Discrete Mathematics 309 (2009) 3318–3322

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

A remark on Haas' method

Alain Plagne

Centre de Mathématiques Laurent Schwartz, UMR 7640 du CNRS, École polytechnique, 91128 Palaiseau Cedex, France

ARTICLE INFO

Article history:
Received 11 February 2008
Received in revised form 2 August 2008
Accepted 19 September 2008
Available online 18 November 2008

Keywords:
Covering codes

ABSTRACT

We introduce a refinement in the method proposed some time ago by Haas for obtaining new lower bounds for the cardinality of codes with covering radius 1. As an application, we show that the minimal cardinality of a binary code in dimension 27 with covering radius 1 is at least $K_2(27, 1) \geq 4\,794\,174$.

© 2008 Elsevier B.V. All rights reserved.

1. Introduction

Let $\mathcal{A}^n$ be the nth power of a finite alphabet $\mathcal{A}$ with two elements, equipped with the Hamming distance d. Recall that the covering radius R of a code $\mathcal{C}$ defined on $\mathcal{A}^n$ is

$$R = \min\{r \geq 0 \text{ such that } \cup_{c\in\mathcal{C}} \mathcal{B}_r(c) = \mathcal{A}^n\},$$

where $\mathcal{B}_r(c)$ denotes the ball centered in c with radius r. In what follows, we restrict ourselves to the case $R = 1$. We denote by $K_2(n, 1)$ the minimal cardinality of a code with covering radius 1 on $\mathcal{A}^n$ (it is not required that such a covering code with minimal cardinality be linear but in some specific situations, this may well happen).

Establishing good estimates on this function is the simplest (binary, $R = 1$) case of the basic problem of the theory of covering codes. Up to now, only very few exact values of $K_2(n, 1)$ are known. Indeed, such exact values are known only for small dimensions n (namely $n \leq 9$, the case $n = 9$ using heavy computational means [5]) and for some n having a special arithmetic property (like, for instance, being a power of 2). In general, only upper and lower bounds have been achieved. The reader is referred to the book [1], to read a complete account on the whole theory of covering codes. By now, the bounds contained in the tables of this book have been in general largely improved. An up-to-date table [4] is available on the website maintained by G. Kéri. It contains, in particular, bounds in the cases of interest of this paper.

In 2002, Haas proposed a method [2] which, in particular, can be used to obtain good lower bounds on the function $K_2(n, 1)$. Haas' method builds on the classical method of linear inequalities of a code. Loosely speaking, a parameter k is introduced and $\mathcal{A}^n$ is partitioned into 2^k parallel $(n - k)$-dimensional subspaces. Then the distribution of the number of elements of the code in each subspace of the partition is studied (cf. the quantity n_σ below) and a general bound $l(k, s)$ is obtained (this is Theorem 2 in the above-quoted paper) depending on this parameter k and yet another integral parameter s. Finally the parameters k and s have to be chosen so as to obtain a lower bound on $K_2(n, 1)$ which is as good as possible. Although it is not clear how the parameters should be chosen so as to maximize $l(k, s)$ numerically, it is always possible to do so since there is only a finite number of possible choices. It has been observed experimentally by Haas that the choice $k = [(n - 1)/2]$ always led to the largest possible numerical value of $l(k, s)$. Unfortunately, however, the choice of the parameters k and s is not completely free since some restrictions apply in order to make the bound valid. In particular, a numerical condition (this is condition (15) in Haas' Theorem 2) has to be checked to ensure that some remaining term

E-mail address: plagne@math.polytechnique.fr.

0012-365X/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2008.09.042

is positive (strictly speaking, this term is hidden in Haas' Theorem). As stated in the first paragraph of Section 3 of [2], this condition does not seem very natural and sometimes prevents from making an optimal choice of the parameters, in the above sense. In his paper [2], Haas underlines in particular the case $n = 27$ where the potentially optimal choice of parameters is not allowed, due to the above-mentioned numerical constraint. Making a "suboptimal" but allowed choice only leads to the lower bound

$$K_2(27, 1) \geq 4\,793\,959$$

while the forbidden choice of parameters would yield 4 794 248 instead.

Roughly speaking, the goal of this article is to show that it is always possible to make an optimal choice of parameters. Indeed, following closely Haas' method, it is possible to make it precise enough to obtain an explicit form for the remaining term. Even when this term is not positive (that is, in the cases when Haas' theorem is not available), it is possible to control its size and thus optimize Haas' approach. The price to be paid, however, is that the bound derived is slightly less good than what was to be expected if there would be no remaining term (that is, if Haas' Theorem 2 was valid with no restriction) since a small negative contribution must be added. Nevertheless, when this negative contribution is not too large, a good bound (at least, better than the one obtained with a suboptimal choice of parameters) can still be obtained.

As an application, we consider the case $n = 27$, which is indeed the only case listed in Haas' paper where an optimal choice (in the above sense) of parameters is not allowed. As reported in [4] (at the end of 2007), the best that is known in this case is

$$4\,793\,959 \leq K_2(27, 1) \leq 5\,767\,168.$$

The upper bound is due to Östergård and Kaikkonen [6] while the lower bound follows from [2]. Our present result implies

$$K_2(27, 1) \geq 4\,794\,174. \tag{1}$$

As explained earlier, it is not as good as the conjectural value 4 794 248, which is the best possible value obtainable by Haas' method, but it is better than the previous best lower bound (which followed from a suboptimal choice of parameters). As almost always in this area of research, the improvement is modest. Nevertheless, it is a positive sign that the methods are still in progress.

We now give some notation. In what follows, we consider a fixed binary code $\mathcal{C}$ in $\mathcal{A}^n$ (n a positive integer) with covering radius $R = 1$.

We first choose several integers that will be considered as fixed from now on. Let $1 \leq k \leq n$ and r be two such fixed positive integers.

For any $\sigma \in \mathcal{A}^k$, we define

$$n_\sigma = |\{c \in \mathcal{C} : (c_1, \ldots, c_k) = \sigma\}|$$

that is, the number of codewords having σ as its beginning. For any (possibly negative) integer $i \leq r$, we put

$$W_i = \{\sigma \in \mathcal{A}^k : n_\sigma = r - i\}$$

and

$$N_i = |W_i|.$$

For any integer $\varepsilon \leq r$, we define

$$W^{(\varepsilon)} = \{\sigma \in \mathcal{A}^k : n_\sigma \leq r - \varepsilon\} = \bigcup_{i=\varepsilon}^{r} W_i.$$

We denote by $\mathcal{S}(x)$ the sphere of radius 1 centered in x (the space in which the sphere is to be considered is clearly the one where x lives).

Here is our main result.

Theorem. *Let n be a positive integer. Let k, r and s be three positive integers satisfying the inequalities $1 \leq k \leq n$ and*

$$s \leq 2^{n-k} - (n + 1)r.$$

If $\mathcal{C}$ is a code with covering radius 1 in $\mathcal{A}^n$ then

$$|\mathcal{C}| \geq \left(r + \frac{s}{s+k}\right) 2^k + \frac{1}{s+k} \sum_{i=1}^{r} \left(\left(\frac{s(n-k+1)}{k} + n + 1 - s - 2k\right) \mathrm{i} + \frac{s(s-k)}{k}\right) N_i.$$

Here, similarly as in Haas' theorem, the lower bound depends on a dimensional parameter k and Haas' parameter s. A third parameter r which can be seen as a "reference" value for the number of codewords belonging to a given intervening $(n - k)$-dimensional subspace enters the picture. (See the last paragraph of Section 3 for an empirical discussion on how these parameters can be chosen).

The proof of this theorem will be given in Section 2. For the reader's convenience, we shall give a self-contained account of the argument (trying to follow the main lines of [2]), using only well-known inequalities.

In Section 3, we show how the lower bound (1) can be derived from this theorem.

In Section 4, we discuss a possible improvement of the method.

2. Proof of the theorem

Again, a code $\mathcal{C}$ in $\mathcal{A}^n$ with covering radius $R = 1$ and the integers k, r and s subject to the restrictions given in the theorem are considered as fixed.

We shall use the following two equalities which follow by definition. This first one, namely

$$\sum_{i\leq r} N_i = 2^k, \tag{2}$$

is immediate (here and in what follows, seemingly infinite sums always contain in fact a finite number of non-zero terms and are therefore well defined) while the second one

$$|\mathcal{C}| = r2^k - \sum_{i\leq r} iN_i \tag{3}$$

follows from the following simple counting argument

$$\sum_{i\leq r} iN_i = \sum_{i\leq r} i|\{\sigma \in \mathcal{A}^k : n_\sigma = r - i\}| = \sum_{\sigma\in\mathcal{A}^k} (r - n_\sigma) = r2^k - \sum_{\sigma\in\mathcal{A}^k} n_\sigma = r2^k - |\mathcal{C}|.$$

Moreover, as shown by Habsieger [3], the projection of the sphere covering bound yields (this is for instance Lemma 1 in [2]), for any $\mu \in \mathcal{A}^k$,

$$\sum_{\sigma\in\mathcal{S}(\mu)} n_\sigma \geq 2^{n-k} - (n - k + 1)n_\mu. \tag{4}$$

Here is now a lemma which contains several computations included in Haas' argument.

Lemma. *Let $\varepsilon = 0$ or 1. We have*

$$k\sum_{j=1}^{+\infty}(j-\varepsilon)N_{-j} \geq (s - \varepsilon k)\sum_{i=\varepsilon}^{r} N_i + (n - k + 1)\sum_{i=\varepsilon}^{r} iN_i.$$

Proof of the Lemma. We have the following chain of computations

$$\begin{aligned}
k\sum_{j=1}^{+\infty}(j-\varepsilon)N_{-j} &= k\left(\sum_{j=1}^{+\infty}\sum_{\sigma\in W_{-j}}(j-\varepsilon) + \sum_{j\leq 0}\sum_{\sigma\in W_{-j}} 0\right)\\
&= k\sum_{\sigma\in\mathcal{A}^k}\max(n_\sigma - r - \varepsilon, 0)\\
&= \sum_{\sigma\in\mathcal{A}^k}\max(n_\sigma - r - \varepsilon, 0)|\mathcal{S}(\sigma)|\\
&\geq \sum_{\sigma\in\mathcal{A}^k}\max(n_\sigma - r - \varepsilon, 0)|\mathcal{S}(\sigma)\cap W^{(\varepsilon)}|\\
&= \sum_{\sigma,\mu\in\mathcal{A}^k,\ n_\mu\leq r-\varepsilon,\ \mathrm{d}(\sigma,\mu)=1}\max(n_\sigma - r - \varepsilon, 0)\\
&= \sum_{\mu\in\mathcal{A}^k,\ n_\mu\leq r-\varepsilon}\ \sum_{\sigma\in\mathcal{S}(\mu)}\max(n_\sigma - r - \varepsilon, 0)\\
&\geq \sum_{\mu\in\mathcal{A}^k,\ n_\mu\leq r-\varepsilon}\ \sum_{\sigma\in\mathcal{S}(\mu)}(n_\sigma - r - \varepsilon)\\
&= \sum_{\mu\in W^{(\varepsilon)}}\left(\left(\sum_{\sigma\in\mathcal{S}(\mu)} n_\sigma\right) - k(r+\varepsilon)\right).
\end{aligned}$$

Using (4) we then derive

$$\begin{aligned} k\sum_{j=1}^{+\infty}(j-\varepsilon)N_{-j} &\geq \sum_{\mu\in W^{(\varepsilon)}}\left(2^{n-k}-(n-k+1)n_\mu-k(r+\varepsilon)\right)\\ &= \sum_{i=\varepsilon}^{r}\left(2^{n-k}-(n-k+1)(r-i)-k(r+\varepsilon)\right)N_i\\ &= (2^{n-k}-(n+1)r-\varepsilon k)\sum_{i=\varepsilon}^{r}N_i+(n-k+1)\sum_{i=\varepsilon}^{r}\mathrm{i}N_i. \end{aligned}$$

By definition of s, the result follows. □

Applying the lemma with $\varepsilon = 0$ and using (2) gives

$$k\sum_{j=1}^{+\infty}jN_{-j}\geq s\left(2^k-\sum_{j=1}^{+\infty}N_{-j}\right)+(n-k+1)\sum_{i=0}^{r}\mathrm{i}N_i.$$

It follows

$$\begin{aligned} s2^k &\leq k\sum_{j=1}^{+\infty}jN_{-j}+s\sum_{j=1}^{+\infty}N_{-j}-(n-k+1)\sum_{i=1}^{r}\mathrm{i}N_i\\ &= (s+k)\left(\sum_{j=1}^{+\infty}jN_{-j}-\sum_{i=1}^{r}\mathrm{i}N_i\right)-s\sum_{j=1}^{+\infty}(j-1)N_{-j}+(s+2k-n-1)\sum_{i=1}^{r}\mathrm{i}N_i \end{aligned}$$

and using (3)

$$s2^k\leq(s+k)\left(|\mathcal{C}|-r2^k\right)-s\sum_{j=1}^{+\infty}(j-1)N_{-j}+(s+2k-n-1)\sum_{i=1}^{r}\mathrm{i}N_i. \tag{5}$$

We now apply again the lemma but with the value $\varepsilon = 1$. We obtain

$$k\sum_{j=1}^{+\infty}(j-1)N_{-j}\geq(s-k)\sum_{i=1}^{r}N_i+(n-k+1)\sum_{i=1}^{r}\mathrm{i}N_i. \tag{6}$$

Injecting (6) in (5) yields

$$s2^k\leq(s+k)\left(|\mathcal{C}|-r2^k\right)-\frac{s}{k}\left((s-k)\sum_{i=1}^{r}N_i+(n-k+1)\sum_{i=1}^{r}\mathrm{i}N_i\right)+(s+2k-n-1)\sum_{i=1}^{r}\mathrm{i}N_i$$

which is equivalent to the inequality proposed in the statement of the theorem.

3. Proof of the lower bound (1)

Let $n = 27$. We choose the following parameters $k = 13$, $r = 585$, $s = 4$ and check that $s = 2^{n-k} - (n+1)r$.
Let $\mathcal{C}$ be a code with covering radius 1. By the theorem, we have

$$|\mathcal{C}|\geq\left(585+\frac{4}{17}\right)2^{13}+\frac{1}{221}\sum_{i=1}^{r}(34\mathrm{i}-36)N_i\geq\left(585+\frac{4}{17}\right)2^{13}-\frac{2}{221}N_1.$$

Since $N_1 \leq 2^k$, it follows that

$$|\mathcal{C}|\geq\left(585+\frac{4}{17}-\frac{2}{221}\right)2^{13}=4\,794\,173+\frac{87}{221}$$

that is

$$|\mathcal{C}|\geq 4\,794\,174$$

as announced.

The parameters used here can be easily determined in an experimental fashion since there is only a finite number of possible sets of values to check. However, it is noticeable that, as in Haas' article, k is taken equal to $(n-1)/2$. On the more, the value of r appears to be some kind of mean value since

$$r = \left[\frac{2^{n-k}}{n+1}\right].$$

(Recall that the sphere covering bound yields $|\mathcal{C}| \geq 2^n/(n+1)$ and that the method uses a partition of the Hamming space into 2^k parallel $(n-k)$-dimensional spaces). Finally s is chosen as large as possible subject to the numerical constraint it has to satisfy: this can be understood as being the choice which maximizes the main term, namely $(r + s/(s+k))2^k$ in our theorem.

4. A final remark

Having in mind the shape of the inequality of our theorem, it is clear that a better knowledge on the distribution of the N_i's would certainly be very useful.

For instance, in our proof of a lower bound for $K_2(27, 1)$ we have used the trivial $N_1 \leq 8192$. A better upper bound for N_1 would lead to a better lower bound for $K_2(27, 1)$.

Another, maybe more important remark, is that a precise knowledge of the N_i's would make the present method usable in a much more general context. Indeed, very often, the additional contribution of our theorem compared to Haas' Theorem 2 is positive because it is a weighted sum of N_i's with positive weights. If something is known on the N_i's then a lower bound for the additional contribution can be derived which in turn implies an improvement of the lower bound on $K_2(n, 1)$.

It is likely that precise information on the distribution of the N_i's is rather difficult to obtain. However, either the N_i's have good properties with respect to the present discussion and we may improve the method, or this is not the case, but in this case this fact might be reinjected into another argument which in turn may lead to another good lower bound.

References

[1] G. Cohen, I. Honkala, S. Litsyn, A. Lobstein, Covering Codes, North-Holland, 1997.
[2] W. Haas, Binary and ternary codes of covering radius one: Some new lower bounds, Discrete Math. 256 (2002) 161–178.
[3] L. Habsieger, Lower bounds for q-ary coverings by spheres of radius one, J. Combin. Theory Ser. A 67 (1994) 199–222.
[4] G. Kéri, Bounds for binary covering codes, listed for $n \leq 33$, $R \leq 10$, available at http://www.sztaki.hu/~keri/codes/2_tables.pdf.
[5] P.R.J. Östergård, U. Blass, On the size of optimal binary codes of length 9 and covering radius 1, IEEE Trans. Inform. Theory 47 (2001) 2556–2557.
[6] P.R.J. Östergård, M.K. Kaikkonen, New upper bounds for binary covering codes, Discrete Math. 178 (1998) 165–179.