On the failing cases of the Johnson bound for error-correcting codes

Wolfgang Haas
Albert-Ludwigs-Universität
Mathematisches Institut
Eckerstr. 1
79104 Freiburg, Germany
wolfgang_haas@gmx.net

Submitted: Mar 4, 2008; Accepted: Apr 4, 2008; Published: Apr 18, 2008
Mathematics Subject Classification: 94B25, 94B65

Abstract

A central problem in coding theory is to determine $A_q(n, 2e+1)$, the maximal cardinality of a q-ary code of length n correcting up to e errors. When e is fixed and n is large, the best upper bound for $A(n, 2e+1)$ (the binary case) is the well-known Johnson bound from 1962. This however simply reduces to the sphere-packing bound if a Steiner system $S(e+1, 2e+1, n)$ exists. Despite the fact that no such system is known whenever $e \geq 5$, they possibly exist for a set of values for n with positive density. Therefore in these cases no non-trivial numerical upper bounds for $A(n, 2e+1)$ are known.

In this paper the author presents a technique for upper-bounding $A_q(n, 2e+1)$, which closes this gap in coding theory. The author extends his earlier work on the system of linear inequalities satisfied by the number of elements of certain codes lying in k-dimensional subspaces of the Hamming Space. The method suffices to give the first proof, that the difference between the sphere-packing bound and $A_q(n, 2e+1)$ approaches infinity with increasing n whenever q and $e \geq 2$ are fixed. A similar result holds for $K_q(n, R)$, the minimal cardinality of a q-ary code of length n and covering radius R. Moreover the author presents a new bound for $A(n, 3)$ giving for instance $A(19, 3) \leq 26168$.

1 Introduction

In the whole paper let q denote an integer greater than one and Q a set with $|Q| = q$. The Hamming distance $d(\lambda, \rho)$ between $\lambda = (x_1, \dots, x_n) \in Q^n$ and $\rho = (y_1, \dots, y_n) \in Q^n$ is defined by

$$d(\lambda, \rho) = |\{i \in \{1, \dots, n\} : x_i \neq y_i\}|.$$

Let $B_q(\lambda, e)$ denote the Hamming sphere with radius e centered on $\lambda \in Q^n$,

$$B_q(\lambda, e) = \{\rho \in Q^n : d(\rho, \lambda) \leq e\}.$$

We set

$$V_q(n, e) = |B_q(\lambda, e)| = \sum_{0 \leq i \leq e} \binom{n}{i} (q-1)^i$$

and

$$\overline{V}_q(n, e) = |\{\rho \in Q^n : d(\rho, \lambda) = e\}|$$

for any $\lambda \in Q^n$. Assume d and R are nonnegative integers. We say, that $C \subset Q^n$ has minimum distance at least d, if

$$\forall \lambda, \rho \in C \ (\lambda \neq \rho \Rightarrow d(\lambda, \rho) \geq d)$$

holds. $C \subset Q^n$ has covering radius at most R, if

$$\forall \rho \in Q^n \ \exists \lambda \in C \quad \text{with} \quad d(\rho, \lambda) \leq \mathrm{R}$$

holds. $A_q(n, d)$ denotes the maximal cardinality of a code $C \subset Q^n$ with minimal distance at least d. $K_q(n, R)$ denotes the minimal cardinality of a code $C \subset Q^n$ with covering radius at most R. In the binary case $q = 2$ the subscript usually is omitted.

$A_q(n, d)$ is the most important quantity in coding theory, since $A_q(n, 2e+1)$ is the maximal size of a q-ary code of length n correcting up to e errors.

Much work has been done in the last decades to give bounds for $A_q(n, d)$ and $K_q(n, R)$ (see [15], [3]). Updated internet tables are given by Brouwer [2] and Kéri [12]. Especially well-known are the sphere-packing bound

$$A_q(n, 2e+1) \leq \frac{q^n}{V_q(n, e)}$$

and the sphere-covering bound

$$K_q(n, R) \geq \frac{q^n}{V_q(n, R)}.$$

When n and e are comparatively small, the best upper bounds on $A_q(n, 2e+1)$ usually are obtained via optimization. The Linear Programming Bound (LP) was introduced by Delsarte in (1972) [4]. Recently Schrijver [18] introduced an upper bound for $A(n, d)$, which refines the classical bound of Delsarte and is computed via semidefinite programming. Even more recently, a new SDP bound for the nonbinary case was given in [5]. However, the computation of LP and SDP bounds is not tractable for large values of n.

In this case the best bound is the well-known Johnson bound [9] from 1962, which improves on the sphere-packing bound. In the binary case $q = 2$ a new bound was obtained by Mounits, Etzion and Litsyn [16], which always is at least as good as the Johnson bound. This bound however (like the Johnson bound) reduces to the sphere-packing bound iff a Steiner system $S(e+2, 2e+2, n+1)$ exists (see [15]). A Steiner system $S(t,k,v)$ is a collection of k-subsets (blocks) of a v-set S, such that every t-subset of S is contained in exactly one of the blocks. More information about Steiner systems can be found in every monograph on design theory, see for instance [1].

Despite the fact, that no system $S(e+2,2e+2,n+1)$ is known whenever $e \geq 4$, they possibly exist for a set of integers n of positive density when e is fixed (see [15]). Therefore in these cases no nontrivial numerical upper bounds for $A(n,2e+1)$ are known.

In this paper the author makes use of a third method for upper-bounding $A_q(n,2e+1)$, which closes this gap in coding theory. The author extends his earlier work [6] on the system of linear inequalities satisfied by the number of elements of a code with covering radius one lying in k-dimensional subspaces of Q^n. In this paper the author applies a corresponding system for error-correcting codes, which in full generality is due to Quistorff [17]. The method was introduced in the late 1960s and early 1970s by Kamps, van Lint [11] and Horten, Kalbfleisch, Stanton [10], [20]. It was used in several papers, mainly for lower-bounding $K_q(n,R)$, see for instance Haas [6], [7], Habsieger [8], Quistorff [17] or Lang, Quistorff, Schneider [13]. Most papers deal with bounded values of k. Like in [6] we present an approach, where k is unlimited with increasing n. The method is strong enough to give the first proof (to the authors best knowledge) of the following theorem.

Theorem 1. *Whenever q and $e \geq 2$ are fixed, then*

$$\frac{q^n}{V_q(n,e)} - A_q(n,2e+1) \to \infty \text{ for } n \to \infty.$$

Since it is well-known, that $V_q(n,e)$ divides q^n at most for a finite set of values for n when q and $e \geq 2$ are fixed (a consequence of a classical theorem of Siegel [19] on Diophantine approximation, see also [15]), Theorem 1 immediately follows from

Theorem 2. *If $V_q(n,e)$ does not divide q^n,*

$$n \geq \exp 96 \tag{1}$$

and

$$1 \leq e \leq \frac{\log n}{6(\log\log n + \log q)}, \tag{2}$$

then

$$A_q(n,2e+1) \leq \frac{q^n}{V_q(n,e)} - \frac{1}{2} q^{\frac{1}{6q}} n^{\frac{1}{2e}}.$$

The quantities $K_q(n,R)$ and $A_q(n,d)$ are connected by the well-known Lobstein-van Wee bound (see [14] and [21])

$$K_q(n,R) \geq \frac{q^n - A_q(n,2R+1)\binom{2R}{R}}{V_q(n,R) - \binom{2R}{R}} \tag{3}$$

whenever $n \geq 2R$, so that improved bounds on $A_q(n,2e+1)$ may lead to improved bounds on $K_q(n,R)$. Using (3), from Theorem 2 we derive

Theorem 3. *If $V_q(n,R)$ does not divide q^n,*

$$n \geq \exp 96$$

and

$$1 \leq R \leq \frac{\log n}{6(\log\log n + \log q)},$$

then

$$K_q(n,R) \geq \frac{q^n}{V_q(n,R)} + \frac{1}{2} q^{\frac{7}{48q} n^{\frac{1}{2R}}}.$$

From this we get

Theorem 4. *Whenever q and $R \geq 2$ are fixed, then*

$$K_q(n,R) - \frac{q^n}{V_q(n,R)} \to \infty \text{ for } n \to \infty.$$

In the binary case $q = 2$ and $e = 1$ we modify Theorem 3 in [7] to get a new upper bound for $A(n,3)$, which appears to be the best known in many cases, including the case $n = 4p - 1$ with a prime $p \geq 5$.

Theorem 5. *If $1 \leq k \leq \frac{n+1}{2}$, then*

$$A(n,3) \leq \left(2 \left\lceil \frac{2^{n-k}+k}{n+1} \right\rceil - 1 - \frac{s}{k} \right) 2^{k-1}$$

with

$$s = \min\left\{ \left\lceil \frac{2^{n-k}+k}{n+1} \right\rceil (n+1) - 2^{n-k} - k; k \right\}. \tag{4}$$

Applying Theorem 5 with $n = 19$, $k = 9$ and $n = 27$, $k = 13$ gives the following

Corollary 1.

$$\begin{aligned} A(19,3) &\leq 26168 \quad (26208\ [15]), \\ A(27,3) &\leq 4792950 \quad (4793472\ [16]). \end{aligned}$$

This paper is organized as follows. Section 2 contains some lemmas. In the sections 3, 4, 5 we prove the Theorems 2, 3, 5 respectively.

2 Some Lemmas

Lemma 1. *For $1 \leq e \leq n$ we have*

$$V_q(n,e) \leq (qn)^e.$$

Proof. Since $n-k \leq (e-k)(n-e+1)$ for $0 \leq k \leq e-1$, we get

$$\begin{aligned} V_q(n,e) &= \sum_{0\leq i\leq e} \binom{n}{i}(q-1)^i \leq \sum_{0\leq i\leq e} \binom{e}{i}(q-1)^i(n-e+1)^i \\ &= (1+(q-1)(n-e+1))^e \leq (qn)^e. \end{aligned}$$

□

Lemma 2. *For $1 \leq e \leq \frac{n}{2}$ we have*

$$V_q(n,e-1) \leq \frac{4e}{qn} V_q(n,e).$$

Proof. Since $q \geq 2$ and $\binom{n}{i+1}/\binom{n}{i} = (n-i)/(i+1) \geq (n-e+1)/e$ for $0 \leq i \leq e-1$, we get

$$\begin{aligned} V_q(n,e) &= \sum_{0\leq i\leq e} \binom{n}{i}(q-1)^i \\ &\geq \sum_{0\leq i\leq e-1} \binom{n}{i+1}(q-1)^{i+1} \\ &\geq \frac{(q-1)(n-e+1)}{e} V_q(n,e-1) \\ &\geq \frac{qn}{4e} V_q(n,e-1). \end{aligned}$$

□

The next Lemma generalizes Lemma 3 in [6]. Here $\|\xi\|$ means the difference from ξ to a nearest integer.

Lemma 3. *Let n, s, e be integers with $n \geq 3$, $1 \leq e \leq n$ and $3e\log n + 1 \leq s \leq n$. If $V_q(n,e)$ does not divide q^n, then there exists an integer k with $s - 3e\log n \leq k \leq s$ satisfying*

$$\left\| \frac{q^{n-k}}{V_q(n,e)} \right\| \geq \frac{1}{2q}. \tag{5}$$

Proof. Since $V_q(n,e)$ does not divide q^n, we get

$$\theta := \left\| \frac{q^{n-s}}{V_q(n,e)} \right\| > 0.$$

Let m be the smallest nonnegative integer satisfying $q^m\theta \geq 1/(2q)$. We have $q^m\theta \leq 1/2$, which is obvious if $m = 0$ and follows from the minimality of m otherwise. This implies

$$\left\| \frac{q^{n-k}}{V_q(n,e)} \right\| = \left\| q^m \frac{q^{n-s}}{V_q(n,e)} \right\| = \|q^m\theta\| = q^m\theta \geq \frac{1}{2q}$$

with $k := s - m$, proving (5). Lemma 1 implies

$$\frac{1}{(qn)^e} \leq \frac{1}{V_q(n,e)} \leq \theta \leq \frac{1}{2q^m}$$

and therefore

$$m \leq \frac{e\log(qn) - \log 2}{\log q} < e\left(1 + \frac{\log n}{\log q}\right) \leq 3e\log n,$$

which means $s - 3e\log n \leq k \leq s$. $\square$

Lemma 4. *Let k, r, e be integers with $1 \leq e \leq k$. Assume k_σ is an integer for each $\sigma \in Q^k$. If for every $\sigma \in Q^k$*

$$\min_{\substack{\mu \in Q^k \\ d(\mu,\sigma) \leq e}} k_\mu \leq r - (k_\sigma - r)V_q(k,e) \tag{6}$$

is satisfied, then we have

$$\sum_{\sigma \in Q^k} k_\sigma \leq rq^k.$$

Proof. By (6) there is a function f defined on Q^k, such that for each $\sigma \in Q^k$ the element $f(\sigma) = \mu \in Q^k$ satisfies $d(\mu, \sigma) \leq e$ and

$$k_\mu \leq r - (k_\sigma - r)V_q(k,e). \tag{7}$$

We set

$$\begin{aligned} A &= \{\sigma \in Q^k : k_\sigma > r\}, \\ B &= \{\mu \in Q^k : \exists \sigma \in A \text{ with } f(\sigma) = \mu\}. \end{aligned}$$

For $\mu \in B$ we have $k_\mu \leq r$ by (7) and thus A, B are disjoint. For $\mu \in B$ we set

$$A_\mu = \{\sigma \in A : f(\sigma) = \mu\} \cup \{\mu\}.$$

The sets $A_\mu, \mu \in B$ are pairwise disjoint. For $\mu \in B$ we have $A_\mu \cap A \neq \emptyset$. Thus for $\mu \in B$ we may fix $\sigma_\mu \in A_\mu \cap A$ with $k_{\sigma_\mu} = \max_{\sigma \in A_\mu \cap A} k_\sigma$. For $\mu \in B$

$$\begin{aligned} \sum_{\sigma \in A_\mu} k_\sigma &= \sum_{\sigma \in A_\mu \cap A} k_\sigma + k_\mu \\ &\leq |A_\mu \cap A| k_{\sigma_\mu} + r - (k_{\sigma_\mu} - r)V_q(k,e) \qquad \text{by (7)} \\ &\leq |A_\mu \cap A| k_{\sigma_\mu} + r - (k_{\sigma_\mu} - r)|A_\mu \cap A| \\ &= r(1 + |A_\mu \cap A|) \\ &= r|A_\mu|. \end{aligned}$$

By $A \subset \cup_{\mu \in B} A_\mu$ we have $k_\sigma \leq r$ for $\sigma \in Q^k - \bigcup_{\mu \in B} A_\mu$. Thus

$$\begin{aligned} \sum_{\sigma \in Q^k} k_\sigma &= \sum_{\mu \in B} \sum_{\sigma \in A_\mu} k_\sigma + \sum_{\sigma \in Q^k - \bigcup_{\mu \in B} A_\mu} k_\sigma \\ &\leq r \sum_{\mu \in B} |A_\mu| + r\Big(\sum_{\sigma \in Q^k} 1 - \sum_{\mu \in B} |A_\mu|\Big) \\ &= rq^k. \end{aligned}$$

$\square$

3 Proof of Theorem 2

Without proof we first state our main tool, Quistorff's system of linear inequalities. Assume $C \subset Q^n$. For $\sigma \in Q^k$, $1 \le k \le n$ we define

$$\begin{aligned} Q^n_\sigma &= \{(x_1, \dots, x_k, \dots, x_n) \in Q^n : (x_1, \dots, x_k) = \sigma\}, \\ k_\sigma &= |C \cap Q^n_\sigma|. \end{aligned} \tag{8}$$

Theorem 6 (Quistorff [17]). *Assume $1 \le e \le k < n$. If $C \subset Q^n$ has minimal distance at least $2e+1$, then for each $\sigma \in Q^k$ we have*

$$\sum_{0 \le i \le e} \sum_{\substack{\mu \in Q^k \\ d(\mu,\sigma)=i}} k_\mu V_q(n-k, e-i) \le q^{n-k}.$$

For the proof of Theorem 2 let $C \subset Q^n$ be a code with minimal distance at least $2e+1$ and $|C| = A_q(n, 2e+1)$. We set

$$s = \left\lfloor \frac{1}{4q} n^{\frac{1}{2e}} \right\rfloor .$$

By (1) and (2) we have $\log 4 \le \log \frac{1}{24} + \log\log n$ and $e \le \log n$. Thus

$$\begin{aligned} \log 4 + \log e + \log\log n &\le \log 4 + 2\log\log n \\ &\le \log \frac{1}{24} + 3\log\log n \\ &\le \log \frac{1}{24} - \log q + 3(\log\log n + \log q) \\ &\le \log \frac{1}{24} - \log q + \frac{1}{2e}\log n \quad \text{by (2).} \end{aligned}$$

Exponentiation yields

$$3e\log n + 1 \le 4e \log n \le \frac{1}{24q} n^{\frac{1}{2e}} \le \frac{1}{4q} n^{\frac{1}{2e}} - 1 \le s \le \frac{n}{2}. \tag{9}$$

We therefore may apply Lemma 3 and find an integer k in the interval $[s - 3e\log n, s]$, such that (5) is satisfied. By (9) we have

$$\begin{aligned} k - 1 &\ge s - 3e\log n - 1 \\ &\ge \frac{1}{4q} n^{\frac{1}{2e}} - 2(3e\log n + 1) \\ &\ge \frac{1}{6q} n^{\frac{1}{2e}} \end{aligned} \tag{10}$$

and

$$1 \le e \le k \le s \le \frac{n}{2}. \tag{11}$$

Moreover, since $(16e)^{1/(2e)}$ is decreasing for $e \geq 1$,

$$k \leq s \leq \frac{1}{4q} n^{\frac{1}{2e}} \leq \frac{1}{(16e)^{1/(2e)} q} n^{\frac{1}{2e}},$$

which by Lemma 1 implies

$$n \geq 16e(qk)^{2e} \geq 16eV_q^2(k,e). \tag{12}$$

We now set

$$r = \left\lfloor \frac{q^{n-k}}{V_q(n,e)} \right\rfloor .$$

From (5) follows

$$r + \frac{1}{2q} \leq \frac{q^{n-k}}{V_q(n,e)} \leq r + 1 - \frac{1}{2q}. \tag{13}$$

Now consider the numbers $k_\sigma, \sigma \in Q^k$ defined in (8). We fix $\sigma \in Q^k$ and set

$$N = \min_{\substack{\mu \in Q^k \\ d(\mu,\sigma) \leq e}} k_\mu \leq k_\sigma.$$

By (11) we may apply Theorem 6 to get

$$\begin{aligned}
q^{n-k} &\geq \sum_{0 \leq i \leq e} \sum_{\substack{\mu \in Q^k \\ d(\mu,\sigma)=i}} k_\mu V_q(n-k, e-i) \\
&\geq k_\sigma V_q(n-k,e) + N \sum_{1 \leq i \leq e} \overline{V}_q(k,i) V_q(n-k,e-i) \\
&= k_\sigma V_q(n,e) - (k_\sigma - N) \sum_{1 \leq i \leq e} \overline{V}_q(k,i) V_q(n-k,e-i) \\
&\geq k_\sigma V_q(n,e) - (k_\sigma - N) V_q(k,e) V_q(n,e-1) \\
&\geq k_\sigma V_q(n,e) - (k_\sigma - N) \frac{4e}{qn} V_q(k,e) V_q(n,e) \qquad \text{by Lemma 2} \\
&\geq k_\sigma V_q(n,e) - (k_\sigma - N) \frac{V_q(n,e)}{4qV_q(k,e)} \qquad \text{by (12)}
\end{aligned}$$

and thus

$$r + 1 - \frac{1}{2q} \geq \frac{q^{n-k}}{V_q(n,e)} \geq k_\sigma - \frac{k_\sigma - N}{4qV_q(k,e)}.$$

by (13). We now apply Lemma 4. Assume $k_\sigma > r$. Then

$$\frac{k_\sigma - r}{2q} \leq k_\sigma - r - 1 + \frac{1}{2q} \leq \frac{k_\sigma - N}{4qV_q(k,e)},$$

which is equivalent to

$$\begin{aligned}\min_{\substack{\mu\in Q^k\\ d(\mu,\sigma)\le e}} k_\mu = N &\le k_\sigma - 2(k_\sigma - r)V_q(k,e)\\ &= r + (k_\sigma - r) - 2(k_\sigma - r)V_q(k,e)\\ &\le r - (k_\sigma - r)V_q(k,e).\end{aligned}$$

Therefore the proposition (6) in Lemma 4 is satisfied for the numbers k_σ defined in (8) (the case $k_\sigma \le r$ is trivial). An application of Lemma 4 now yields

$$\begin{aligned}A_q(n,2e+1) = |C| &= \sum_{\sigma\in Q^k} k_\sigma\\ &\le rq^k\\ &\le \left(\frac{q^{n-k}}{V_q(n,e)} - \frac{1}{2q}\right)q^k \qquad \text{by (13)}\\ &= \frac{q^n}{V_q(n,e)} - \frac{1}{2}q^{k-1}\\ &\le \frac{q^n}{V_q(n,e)} - \frac{1}{2}q^{\frac{1}{6q}n^{\frac{1}{2e}}} \qquad \text{by (10),}\end{aligned}$$

completing the proof of Theorem 2.

4 Proof of Theorem 3

The propositions of Theorem 2 are satisfied for $e = R$ and we get

$$A_q(n,2R+1) \le \frac{q^n}{V_q(n,R)} - \frac{1}{2}q^{\frac{1}{6q}n^{\frac{1}{2R}}}.$$

This inserted in (3) yields

$$K_q(n,R) \ge \frac{q^n}{V_q(n,R)} + \frac{q^{\frac{1}{6q}n^{\frac{1}{2R}}}}{2V_q(n,R)}.$$

By Lemma 1 we have

$$\begin{aligned}V_q(n,R) &\le (qn)^R\\ &= \exp(R\log qn)\\ &\le \exp(2R\log q\log n)\\ &\le \exp\left(\frac{1}{48q}n^{\frac{1}{2R}}\log q\right) \qquad \text{by (9) (with } e=R)\\ &= q^{\frac{1}{48q}n^{\frac{1}{2R}}}\end{aligned}$$

and Theorem 3 follows.

5 Proof of Theorem 5

Let $\mathbf{F} = \{0, 1\}$ denote the finite field with two elements. We start with

Lemma 5. *Let k, l, r and s be integers with $1 \le k \le l$ and $0 \le s \le k$. Assume the integers x_σ, $\sigma \in \boldsymbol{F}^k$ satisfy*

$$lx_\sigma + \sum_{\mu \in \boldsymbol{F}^k, d(\mu,\sigma)=1} x_\mu \le l(r+1) + kr - s \tag{14}$$

for each $\sigma \in \boldsymbol{F}^k$. Then

$$\sum_{\sigma \in \boldsymbol{F}^k} x_\sigma \le \left(2r + 1 - \frac{s}{k}\right) 2^{k-1}. \tag{15}$$

Proof. Put

$$B = \{\sigma \in \mathbf{F}^k : x_\sigma > r\}, \quad N = |B|.$$

For $\sigma \in \mathbf{F}^k$, $1 \le i \le k$ and $0 \le j \le 2$ we define

$$\begin{aligned}
L(\sigma, i) &= \{\mu \in \mathbf{F}^k : \mu \text{ and } \sigma \text{ differ at most in the } i\text{th coordinate}\}, \\
\mathcal{L} &= \{L(\sigma, i) : \sigma \in \mathbf{F}^k,\ 1 \le i \le k\}, \\
\mathcal{L}_j &= \{L \in \mathcal{L} : |L \cap B| = j\}, \\
y_j &= |\mathcal{L}_j|.
\end{aligned}$$

One easily gets $|L| = 2$ for $L \in \mathcal{L}$ and $|\mathcal{L}| = k2^{k-1}$. Thus we have

$$k2^{k-1} = |\mathcal{L}| = y_0 + y_1 + y_2. \tag{16}$$

Moreover for each $\sigma \in \mathbf{F}^k$

$$\sum_{L \in \mathcal{L}, \sigma \in L} 1 = k. \tag{17}$$

Finally we define a function g on $\mathcal{L}$ by

$$g(L) = \sum_{\mu \in L} x_\mu - (2r+1) \qquad \text{for } L \in \mathcal{L}. \tag{18}$$

We have

$$\begin{aligned}
\sum_{L \in \mathcal{L}} g(L) &= \sum_{0 \le j \le 2} \sum_{L \in \mathcal{L}_j} g(L) \qquad (19) \\
&= \frac{1}{2} \sum_{1 \le j \le 2} j \sum_{L \in \mathcal{L}_j} g(L) + \frac{1}{2} \sum_{L \in \mathcal{L}_1} g(L) + \sum_{L \in \mathcal{L}_0} g(L) \\
&= \frac{1}{2} \sum_{\sigma \in B} \sum_{L \in \mathcal{L}, \sigma \in L} g(L) + \frac{1}{2} \sum_{L \in \mathcal{L}_1} g(L) + \sum_{L \in \mathcal{L}_0} g(L),
\end{aligned}$$

because in the sum $\sum_{\sigma\in B}\sum_{L\in\mathcal{L},\sigma\in L} g(L)$ every $g(L)$ with $L\in\mathcal{L}$ and $|L\cap B|=j$ ($j\in\{1,2\}$) is counted exactly j times. We now estimate the sums occurring at the right-hand side of (19). If $L\in\mathcal{L}_0$ we have $g(L)\leq 2r-(2r+1)=-1$ and thus

$$\sum_{L\in\mathcal{L}_0} g(L)\leq -y_0. \tag{20}$$

If $\sigma\in B$ then

$$\begin{aligned}
\sum_{L\in\mathcal{L},\sigma\in L} g(L) &= \sum_{L\in\mathcal{L},\sigma\in L}\sum_{\mu\in L} x_\mu-(2r+1)k \quad \text{by (17) and (18)}\\
&= kx_\sigma+\sum_{\mu\in\mathbf{F}^k,d(\mu,\sigma)=1} x_\mu-(2r+1)k\\
&= lx_\sigma+\sum_{\mu\in\mathbf{F}^k,d(\mu,\sigma)=1} x_\mu-(l-k)x_\sigma-(2r+1)k\\
&\leq l(r+1)+kr-s-(l-k)(r+1)-(2r+1)k\\
&\quad\ \text{by (14), } l\geq k \text{ and } x_\sigma\geq r+1 \text{ for } \sigma\in B\\
&= -s
\end{aligned}$$

implying

$$\sum_{\sigma\in B}\sum_{L\in\mathcal{L},\sigma\in L} g(L)\leq -Ns. \tag{21}$$

Furthermore, if $\sigma\in B$ and $L\in\mathcal{L}\setminus\mathcal{L}_1$ with $\sigma\in L$, then $L\in\mathcal{L}_2$ implying $g(L)>0$. Thus

$$\sum_{L\in\mathcal{L}_1} g(L)=\sum_{\sigma\in B}\sum_{L\in\mathcal{L}_1,\sigma\in L} g(L)\leq\sum_{\sigma\in B}\sum_{L\in\mathcal{L},\sigma\in L} g(L)\leq -Ns$$

by (21). Inserting this, (20) and (21) in (19) we get

$$\sum_{L\in\mathcal{L}} g(L)\leq -Ns-y_0.$$

Moreover by (17)

$$kN=\sum_{\sigma\in B}\sum_{L\in\mathcal{L},\sigma\in L} 1=y_1+2y_2.$$

Thus by (16) and $0\leq s\leq k$

$$\sum_{L\in\mathcal{L}} g(L)\leq -\frac{kNs}{k}-y_0=-y_0-\frac{s}{k}y_1-\frac{2s}{k}y_2\leq -\frac{s}{k}(y_0+y_1+y_2)=-s2^{k-1}.$$

By (16) we now have

$$\begin{aligned} k \sum_{\sigma \in \mathbf{F}^k} x_\sigma &= \sum_{L \in \mathcal{L}} \sum_{\sigma \in L} x_\sigma \\ &= \sum_{L \in \mathcal{L}} (g(L) + 2r + 1) \\ &= \sum_{L \in \mathcal{L}} g(L) + (2r+1)k2^{k-1} \\ &\leq -s2^{k-1} + (2r+1)k2^{k-1} \end{aligned}$$

and (15) follows. □

Proof of Theorem 5. Assume $C \subset \mathbf{F}^n$ is a binary code of length n with minimal distance at least three and $|C| = A(n,3)$. By Theorem 6 the numbers k_σ, $\sigma \in \mathbf{F}^k$ defined in (8) satisfy

$$(n-k+1)k_\sigma + \sum_{\mu \in \mathbf{F}^k, d(\mu,\sigma)=1} k_\mu \leq 2^{n-k}.$$

We now apply Lemma 5. An easy calculation shows, that (14) is satisfied for the integers k_σ, $\sigma \in \mathbf{F}^k$ with $l = n-k+1$,

$$r = \left\lceil \frac{2^{n-k}+k}{n+1} \right\rceil - 1$$

and s defined in (4). $k \leq l$ holds by $k \leq \frac{n+1}{2}$. Now by (15) we have

$$A(n,3) = |C| = \sum_{\sigma \in \mathbf{F}^k} k_\sigma \leq \left(2 \left\lceil \frac{2^{n-k}+k}{n+1} \right\rceil - 1 - \frac{s}{k} \right) 2^{k-1}.$$

□

Acknowledgement

I wish to thank Jörn Quistorff (Berlin), who informed me on his important system of linear inequalities for error-correcting codes [17], and Laurent Habsieger (Lyon), whose fine paper [8] inspired me to the present work. I am also grateful to anonymous referees for valuable remarks concerning the history of the problem and technical improvements as well as simplifications for section 2.

References

[1] T. Beth, D. Jungnickel, H. Lenz, *Design Theory*, Cambridge University Press, 1999, 2nd edition.

[2] A. Brouwer, *Tables of general binary codes*, http://www.win.tue.nl/∼aeb/codes/binary-1.html.

[3] G. Cohen, I.S. Honkala, S. Litsyn, A. Lobstein*, Covering codes,* North Holland Mathematical Library, vol 54, 1997, Elsevier.

[4] Ph. Delsarte, *Bounds for unrestricted codes, by linear programming*, Philips Res. Repts. **27** (1972), 272-289.

[5] D. Gijswijt, A. Schrijver, H. tanaka*, New upper bounds for nonbinary codes based on the Terwilliger algebra and semidefinite programming*, J. Comb. Theory, Ser. A **113** (8) (2006), 1719-1731.

[6] W. Haas*, Lower bounds for q-ary codes of covering radius one,* Discr. Mathematics **219** (2000), 97-106.

[7] W. Haas*, Binary and ternary codes with covering radius one: Some new lower bounds,* Discr. Mathematics **256** (2002), 161-178.

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

[9] S. M. Johnson*, A new upper bound for error-correcting codes*, IEEE Trans. Inform. Th. **8** (1962), 203-207.

[10] J. G. Kalbfleisch, R. G. Stanton, J. D. Horten*, On covering sets and error-correcting codes* , J. Comb. Theory **11** (1971), 233-250.

[11] H. J. L. Kamps, J. H. van Lint*, The football pool problem for 5 matches* , J. Comb. Theory **3** (1967), 315-325.

[12] G. Kéri, *Tables for Covering Codes*, http://www.sztaki.hu/∼ keri/codes/.

[13] W. Lang, J. Quistorff, E. Schneider*, New Results on Integer Programming for Codes*, Cong. Numer. **188** (2007), 97-107.

[14] A. C. Lobstein*, Contributions au codage combinatoire; ordres additifs, rayon de recouvrements, Thesè*, Télékom, France, (1985), 163 pp.

[15] F.J. MacWilliams, N.J.A. Sloane*, The Theory of Error-Correcting Codes,* Amsterdam, North-Holland, 1977.

[16] B. Mounits, T. Etzion, S. Litsyn*, Improved Upper Bounds on Sizes of Codes*, IEEE Trans. Inform. Th. **48** (2002), 880-886.

[17] J. Quistorff*, Improved Sphere Bounds in Finite Metric Spaces*, Bull. of the ICA **46** (2006), 69-80.

[18] A. Schrijver*, New code upper bounds from the Terwilliger algebra and semidefinite programming*, IEEE Trans. Inform. Th. **51** (2005), 2859-2866.

[19] C. L. Siegel*, Approximation algebraischer Zahlen*, Math. Zeit. **10** (1921), 173-213.

[20] R. G. Stanton, J. G. Kalbfleisch*, Intersection inequalities for the covering problem*, SIAM J. Appl. Math. **17** (1969), 1311-1316.

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