ii) A $[51, 41]2$ code. The M part is 1B6, 193, 1CC, 187, 1F6, F7, 16E, 140, 3C, 296, 22F, 303, 381, 365, 11D, 1A3, 274, 2F2, 254, 56, F, 41, 357, 208, 34, 329, 28D, 31D, 3D5, 129, 3D7, B7, 3EC, 2E2, 23C, AD, 34E, 155, 2E6, 371, D4.

iii) A $[32, 8]10$ code. The M part is 6AD83A, 656BB6, 17DA79, 35E589, E9B825, 2E157F, 96FED5, EC01F9.

The ADS of the code in i) and the binary Golay code produces a $[45, 20]8$ code. This is a new code.

REFERENCES

[1] A. Blokhuis and C. W. H. Lam, "More coverings by rook domains," *J. Combin. Theory*, ser. A, vol. 36, pp. 240–244, 1984.

[2] G. D. Cohen, I. S. Honkala, S. N. Litsyn, and A. C. Lobstein, *Covering Codes*. Amsterdam, The Netherlands: North-Holland, 1997.

[3] E. M. Gabidulin, A. A. Davydov, and L. M. Tombak, "Linear codes with covering radius 2 and other new covering codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 219–224, Jan. 1991.

[4] R. L. Graham and N. J. A. Sloane, "On the covering radius of codes," *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 385–401, May 1985.

[5] J. H. van Lint, Jr., "Covering radius problems," Master's thesis, Eindhoven Univ. Technol., Eindhoven, The Netherlands, 1988.

[6] P. R. J. Östergård and M. K. Kaikkonen, "New upper bounds for binary covering codes," *Discr. Math.*, vol. 178, pp. 165–179, 1998.

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 (least) density of the best binary covering codes of radius R. In particular, this inequality implies that $\mu^*(R) \leq e \cdot (R \log R + \log R + \log\log R + 2)$, 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,

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

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 (least) 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, $\mu^*(R) \geq 1$. One of the fundamental problems in coding theory is to settle the following conjecture [1, Ch. 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]

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

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 correspondence, we shall significantly improve upon this bound. Our main result is the following recursive inequality.

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

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

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 the following.

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

Proof: Choosing $R_1 = 1$, we have

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

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

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

We now optimize

$$f(x) = \frac{ex}{1 - e^{-x} R^R}$$

over x. The derivative of $f(x)$ is $e\left(\frac{1-(x+1)e^{-x}R^R}{(1-e^{-x}R^R)^2}\right)$. Conditioned on $1 - e^{-x} R^R > 0$, $f(x)$ reaches it minimum at the larger root x_0 of the

Manuscript received May 29, 2002; revised January 6, 2003. The work of M. Krivelevich was supported in part by a USA–Israel BSF Grant, by a grant from the Israel Science Foundation, and by a Bergmann Memorial Grant. The work of B. Sudakov was supported in part by the National Science Foundation under Grants DMS-0106589, CCR-9987845, and by the State of New Jersey. The work of V. H. Vu was supported in part by the University of California, San Diego under Grant RB091G-VU, by the National Science Foundation under Grant DMS-0200357, and by an A. Sloan Fellowship.

M. Krivelevich is with the Department of Mathematics, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel-Aviv University, Ramat-Aviv 69978, Tel-Aviv, Israel (e-mail: krivelev@post.tau.ac.il).

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).

V. H. Vu is with the Department of Mathematics, University of California, San Diego, La Jolla, CA 92093 USA (e-mail:vanvu@ucsd.edu).

Communicated by S. Litsyn, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2003.813490

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 $R\geq 3$, $x_0\leq R\log R+\log R+\log\log R+1$, 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 $R\geq 3$

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

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

$$\mu^*(R)\leq\frac{(\frac{R}{R-1})^{R-1}x}{1-e^{-x}(\frac{R}{R-1})^R}\,\mu^*(R-1)<\frac{2e}{1/2}\,\mu^*(R-1)$$
$$=4e\mu^*(R-1) \tag{4}$$

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 the following.

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

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

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., [1, Corollary 12.4.9]) that $\mu_q^*(1)\leq 2$ for any fixed q, we can obtain the following corollary.

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

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

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 IV for more details). The rest of this correspondence is organized as follows. The next two sections are devoted to the proof of Theorem 1.2. Section II contains a few lemmas and Section III presents the rest of the proof. At the end of Section III, we show how to modify the proof of Theorem 1.2 to prove Theorem 1.5. The final section, Section IV, 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

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

and

$$s_n\leq a_nf_{\lfloor n/y\rfloor}+b_ns_{\lfloor n/y\rfloor} \tag{6}$$

where $y>1$ is a constant. Then

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

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

$$s\leq af+bs$$

which implies that $s\leq\frac{af}{1-b}$, 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 $\overline{N}(X)=V\backslash N(X)$.

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

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

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

$$\boldsymbol{P}=\frac{\binom{m-d-1}{k}}{\binom{m}{k}}=\frac{(m-d-1)\cdots(m-d-k)}{m\cdots(m-k+1)}$$
$$\leq\left(1-\frac{d+1}{m}\right)^k\leq\left(1-\frac{d+1}{m}\right)^{\frac{mx}{d+1}-1}$$
$$\leq e^{-(\frac{d+1}{m})(\frac{xm}{d+1}-1)}=e^{-x}e^{\frac{d+1}{m}}.$$

Here, we used the trivial fact that $e^{-z}\geq 1-z$ for any z between 0 and 1. It follows that expectation of $|\overline{N}(X)|$ is at most $e^{-x}e^{\frac{d+1}{m}}m$ and, therefore, there exists a set X such that $|\overline{N}(X)|\leq e^{-x}e^{\frac{d+1}{m}}m$, 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 $1\leq R_1<R$, $n_1'=n-n_1$, 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

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

is a covering code of radius R in $\mathbb{F}_2^n$. As K_1 and K_2 are optimal, their cardinalities are

$$\mu(n_1,\,R_1)\frac{2^{n_1}}{V(n_1,\,R_1)}\quad\text{and}\quad\mu(n_1,\,R)\frac{2^{n_1}}{V(n_1,\,R)}$$

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

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

which implies

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

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

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

Similarly

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

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

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

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)–(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 Section III 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 $|\overline{N}(X)|$ 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 $|\overline{N}(X)|$ is

$$\sum_{y\in\overline{N}(X_{i-1}')}\boldsymbol{P}\left[y\in\overline{N}(X)\right]$$

where $\boldsymbol{P}\left[y\in\overline{N}(X)\right]$ (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 ys 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 $\mu^*_{os}(R) \le c(R)$. 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 $R > R_1 \ge 1$

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

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

Then we have the following.

Corollary 4.2: For all $R \ge 3$

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

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

The authors wish to thank the Associate Editor S. Litsyn for several useful comments.

REFERENCES

[1] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*, ser. North-Holland Mathematical Library. Amsterdam, The Netherlands: North-Holland, 1997, vol. 54.

[2] J. Cooper, R. Ellis, and A. Kahng, "Asymmetric binary covering codes," *J. Comb. Theory Ser. A*, vol. 100, no. 2, pp. 232–249, 2002.

[3] R. Motwani and P. Raghavan, *Randomized Algorithms*. Cambridge, U.K.: Cambridge Univ. Press, 1995.

Near-Ellipsoidal Voronoi Coding

Stéphane Ragot, *Student Member, IEEE*, Minjie Xie, and Roch Lefebvre, *Member, IEEE*

***Abstract*—In this correspondence, we consider a special case of Voronoi coding, where a lattice Λ in $\mathbb{R}^n$ is shaped (or truncated) using a lattice $\Lambda' = \{(m_1 x_1, \ldots, m_n x_n) | (x_1, \ldots, x_n) \in \Lambda\}$ for a fixed $\underline{m} = (m_1, \ldots, m_n) \in (\mathbb{N} \setminus \{0, 1\})^n$. Using this technique, the shaping boundary is near-ellipsoidal. It is shown that the resulting codes can be indexed by standard Voronoi indexing algorithms plus a conditional modification step, as far as Λ' is a sublattice of Λ. We derive the underlying conditions on $\underline{m}$ and present generic near-ellipsoidal Voronoi indexing algorithms. Examples of constraints on $\underline{m}$ and conditional modification are provided for the lattices A_2, D_n ($n \ge 2$) and $2D_n^+$ (n even ≥ 4).**

***Index Terms*—Lattice, lattice codes, lattice indexing, Voronoi coding.**

I. INTRODUCTION

We address the problem of designing (near-)ellipsoidal lattice codes with fast indexing algorithms. The motivation for this work lies in wide-band speech coding. More specifically, we are interested in designing low-complexity high-dimensional algebraic spectrum coding based on a Gaussian mixture model [6], which implies construction of codes to quantize correlated Gaussian vector sources.

Lattices, which are extensively studied in [10], are linear discrete sets of points. Without loss of generality, we will consider here only lattices defined in $\mathbb{R}^n$. A lattice code is defined by selecting a finite subset of a lattice. Lattice codes find important applications, such as coded modulation and vector quantization. They are known to yield potential good performance–complexity tradeoffs and to be asymptotically good in certain conditions.

Given a lattice, two important steps are required to implement a lattice code.

1) Shape the lattice properly (i.e., define the support region of the lattice code) and design the indexing algorithms to label codevectors.

2) Design a procedure to find the closest lattice point *within the code*, that is, the nearest codevector to any arbitrary point.

In this correspondence we deal only with the lattice shaping and indexing problem. This problem is important, since an optimized lattice shaping may bring significant performance gains compared to a baseline shaping (e.g., scalar quantization in source coding applications) [2], [13]. To be more specific, we will focus hereafter on lattice codes defined by ellipsoidal truncation. As mentioned earlier, this restriction is motivated by the need in certain applications to quantize correlated Gaussian vector sources. Other shaping techniques, yielding, for instance, codes defined *on* or *inside* spherical [11], [12] or pyramidal [7], [14], [15] shapes, are not considered.

Manuscript received June 2, 2001; revised December 20, 2002. This work was supported by the Natural Sciences and Engineering Research Council of Canada and VoiceAge Corp. The material in this correspondence was presented in part at the 7th Canadian Workshop on Information Theory, Vancouver, BC, Canada, June 2001.

S. Ragot and R. Lefebvre are with the Department of Electrical and Computer Engineering, University of Sherbrooke, Sherbrooke, QC J1K 2R1 Canada (e-mail: ragot@hermes.usherb.ca; roch.lefebvre@courrier.usherb.ca)

M. Xie was with the University of Sherbrooke. He is now with Polycom, Inc., Burlington, MA 01803 USA (e-mail: mxie@AUSTIN.Polycom.com).

Communicated by R. Zamir, Associate Editor for Source Coding.

Digital Object Identifier 10.1109/TIT.2003.813484