Designs, Codes and Cryptography, 14, 207–212 (1998)

An Inequality on the Coding Gain of Densest Lattice Packings in Successive Dimensions

AMIR H. BANIHASHEMI ahashemi@comm.toronto.edu
Department of Electrical and Computer Engineering, University of Toronto, Toronto, Ontario, Canada M5S 1A4

AMIR K. KHANDANI
Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

Communicated by: E. F. Assmus, Jr.

Received October 29, 1996; Revised September 16, 1997; Accepted November 11, 1997

Abstract. A lower bound of the form $(\frac{2n}{n+1})^{\frac{1}{n}}\gamma_{n-1}^{\frac{n-1}{n}}$ is derived on the coding gain γ_n of the densest n-dimensional (n-D) lattice(s). The bound is obtained based on constructing an n-D lattice which consists of parallel layers. Each layer is selected as a translated version of a densest $(n-1)$-D lattice. The relative positioning of the layers is adjusted to make the coding gain as large as possible. For large values of n, the bound is improved through tightening Ryškov's inequality on covering radius and minimum distance of a lattice.

Keywords: Lattice sphere packing, coding gain, densest lattices, covering radius, minimum distance

1. Introduction

Coding gain γ is an important structural parameter of a lattice. The problem of finding dense lattice packings (large γ) is of great importance in both mathematics and communications [3, pp. 385–411], [1, pp. 66–74]. The maximum value of γ in a given dimension n is denoted as γ_n, and is called the Hermite's constant. The value of γ_n is known only for the dimensions $n \leq 8$ [3, p. 410]. It has never been proved that γ_n is an increasing function of n, although this is very likely to be true. In this work, we establish a lower bound on γ_n in terms of γ_{n-1} and n. The bound is derived using a densely constructed n-dimensional (n-D) lattice which is composed of parallel layers. Each layer is a translated version of a densest $(n-1)$-D lattice. The layers are placed such that the lattice points in one layer are orthogonally projected to the deep holes of the two adjacent layers. This, along with the proper adjustment of the spacing between the layers, helps to increase the coding gain.

In deriving the bound on γ_n, we make use of a lower bound on the covering radius of a lattice (μ) in terms of its minimum distance (λ) and dimension (n) which is due to Ryškov [9]. For large values of n, the derived bound on γ_n is improved through establishing a lower bound on μ in terms of λ and n which is tighter than the Ryškov's bound (for $n > 42$).

It should be also noted that Mordell and Oppenheim, independent of each other, have obtained an upper bound of the form $(\gamma_{n-1})^{(n-1)/(n-2)}$ on γ_n, see [3, p. 376]. This, in conjunction with the lower bound presented here, provides a tight range for γ_n in terms of γ_{n-1}.

It is quite known how to build up a packing in $\mathbb{R}^n$ from a given lattice packing (corresponding to a lattice L) in $\mathbb{R}^{n-1}$ by extending the latter to a layer of spheres in $\mathbb{R}^n$ (with centers at the points of L), and stacking congruent layers as densely as possible [4]-[7], [2]. In fact, it appears that the densest lattices in dimensions $n \leq 8$ have a layer structure, see e.g., [1, p. 164]. In the above construction, we call the lattice L the *base* for the resulting packing. As explained before, we select the base to be a densest $(n-1)$-D lattice. To preserve the lattice property, we form the successive layers by translating the base with a fixed n-D vector, called the *generator vector*, successively. The generator vector is selected such that the density (coding gain) of the resulting lattice is as large as possible.

2. Preliminaries

Let $\mathbb{R}^m$ be the m-dimensional real vector space with the standard inner product $\langle .,. \rangle$, and Euclidean length $\|\mathbf{x}\| = \langle \mathbf{x}, \mathbf{x} \rangle^{\frac{1}{2}}$. A *lattice* is a discrete additive subgroup L of $\mathbb{R}^m$. Its *dimension* is the dimension of the $\mathbb{R}$-subspace $span(L)$ that it spans. Each lattice L of dimension n has a *basis*, i.e., a set $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ of n linearly independent elements of L that generate L as their linear integer combinations. The corresponding *generator matrix* (also called *basis matrix*) is the $n \times m$ matrix B which has the basis vectors as its rows. The *determinant* of L, $\det(L)$, is defined as $\det(L) = [\det(BB^T)]^{1/2}$. We assume lattices to be *full-dimensional*, i.e., $n = m$, resulting in $\det(L) = |\det(B)|$.

Consider a n-D lattice L. The length of the shortest nonzero vector(s) of L (also called the *minimum distance* of L) is denoted by $\lambda(L)$. Assume that an n-D sphere of radius $\lambda(L)/2$ is centered at each lattice point. This arrangement of spheres is called a *lattice sphere packing* or briefly *packing* corresponding to the lattice L. Related to the density of the lattice packing L [1, p. 73], the *coding gain* is defined as

$$\gamma(L) = \lambda(L)^2 \det(L)^{-\frac{2}{n}}. \tag{1}$$

This is also a measure of the performance of the corresponding lattice code in channel coding applications. *Hermite's constant* γ_n is defined as the supremum value of γ over all n-D lattices. It is known that γ_n is attainable [3, p. 267]. The value of γ_n, however, is explicitly known only for $n \leq 8$.

The *covering radius* $\mu(L)$ of a lattice L is the smallest number r such that all vectors $\mathbf{v} \in span(L)$ are at distance at most r from a lattice point. The *Voronoi cell* $\mathcal{V}(\mathbf{p})$ of a point $\mathbf{p} \in L$ consists of those points of $span(L)$ which are at least as close to $\mathbf{p}$ as to any other lattice point. (Voronoi cells are also called *Dirichlet regions*, mainly in Geometry of Numbers). $\mathcal{V}(\mathbf{p})$ has at least two vertices at distance $\mu(L)$ from $\mathbf{p}$. These are called the *deep holes* of the lattice corresponding to the point $\mathbf{p}$.

We need the following lemma from [9]:

LEMMA 1 *The length of the smallest edge of an arbitrary n-D simplex located inside a n-D sphere of radius r is upper bounded by $[2(n+1)/n]^{1/2}r$. This bound is achieved only for a regular simplex inscribed in the sphere.*

THEOREM 1 (*Ryškov*) *For an n-D lattice L, we have*

$$\mu(L) \geq \sqrt{\frac{n}{2(n+1)}}\lambda(L). \tag{2}$$

Proof. Consider a sphere $\mathcal{S}(\mathbf{v})$ of radius $\mu(L)$ centered at an arbitrary deep hole $\mathbf{v}$ of the lattice L. Since $\mathbf{v}$ is the common vertex of some adjacent n-D polytopes (Voronoi cells of L), it is located at the intersection of at least n hyper-planes (which are the facets of the corresponding Voronoi cells). It is not then difficult to see that $\mathbf{v}$ is the deep hole corresponding to at least $n+1$ adjacent Voronoi cells. This means that there exist at least $n+1$ lattice points on the surface of $\mathcal{S}(\mathbf{v})$. Let the minimum distance between these points be denoted by d. We have $\lambda(L) \leq d$. Considering the aforementioned $n+1$ lattice points as the vertices of a simplex, and using Lemma 1, we obtain $d \leq [2(n+1)/n]^{1/2}\mu(L)$. Combining these inequalities proves the theorem. ■

It is interesting to note that inequality (2) is satisfied with equality for the densest one- and two-dimensional lattices, i.e., the integer lattice $\mathbb{Z}$ and the hexagonal lattice.

Inequality (2) could also be obtained by combining the upper bound on the density of packings given by Rogers (see [1, p. 19]), with the lower bound on the thickness of coverings due to Coxeter, Few and Rogers (C-F-R) (see [1, p. 40]). Note that both of these results had been available quite a while before the publication of the Ryškov's bound in [8]. It is clear from the above observation that by tightening either bounds, one can improve the inequality given in (2). Rogers' bound is the best known bound for $n \leq 42$, [1, p. 20]. For $n > 42$, the Kabatiansky-Levenshtein (K-L) bound (see [1, pp. 264-265]) takes over [1, p. 20]. There does not, however, exist a simple expression for K-L bound except for the large values of n. Combining K-L and C-F-R bounds for large values of n, as given in [1, p. 19, p. 40], we obtain

$$\mu(L) \geq 0.7573\left(\frac{n}{e\sqrt{e}}\right)^{1/n}\lambda(L), \tag{3}$$

which is tighter than (2).

Remark. For a review of earlier works on sphere packing and covering, and in particular, bounds on packing and covering densities, the interested reader is referred to [8].

3. Main Result

Let L_b be an $(n-1)$-D lattice with basis $\mathbf{b}_1, \ldots, \mathbf{b}_{n-1}$, where $\mathbf{b}_i = (b_{i,1}, \ldots, b_{i,n-1})$, and let $\mathbf{v} = (v_1, \ldots, v_{n-1})$ be a deep hole of L_b. We construct a n-D lattice L using the following generator matrix

$$B' = \begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,n-1} & 0 \\ b_{2,1} & b_{2,2} & \cdots & b_{2,n-1} & 0 \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ b_{n-1,1} & b_{n-1,2} & \cdots & b_{n-1,n-1} & 0 \\ v_1 & v_2 & \cdots & v_{n-1} & h \end{pmatrix}, \tag{4}$$

where h is a properly selected positive number. It is easy to see that the lattice L has a layer structure with the base lattice L_b, and the generator vector $\mathbf{b}'_n = (v_1, \ldots, v_{n-1}, h)$. As we will see later, the selection of $\mathbf{v}$ as a deep hole helps to increase the coding gain (density) of L. It is easy to show that

$$\det(L) = h \det(L_b). \tag{5}$$

To maximize the coding gain of L, we would like to select h as the smallest number such that $\lambda' \stackrel{\Delta}{=} \lambda(L) = \lambda(L_b) \stackrel{\Delta}{=} \lambda$. Choosing a proper value for h requires checking the distance between lattice points in different layers. The value of h also depends on the values of $\mu \stackrel{\Delta}{=} \mu(L_b)$ and λ. We select L_b to be a densest $(n-1)$-D lattice, denoted by L_{n-1}. Since we do not know much about the structure of L_{n-1}, for a general value of n, we choose

$$h \geq \frac{\lambda}{2}. \tag{6}$$

This selection guarantees that, except for the lattice points in two adjacent layers, the distance between the other lattice points is at least λ. It is easy to see that the minimum distance between lattice points in two adjacent layers is $\sqrt{\mu^2 + h^2}$. Therefore, to keep λ' equal to λ, we also need

$$h^2 \geq \lambda^2 - \mu^2. \tag{7}$$

The value of h is selected as the smallest number satisfying both (6) and (7). The corresponding value is denoted by h_0. We have

$$h_0 = \begin{cases} \sqrt{\lambda^2 - \mu^2} & \text{if } \mu \leq \frac{\sqrt{3}}{2}\lambda, \\ \lambda/2 & \text{otherwise.} \end{cases} \tag{8}$$

According to (8), the value of h_0 depends on the range of μ (as determined by λ). However, later in Proposition 2, we will present an upper bound on h_0 which depends only on λ and n. This upper bound will be used in conjunction with the following proposition to derive our main result.

PROPOSITION 1 *We have*

$$\gamma(L) = \left(\frac{\lambda}{h_0}\right)^{\frac{2}{n}} \gamma(L_b)^{\frac{n-1}{n}}. \tag{9}$$

Proof. The proof follows using the definition (1), and the facts that $\lambda' = \lambda$ and (5). ∎

PROPOSITION 2 *We have*

$$h_0 \leq \sqrt{\frac{n+1}{2n}}\lambda. \tag{10}$$

Proof. We consider the following two cases:

(i) $\mu \leq \sqrt{3}\lambda/2$. In this case, the result follows by applying inequality (2) to the first expression of (8).

(ii) $\mu > \sqrt{3}\lambda/2$. In this case, using (8), we obtain $h_0 = \lambda/2$ which also satisfies (10). ■

THEOREM 2 (MAIN RESULT) *We have*

$$\gamma_n \geq \left(\frac{2n}{n+1}\right)^{\frac{1}{n}} \gamma_{n-1}^{\frac{n-1}{n}}. \tag{11}$$

Proof. Using Proposition 1, and the facts that $L_b = L_{n-1}$, and $\gamma_n \geq \gamma(L)$, we obtain

$$\gamma_n \geq \left(\frac{\lambda}{h_0}\right)^{\frac{2}{n}} \gamma_{n-1}^{\frac{n-1}{n}}. \tag{12}$$

The proof then follows by applying (10) to (12). ■

Note that inequality (11) is satisfied with equality for $n = 2$.

For large values of n, applying (3), and using the same arguments as in the proofs of Proposition 2 and Theorem 2, we can find a tighter bound than (11) as

$$\gamma_n \geq \left[1 - (0.7573)^2 \left(\frac{n-1}{e\sqrt{e}}\right)^{\frac{2}{n-1}}\right]^{\frac{-1}{n}} \gamma_{n-1}^{\frac{n-1}{n}} > (2.345)^{\frac{1}{n}} \gamma_{n-1}^{\frac{n-1}{n}}. \tag{13}$$

It can be seen that the expression $2n/(n+1)$ in (11) is always less than 2. This, unfortunately, implies that the inequality (11) cannot result in the proof of $\gamma_n \geq \gamma_{n-1}$ for any interesting values of n, i.e., $n \geq 10$. The reason is that to conclude such a result from (11), we need to have $\gamma_{n-1} \leq 2n/(n+1) < 2$. However, referring to the Tables 1.2 and 1.3 of [1], we observe that there already exist lattices in dimensions $n \geq 9$ which have coding gains larger than 2. It is not difficult to see that combining K-L and C-F-R bounds for $n > 42$ cannot help either.

It seems, however, quite natural that one tries to prove $\gamma_n \geq \gamma_{n-1}$ for certain values of $n \geq 10$ by the proper improvement of inequality (2) for the corresponding densest lattices. For the densest lattices in dimensions $n \geq 9$, we expect the number of lattice points on the surface of $\mathcal{S}(\mathbf{v})$, as defined in Theorem 1, to be larger than $n + 1$. To make inequality (2) tighter for these lattices, one might be able to use a well-quantified version of this argument to improve the bound given in Lemma 1.

Acknowledgments

This work was supported in part by an Ontario Graduate Scholarship (OGS) and in part by Natural Sciences and Engineering Research Council of Canada (NSERC).

When this research was conducted A. H. Banihashemi was with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1.

References

1. J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 2nd ed, Springer-Verlag, New York (1993).
2. J. H. Conway and N. J. A. Sloane, Laminated lattices, *Annals Math*., Vol. 116 (1982) pp. 593–620.
3. P. M. Gruber and C. G. Lekkerkerker, *Geometry of Numbers*, 2nd ed., Elsevier Science Publishers B.V., North-Holland, Amsterdam (1987).
4. J. Leech, Some sphere packings in higher space, *Can. J. Math*., Vol. 16 (1964) pp. 657–682.
5. J. Leech, Five dimensional non-lattice sphere packings, *Canad. Math. Bull*., Vol. 10 (1967) pp. 387–393.
6. J. Leech, Six and seven dimensional non-lattice sphere packings, *Canad. Math. Bull*., Vol. 12 (1969) pp. 151–155.
7. J. Leech and N. J. A. Sloane, Sphere packings and error-correcting codes, *Can. J. Math*., Vol. 23 (1971) pp. 718–745.
8. C. A. Rogers, *Packing and Covering*, Cambridge Univ. Press, New York (1964).
9. S. S. Ryškov, Density of an (r, R)-system, *Mat. Zametki*, Vol. 16, No. 3 (1974) pp. 447–454, English translation in *Math. Notes of the Academy of Sciences of the USSR*, Vol. 16 (1975) pp. 855–858.