 1} = 0$ because $(q - 1)n + 1$ does not divide $q^n$. Furthermore, $q^{n-s} = d((q - 1)n + 1) + \frac{r}{(q - 1)n + 1}$ and therefore $\frac{r}{(q - 1)n + 1}$ is an integer $r \neq 0$. It follows $q^{n-s} = d + \frac{r}{(q - 1)n + 1}$ with $r \leq 1$.

(20)

Now let $m$ be the smallest nonnegative integer satisfying

\begin{align*}
\left| \frac{r}{(q - 1)n + 1} \right| \geq \frac{1}{2q}.
\end{align*}

(21)

Such an integer $m$ exists because $r \neq 0$ and $q \geq 2$. If $m = 0$, (19) holds with $k = s$ by (20). If $m > 0$ then we have by definition $|r/((q - 1)n + 1)|q^{m-1} < 1/2q$, i.e.

\begin{align*}
\left| \frac{r}{(q - 1)n + 1} \right| q^m \leq \frac{1}{2q}.
\end{align*}

(22)

This further implies $q^m \leq [(q - 1)n + 1]/2|r| \leq [(q - 1)n + 1]/2 \leq qn/2 \leq qn$ and therefore

\begin{align*}
m \leq \frac{\log qn}{\log q} = 1 + \frac{\log n}{\log q} \leq 2 \frac{\log n}{\log 2} < 3 \log n
\end{align*}

(23)

because of $q \geq 2$ and $n \geq 2$. Now we claim that $k = s - m$ satisfies (19). $k$ lies in the interval $[s - 3\log n, s]$ because of $m \geq 0$ and (23). Moreover, we have

\begin{align*}
\frac{q^{n-k}}{(q - 1)n + 1} = \frac{q^{n-(s-m)}}{(q - 1)n + 1} = \frac{q^{n-s}}{(q - 1)n + 1} q^m = dq^m + \frac{r}{(q - 1)n + 1} q^m,
\end{align*}

which implies (19) by (21) and (22). This completes the proof of Lemma 3. \qed

Proof of Theorem 1. Assume $C \in \mathcal{S}_q(n)$ with $|C| = k_q(n)$. Let $s = \lfloor n/4q \rfloor$, where $\lfloor t \rfloor$ denotes the greatest integer $\leq t$. For $n > n_1(q)$ the integer $s$ satisfies $3\log n + 1 \leq s \leq n$. According to Lemma 3 we choose a natural number $k$ with

\begin{align*}
s - 3\log n \leq k \leq s
\end{align*}

(24)

and

\begin{align*}
\left| \frac{q^{n-k}}{(q - 1)n + 1} \right| \geq \frac{1}{2q}.
\end{align*}

(25)

We further define $r = [q^{n-k}/((q - 1)n + 1)]$. From (25) follows

\begin{align*}
r = \frac{q^{n-k}}{(q - 1)n + 1} + \theta
\end{align*}

(26)

with

\begin{align*}
\frac{1}{2q} \leq \theta \leq 1 - \frac{1}{2q}.
\end{align*}

(27)

We now use Theorem 2. Lemma 1, (5) tells us, that the numbers $n_\sigma$ defined in (4) satisfy (6) with $l = (q - 1)(n - k) + 1$ and $h = q^{n-k}$ for each $\sigma \in A^4$. Furthermore, we
have
\[ l(r - 1) + (q - 1)k(r + 1) - (q - 2) \leq l(r - 1) + (q - 1)k(r + 1) \]
\[ = q^{n-k} + (q - 1)((q - 1)n + 1) + 2k(q - 1) \quad \text{by (26)} \]
\[ \leq h - \frac{1}{2q}(q-1)n + 2k(q - 1) \quad \text{by (27)} \]
\[ \leq h \quad \text{by (24)} \]
and thus (7) is satisfied. From \( k \leq n/2 \) follows that (8) is satisfied. An application of Theorem 2 now yields by (9)
\[ k_q(n) = |C| = \sum_{\sigma \in A^*} n_\sigma \geq rq^k \geq \frac{q^n}{(q-1)n+1} + \theta q^k \quad \text{by (26)} \]
\[ \geq \left[ \frac{q^n}{(q-1)n+1} \right] - 1 + \frac{1}{2q^{k-1}} \quad \text{by (27)} \]
\[ \geq \sigma_q(n) - 1 + \frac{1}{2}q^{|n/4q|-3\log q-1} \quad \text{by (24)} \]
\[ > \sigma_q(n) + c^n \]
with \( c = q^{1/5q} \) if \( n > n_0(q) \geq n_1(q) \). This completes the proof of Theorem 1. \( \square \)

5. A general lower bound for \( k_q(n) \)

**Theorem 3.** Let \( q,n,k \) be integers with \( q \geq 2 \) and \( 1 \leq k \leq n/2 \). Then
\[ k_q(n) \geq \left[ \frac{q^{n-k} + (q-1)(n-2k+1)}{(q-1)n+1} \right] q^k. \quad (28) \]

**Proof.** Assume \( C \in \mathcal{C}_q(n) \) with \( |C| = k_q(n) \). We use Theorem 2. By Lemma 1 the numbers \( n_\sigma \) defined in (4) satisfy (6) with \( l = (q-1)(n-k)+1 \) and \( h = q^{n-k} \). Condition (7) is easily seen to be equivalent to
\[ r \leq \frac{h + l - (q-1)k + (q-2)}{l + (q-1)k}, \]
i.e.
\[ r \leq \frac{q^{n-k} + (q-1)(n-2k+1)}{(q-1)n+1}. \]
Therefore (7) is satisfied if we choose \( r = \lfloor [q^{n-k} + (q-1)(n-2k+1)]/(q-1)n+1 \rfloor \).
To check that \( r \geq 1 \) as required in Theorem 2 one uses induction on \( k \) to show that \( q^k \geq (q-1)(2k-1) + 1 \) holds if \( q \geq 2, k \geq 1 \). By \( n-k \geq k \) this implies \( q^{n-k} \geq
\[(q - 1)(2k - 1) + 1, \text{ which is equivalent to } [q^{n-k} + (q - 1)(n - 2k + 1)]/(q - 1)n + 1 \geq 1, \text{ i.e. } r \geq 1. \text{ Eq. (8) is satisfied because of } k \leq n/2. \text{ By (9) we now have}

\[k_q(n) = |C| = \sum_{\sigma \in A^k} n_{\sigma} \geq r q^k = \left\lfloor \frac{q^{n-k} + (q - 1)(n - 2k + 1)}{(q - 1)n + 1} \right\rfloor q^k,

\]

completing the proof of Theorem 3. \(\square\)

The best-known lower bounds for \(k_q(n)\) are summarized in [1]. We list five improvements of these values (given in brackets, all of them are due to Habsieger [2]).

**Corollary.**

\[
k_2(21) \geq 95360 (95330),
\]
\[
k_2(33) \geq 252.645.376 (252.645.140),
\]
\[
k_3(10) \geq 2835 (2818),
\]
\[
k_4(7) \geq 752 (748),
\]
\[
k_5(9) \geq 52800 (52796).
\]

**Proof.** Use Theorem 3 with \(k = 7, 9, 4, 2, 2\) in that order (the optimal choice of \(k\) may not be unique).

6. Concluding remarks

It was shown in van Wee [7] that there are polynomials \(p_2, p_3\), such that for sufficiently large values of \(n\)

\[
k_2(n) - \sigma_2(n) > \frac{2^n}{p^2(n)}, \quad n \not\equiv 1, 3 \pmod{6}, \quad (29)
\]
\[
k_3(n) - \sigma_3(n) > \frac{3^n}{p^3(n)}, \quad n \not\equiv 1 \pmod{3} \quad (30)
\]

holds. In these cases Theorem 3 does not lead to any new result. The reason is that the proof of Theorem 1 does not lead to the best-possible constant \(c\) in (3). Nevertheless Theorem 1 together with (29) and (30) gives good rise to the following conjecture.

**Conjecture.** For every integer \(q\) there is a polynomial \(p_q\) such that if \(n\) is sufficiently large and \((q - 1)n + 1\) does not divide \(q^n\), we have

\[
k_q(n) - \sigma_q(n) > \frac{q^n}{p_q(n)},
\]
Acknowledgements

The author wishes to thank Prof. Dr. D. Wolke (Freiburg) for support in many respects.

References