Covering codes with improved density

Michael Krivelevich , Benny Sudakov, and Van H. Vu

***Abstract*— We prove a general recursive inequality concerning $\mu^*(R)$, the asymptotic (worst) density of the best binary covering codes of radius R. In particular, this inequality implies that $\mu^*(R) \le e \cdot (R\log R + \log R + \log\log R + 2)$, which significantly improves the best known density $2^R R^R(R+1)/R!$. Our inequality also holds for covering codes over arbitrary alphabets.**

***Index Terms*— Covering codes, density, probabilistic methods.**

I. Introduction

Denote by $\mathbb{F}_2^n$ the set of all $(0,1)$ strings of length n. A subset K of $\mathbb{F}_2^n$ is a *covering code of radius* R if for every element $y \in \mathbb{F}_2^n$, there is an element $x \in K$ such that the Hamming distance between x and y is at most R. It is common to view $\mathbb{F}_2^n$ as the set of vertices of the n dimensional unit hypercube. From this point of view, K is a covering code of radius R if the Hamming balls with radius R centered at the elements of K cover all the vertices of the hypercube. Covering codes is a central object in Coding Theory and for more information we refer to a monograph [1], by Cohen, Honkala, Litsyn and Lobstein.

For any vertex $x \in \mathbb{F}_2^n$, the Hamming ball with radius R centered at x contains exactly $V(n,R) = \sum_{i=0}^{R}\binom{n}{i}$ vertices of the cube. Therefore,

$$|K| \ge \frac{2^n}{V(n,R)}.$$

The quantity $|K|/\frac{2^n}{V(n,R)}$ is called the density of K. Denote by $\mu(n,R)$ the minimal density of a covering code of radius R in $\mathbb{F}_2^n$. Define

$$\mu^*(R) = \limsup_{n\to\infty} \mu(n,R),$$

the asymptotic (worst) density for the best covering of a given radius. This quantity plays a central role in the theory of covering codes. From the definition, it is clear that for any fixed R, $\mu^*(R) \ge 1$. One of the fundamental problems in Coding Theory is to settle the following conjecture ([1], Chapter 12)

Conjecture 1.1: For any fixed R, $\mu^*(R) = 1$.

The conjecture has been confirmed for $R = 1$, but is open for all other cases. For a generic R, it seems very hard. The best upper bound on $\mu^*(R)$ for a general R that we know is ([1], Theorem 12.4.3)

$$\mu^*(R) \le \frac{2^R R^R (R+1)}{R!}. \tag{1}$$

By Stirling's formula, for large R the right hand side in (1) is approximately $(2e)^R\sqrt{R/2\pi}$, where e is the base of natural logarithm. In this paper, we shall significantly improve upon this bound. Our main result is the following recursive inequality

Theorem 1.2: Given a pair of positive integers $R > R_1 \ge 1$,

$$\mu^*(R) \le \frac{y^{R_1}(\frac{y}{y-1})^{R-R_1}\binom{R}{R_1}^{-1}x}{1-e^{-x}y^R}\mu^*(R_1), \tag{2}$$

holds for any pair of positive constants x and y satisfying $y > 1$ and $1 - e^{-x}y^R > 0$.

With a particular choice of R_1, y and x, we can derive

Corollary 1.3: For $R \ge 2$, $\mu^*(R) \le e(x_0+1)$, where x_0 is the largest root of the equation $e^x = (x+1)R^R$.

Proof: Choosing $R_1 = 1$, we have

$$\mu^*(R) \le \frac{y(\frac{y}{y-1})^{R-1}\frac{x}{R}}{1-e^{-x}y^R} \tag{3}$$

Next, set $y = R$ and notice that $(\frac{R}{R-1})^{R-1} \le e$. Then (3) yields

$$\mu^*(R) \le \frac{ex}{1-e^{-x}R^R},$$

We now optimize $f(x) = \frac{ex}{1-e^{-x}R^R}$ over x. The derivative of $f(x)$ is $e\Big(\frac{1-(x+1)e^{-x}R^R}{(1-e^{-x}R^R)^2}\Big)$. Conditioned on $1 - e^{-x}R^R > 0$, $f(x)$ reaches it minimum at the larger root x_0 of the equation $1-(x+1)e^{-x}R^R = 0$ (it is easy to check that this equation has two roots). By definition, $e^{-x_0}R^R = \frac{1}{x_0+1}$ and by substituting this in the formula of $f(x)$ we have $f(x_0) = e(x_0+1)$. □

It is easy to see that for $R \ge 3$, $x_0 \le R\log R + \log R + \log\log R + 1$, so we have the following inequality, which improves the exponential function in the right hand side of (1) to an almost linear function. Here and later the logarithms have natural base.

Corollary 1.4: For all $R \ge 3$,

$$\mu^*(R) \le e(R\log R + \log R + \log\log R + 2).$$

In practice, one might be able obtain a good bound for $\mu^*(R)$ where R belongs to a special sequence S. In such a

M. Krivelevich is with the Department of Mathematics, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv 69978, Israel (e-mail: krivelev@post.tau.ac.il). His research was supported in part by a USA-Israel BSF Grant, by a grant from the Israel Science Foundation and by a Bergmann Memorial Grant.

B. Sudakov is with the Department of Mathematics, Princeton University, Princeton, NJ 08540, USA and with the Institute for Advanced Study, Princeton, NJ 08540, USA (e-mail: bsudakov@math.princeton.edu). His research was supported in part by NSF grants DMS-0106589, CCR-9987845 and by the State of New Jersey.

V. H. Vu is with the Department of Mathematics, UCSD, La Jolla, CA 92093, USA (e-mail:vanvu@ucsd.edu). His research was supported in part by grant RB091G-VU from UCSD, by NSF grant DMS-0200357 and by an A. Sloan fellowship.

case, we can use Theorem 1.2 to obtain a good bound for $\mu^*(R)$ for all R close to S. For instance, by setting $R_1 = R-1$, $y = R/(R-1)$ and $x = 2$ one can deduce that

$$\begin{aligned} \mu^*(R) &\le \frac{(\frac{R}{R-1})^{R-1}x}{1-e^{-x}(\frac{R}{R-1})^{R}}\mu^*(R-1) < \frac{2e}{1/2}\mu^*(R-1) \\ &= 4e\mu^*(R-1), \end{aligned} \tag{4}$$

where with a more careful choice of x and y one can replace $4e$ by a smaller constant.

Our bounds generalize to codes over an arbitrary alphabet. Consider a finite alphabet A of cardinality q. Let A^n be the set of all strings of length n formed by the elements of A. Instead of $\mu^*(R)$ we consider its natural generalization $\mu_q^*(R)$. With only nominal changes, we can repeat the proof of Theorem 1.2 to obtain

Theorem 1.5: Given a pair of positive integers $R > R_1 \ge 1$,

$$\mu_q^*(R) \le \frac{y^{R_1}(\frac{y}{y-1})^{R-R_1}\binom{R}{R_1}^{-1}x}{1-e^{-x}y^R}\mu_q^*(R_1), \tag{5}$$

holds for any pair of positive constants x and y satisfying $y > 1$ and $1 - e^{-x}y^R > 0$.

Since it is known (see, e.g. Corollary 12.4.9 of [1]) that $\mu_q^*(1) \le 2$ for any fixed q, we can obtain the following corollary.

Corollary 1.6: For any $R \ge 2$, we have

$$\mu_q^*(R) \le e(x_0+1)\mu_q^*(1) \le 2e(x_0+1),$$

where x_0 is the larger root of the equation $e^x = (x+1)R^R$.

Our proof of Theorem 1.2 provides an efficient algorithm that constructs a code satisfying the claimed bound (see Section 4 for more details). The rest of the paper is organized as follows. The next two sections of the paper are devoted to the proof of Theorem 1.2. Section 2 contains a few lemmas and Section 3 presents the rest of the proof. In the end of Section 3, we show how to modify the proof of Theorem 1.2 to prove Theorem 1.5. The final section, Section 4 contains several concluding remarks.

II. Lemmas

Lemma 2.1: Let $(f_n), (a_n), (b_n)$ and (s_n) be sequences of positive numbers where

$$\limsup_{n\to\infty} f_n \le f, \quad \limsup_{n\to\infty} a_n \le a, \quad \limsup_{n\to\infty} b_n \le b < 1,$$

and

$$s_n \le a_n f_{\lfloor n/y \rfloor} + b_n s_{\lfloor n/y \rfloor}, \tag{6}$$

where $y > 1$ is a constant. Then

$$\limsup_{n\to\infty} s_n \le \frac{af}{1-b}.$$

Proof: As $\limsup_{n\to\infty} b_n < 1$, it is clear that the sequence (s_n) is upper bounded, so its $\limsup$ exists and will be denoted by s. By the recursive inequality (6), s must satisfy

$$s \le af + bs,$$

which implies that $s \le \frac{af}{1-b}$, completing the proof. □

The next lemma is purely graph theoretic. A graph consists of a vertex set V and an edge set E, where E is a subset of the set of all unordered pairs of V. If the pair $(u, v) \in E$, we say that the vertices u and v are adjacent. The degree of u is the number of vertices adjacent to u; G is d-regular if the degree of every vertex is d. For a vertex u, $N(u)$ denotes the union of u with the set of vertices adjacent to it.

Given a graph G with vertex set V, for each subset X of V set $N(X) = \cup_{u\in X} N(u)$. Furthermore, set $\bar{N}(X) = V\backslash N(X)$.

Lemma 2.2: For every positive constant x and a d-regular graph G on m vertices, there is a set X of vertices of cardinality at most $xm/(d+1)$ such that

$$|\bar{N}(X)| \le e^{-x}e^{\frac{d+1}{m}}m.$$

Proof: Pick uniformly at random a set X of $k = \lfloor xm/(d+1) \rfloor$ vertices. A vertex v belongs to $\bar{N}(X)$ if and only if X and $N(v)$ are disjoint. The probability of this event is precisely

$$\begin{aligned} \mathbf{P} &= \frac{\binom{m-d-1}{k}}{\binom{m}{k}} = \frac{(m-d-1)\cdots(m-d-k)}{m\cdots(m-k+1)} \\ &\le \left(1-\frac{d+1}{m}\right)^k \le \left(1-\frac{d+1}{m}\right)^{\frac{mx}{d+1}-1} \\ &\le e^{-(\frac{d+1}{m})(\frac{xm}{d+1}-1)} = e^{-x}e^{\frac{d+1}{m}}. \end{aligned}$$

Here we used the trivial fact that $e^{-z} \ge 1 - z$ for any z between 0 and 1. It follows that expectation of $|\bar{N}(X)|$ is at most $e^{-x}e^{\frac{d+1}{m}}m$ and therefore there exists a set X such that $|\bar{N}(X)| \le e^{-x}e^{\frac{d+1}{m}}m$, completing the proof. □

III. Proof of Theorem 1.2

Let y be an arbitrary positive constant larger than 1. For a pair (n, R) set $n_1 = \lfloor n/y \rfloor$ and let $1 \le R_1 < R$, $n_1' = n - n_1$ and $R_1' = R - R_1$. Given two strings $s' \in \mathbb{F}_2^{n_1'}$ and $s \in \mathbb{F}_2^{n_1}$, $s' \oplus s$ denotes the concatenation of s' and s. Clearly $s' \oplus s$ is a string in $\mathbb{F}_2^n$. Furthermore, for two sets $S' \subset \mathbb{F}_2^{n_1'}$ and $S \subset \mathbb{F}_2^{n_1}$, define $S' \oplus S = \{s' \oplus s | s' \in S', s \in S\}$.

View $\mathbb{F}_2^{n_1'}$ as the vertex set of a graph, where two vertices are adjacent if their Hamming distance is at most R_1'. Clearly, this graph has $m = 2^{n_1'}$ vertices and all degrees equal $d = V(n_1', R_1') - 1$. Consider a set $X \subseteq \mathbb{F}_2^{n_1'}$ as in Lemma 2.2. The parameter x, which depends on R, but does not depend on n, will be later optimized.

Next, we give a recursive construction for a covering code with small density, inspired by a construction of Cooper, Ellis and Kahng [2].

Let K_1 and K_2 be optimal covering codes in $\mathbb{F}_2^{n_1}$ of radii R_1 and R, respectively. By definition, it is easy to see that the set

$$K = (X \oplus K_1) \cup (\bar{N}(X) \oplus K_2),$$

is a covering code of radius R in $\mathbb{F}_2^n$. As K_1 and K_2 are optimal, their cardinalities are $\mu(n_1, R_1)\frac{2^{n_1}}{V(n_1,R_1)}$ and $\mu(n_1, R)\frac{2^{n_1}}{V(n_1,R)}$, respectively. So the cardinality of K is at most

$$x\frac{2^{n_1'}}{V(n_1', R_1')}\frac{\mu(n_1, R_1)2^{n_1}}{V(n_1, R_1)} + e^{-x}e^{\frac{d+1}{m}}2^{n_1'}\frac{\mu(n_1, R)2^{n_1}}{V(n_1, R)}$$
$$= x\frac{\mu(n_1, R_1)2^{n}}{V(n_1', R_1')V(n_1, R_1)} + \frac{\mu(n_1, R)2^{n}}{V(n_1, R)}e^{-x}e^{\frac{d+1}{m}}.$$

On the other hand, by the definition of $\mu(n, R)$, $|K| \geq \mu(n, R)\frac{2^n}{V(n,R)}$, so

$$\begin{aligned}\mu(n, R)\frac{2^n}{V(n, R)} &\leq \frac{2^n}{V(n_1', R_1')V(n_1, R_1)}x\mu(n_1, R_1)\\ &+ \frac{2^n}{V(n_1, R)}e^{-x}e^{\frac{d+1}{m}}\mu(n_1, R),\end{aligned} \qquad (7)$$

which implies

$$\begin{aligned}\mu(n, R) &\leq \frac{V(n, R)}{V(n_1', R_1')V(n_1, R_1)}x\mu(n_1, R_1)\\ &+ \frac{V(n, R)}{V(n_1, R)}e^{-x}e^{\frac{d+1}{m}}\mu(n_1, R).\end{aligned} \qquad (8)$$

Now we are in position to apply Lemma 2.1; $\mu(n, R), \mu(n_1, R_1), \frac{V(n,R)}{V(n_1',R_1')V(n_1,R_1)}x$ and $\frac{V(n,R)}{V(n_1,R)}e^{-x}e^{\frac{d+1}{m}}$ play the roles of s_n, f_n, a_n and b_n, respectively.

First of all, we have (by definition) that

$$\limsup_{n\to\infty} \mu(n_1, R_1) = \limsup_{n_1\to\infty} \mu(n_1, R_1) = \mu^*(R_1)$$

and

$$\limsup_{n\to\infty} \mu(n, R) = \mu^*(R).$$

Next, for all large enough l, $V(l, R) = \sum_{i=0}^{R}\binom{l}{R} \approx \binom{l}{R} \approx \frac{l^R}{R!}$. Moreover, $R_1' = R - R_1$, $\lim_{n\to\infty}\frac{n}{n_1} = y$ and $\lim_{n\to\infty}\frac{n}{n_1'} = \frac{y}{y-1}$. So

$$\begin{aligned}\lim_{n\to\infty}\frac{V(n, R)}{V(n_1', R_1')V(n_1, R_1)} &= \lim_{n\to\infty}\frac{n^R}{n_1^{R_1}n_1^{\prime R_1'}}\frac{R_1!R_1'!}{R!} \qquad (9)\\ &= y^{R_1}\left(\frac{y}{y-1}\right)^{R-R_1}\binom{R}{R_1}^{-1}.\end{aligned}$$

Similarly

$$\lim_{n\to\infty}\frac{V(n, R)}{V(n_1, R)} = \lim_{n\to\infty}\left(\frac{n}{n_1}\right)^R = y^R, \qquad (10)$$

and finally $\lim_{n\to\infty} e^{\frac{d+1}{m}} = 1$ (recall that $m = 2^{n_1'}$ and $d+1 = V(n_1', R_1') \ll m$). Lemma 2.1 yields

$$\mu^*(R) \leq \frac{y^{R_1}(\frac{y}{y-1})^{R-R_1}\binom{R}{R_1}^{-1}x}{1 - e^{-x}y^R}\mu^*(R_1), \qquad (11)$$

for any constant $y > 1$ and any positive constant x satisfying $1 - e^{-x}y^R > 0$. This concludes the proof. □

To prove Theorem 1.5, we only need to make few nominal changes, which are due to the fact that $|A^n| = q^n$ and a Hamming ball with radius R now has $\sum_{i=0}^{R}(q-1)^i\binom{n}{i} \approx (q-1)^R\frac{n^R}{R!}$ vertices. The presence of q does not really matter; a careful look at (7), (8), (9) and (10) reveals that the terms containing q cancel each other and the whole analysis remains the same.

IV. Remarks

A slightly better bound. Corollary 1.3 can be improved slightly by optimizing the estimate in (3) as a two-variable function in x and y (instead of fixing $y = R$ and optimizing x). Consequently, we could also improve Corollary 1.4 slightly. However, the details are a little bit technical and we prefer to present these corollaries in the current form for the sake of clarity.

Algorithmic aspects. Our proof provides an efficient randomized algorithm to find codes with improved densities. Notice that in order to find a code with radius R satisfying the bound in Corollary 1.3, the codes K_1 and K_2 in the Section 3 do not need to be optimal. It is sufficient that they both satisfy the bound in Corollary 1.3 (as we use induction). The only place where randomness is involved is Lemma 2.2. It is simple to show that a random set X satisfies the requirements of the lemma with positive constant probability.

When it becomes important to have a deterministic algorithm, we can derandomize the proof of Lemma 2.2 by the standard "conditioning method" (see [3]). The set X in Lemma 2.2 can be produced by the following deterministic algorithm: Order the vertices of the graph as $v_1, v_2, \ldots, v_m$. Assume that $v_1, \ldots, v_{i-1}$ have been considered and a subset X_{i-1} has been selected (X_0 is the empty set). If $|X_{i-1}| = k$, let $X = X_{i-1}$ and output X. Otherwise, consider v_i and compute the (conditional) expectations of $|\bar{N}(X)|$ with respect to one of the following two cases

(i) v_i is chosen in X and the rest of X is chosen randomly from $v_{i+1}, \ldots, v_n$.

(ii) v_i is not chosen in X and the rest of X is chosen randomly from $v_{i+1}, \ldots, v_n$.

If the first expectation is not larger than the second, choose v_i and set $X_i = X_{i-1} \cup \{v_i\}$. Otherwise, do not choose v_i and set $X_i = X_{i-1}$. Continue with v_{i+1}.

The calculation of the expectations is straightforward. For example, let us consider the first expectation. Assume that $X_{i-1}' = X_{i-1} \cup \{v_i\}$ has l elements. The (conditional) expectation of $|\bar{N}(X)|$ is

$$\sum_{y\in\bar{N}(X_{i-1}')} \mathbf{P}\big[y \in \bar{N}(X)\big],$$

where $\mathbf{P}\big[y \in \bar{N}(X)\big]$ (similar to the calculation in the proof of Lemma 2.2) is the probability that $N(y)$ does not contain any element of a random set of size $k - l$ chosen uniformly from all sets of this size contained in $\{v_{i+1}, \ldots, v_n\}$.

One-sided codes. In a recent paper, Cooper, Ellis and Kahng [2] introduced the notion of one-sided codes. For $x, y \in \mathbb{F}_2^n$, we write $x \succ y$ if $x_i \geq y_i$ for all $1 \leq i \leq n$. The one-sided ball with radius R centered at x consists of those vertices y's where $x \succ y$ and the Hamming distance between x and y is at most R. A subset K of $\mathbb{F}_2^n$ is a one-sided code of radius R if the one-sided balls of radius R centered at the vertices of K cover $\mathbb{F}_2^n$. For a fixed R and large n, the dominating part of the one-sided balls has volume approximately $\binom{n/2}{R}$, so a one-sided code of radius R has at least $(1+o(1))2^n/\binom{n/2}{R}$ elements. (Here and later the asymptotic notation is used under the assumption that $n \to \infty$.) Naturally, we define $|K|/\frac{2^n}{\binom{n/2}{R}}$ as the density of K. Now we can define $\mu^*_{os}(R)$ as the counterpart of $\mu^*(R)$.

The authors of [2] proved (in a somewhat different formulation) that for all fixed R there is a constant $c(R)$ such that $\mu^*_{os}(R) \leq c(R)$. The constant $c(R)$ was not computed explicitly, but a careful reading reveals that it should be at least a^R for some constant $a > 1$. Repeating the proof of Theorem 1.2 for one-sided codes (a minor modification is needed) we can prove the statement of Theorem 1.2 for $\mu^*_{os}(R)$ and (consequently) improve the bound on $\mu^*_{os}(R)$ to order $R \log R$.

Theorem 4.1: Given a pair of positive integers $R > R_1 \geq 1$,

$$\mu^*_{os}(R) \leq \frac{y^{R_1}(\frac{y}{y-1})^{R-R_1}\binom{R}{R_1}^{-1} x\mu^*_{os}(R_1)}{1-e^{-x}y^R},$$

holds for any pair of positive constants x and y satisfying $y > 1$ and $1 - e^{-x}y^R > 0$.

It follows that

Corollary 4.2: For all $R \geq 3$,

$$\mu^*_{os}(R) \leq e(R\log R + \log R + \log\log R + 1)\mu^*_{os}(1).$$

Notice that here we do not know whether $\mu^*_{os}(1) = 1$.

The minor modification we need in the proof of Theorem 4.1 is due to the fact that the one-side balls have different volumes. It is not hard, however, to overcome this obstacle. By the Binomial Distribution, the fraction of vertices of $\mathbb{F}_2^n$ with weights more than $\frac{n}{2} + 10R\sqrt{n\log n}$ or less than $\frac{n}{2} - 10R\sqrt{n\log n}$ is $o(1/n^R)$ (10 can be replaced by a smaller number), so it suffices to focus on the vertices with weights between $\frac{n}{2} - 10R\sqrt{n\log n}$ and $\frac{n}{2} + 10R\sqrt{n\log n}$. The one sided balls centered at these vertices all have volume approximately $\binom{n/2}{R}$. We leave out the details which might serve as an exercise.

Acknowledgment. We thank S. Litsyn for several useful comments.

REFERENCES

[1] G. Cohen, I. Honkala, S. Litsyn and A. Lobstein, *Covering codes*. North-Holland Mathematical Library, 54. North-Holland Publishing Co., Amsterdam, 1997.

[2] J. Cooper, R. Ellis and A. Kahng, Asymmetric binary covering codes, *J. Comb. Th. Ser. A*, to appear.

[3] R. Motwani and P. Raghavan, *Randomized algorithms*. Cambridge Univ. Press, 1995.