

The Lifting Construction: A General Solution for the Fat Strut Problem

Vinay A. Vaishampayan*, N. J. A. Sloane*, Sueli I. R. Costa†

*AT&T Shannon Labs, Florham Park, NJ 07932, USA. Email: {vinay,njas}@research.att.com

†University of Campinas, Campinas, SP 13083-970, Brazil. Email: sueli@ime.unicamp.br

Abstract—A cylinder anchored at two distinct points of a lattice $\Lambda \subset \mathbb{R}^n$ is called a *strut* if its interior does not contain a lattice point. We address the problem of constructing struts of maximal radius in a general number of dimensions. Our main contribution is a general construction technique, which we call the *lifting construction*. The lifting construction, which is based on a given target lattice $\Lambda_t \subset \mathbb{R}^{n-1}$ with packing density Δ_t , produces a sequence of struts whose volume converges to Δ_t as the length of the strut grows without bound. The motivation for the problem comes from studying a nonlinear communication problem. We exhibit performance improvements resulting from this construction. Finally, we tighten a previous result of ours—an achievable lower bound on the volume of a strut.

I. INTRODUCTION

Given a lattice $\Lambda \subset \mathbb{R}^n$, a *strut* is an n -dimensional cylinder with circular cross-section whose face centers coincide with distinct lattice points and whose interior does not contain a lattice point, i.e. a strut is an unobstructed cylinder anchored by two lattice points. Our problem is to determine the maximum radius of a strut of given length. We will refer to a strut of maximal radius between two anchor points as a *fat strut*. The case $n = 2$, illustrated in Fig. 1 for $\Lambda = \mathbb{Z}^2$, can be solved explicitly with the result being that a strut of length l has maximal radius $r = 1/l$, independent of the choice of the anchor points. This illustrates a general principle: longer struts must be thinner.

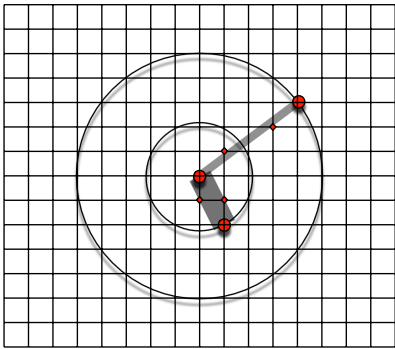


Figure 1. Struts in the two-dimensional lattice \mathbb{Z}^2 . Longer struts are thinner. Diamonds indicate lattice points that constrain the radius.

In dimensions $n > 2$ the situation is different. Two fat struts of the same length may have different radii, and the question then is, for a given length, to find good endpoints for the fattest of fat struts and to determine its radius. Without loss of generality, we may fix one endpoint of the strut at the origin. Henceforth, we refer to the fat strut anchored at the origin and lattice point \mathbf{a} as the fat strut \mathbf{a} .

In this paper we show that the product lr^{n-1} of the length l and radius r of a fat strut \mathbf{a} in $\Lambda \subset \mathbb{R}^n$, is determined by the packing density of the lattice $\Lambda_{\mathbf{a}}$ obtained by projecting Λ into the subspace orthogonal to the axis of the strut. We then construct sequences of struts $\{\mathbf{a}_k\}$ in \mathbb{Z}^n such that $\{\Lambda_{\mathbf{a}_k}\}$ converges to a given target lattice $\Lambda_t \subset \mathbb{R}^{n-1}$. For $n > 2$ we also refine an achievable lower bound on lr^{n-1} using a nonconstructive averaging argument. The achievable lower bound was derived in [13].

The problem has its roots in communication theory [10], [12] but is an interesting geometric question in its own right. It is worth contrasting the problem with the result of Heppes [5] and Horvath [7] that for any lattice sphere packing in dimension three or higher there is always an *infinite* cylinder of nonzero radius which does not touch any of the spheres. This paper completes the work begun in [13] in the following ways: the lifting construction—a general construction for this problem—is given for the first time; a sharper achievable bound is derived which essentially closes the gap with the Minkowski-Hlawka bound [3], and finally, performance improvements using the lifting construction are exhibited through simulation.

The paper is organized as follows: the precise problem formulation is given in Sec. II, some basic results about lattices related to our problem are stated in Sec. III, an upper bound on the radius of a strut is derived in Sec. IV, an example is presented in Sec. V, the lifting construction and formulas for specific lattices are given in Sec. VI, a communication theoretic application is described in Sec. VII and a refinement to a non-constructive lower bound derived in [13] is presented in Sec. VIII.

Vectors will be written in boldface, and are row vectors unless otherwise stated. Matrices are also written in boldface. The $n \times n$ identity matrix is denoted \mathbf{I}_n . The transpose of a matrix \mathbf{G} is denoted \mathbf{G}^{tr} . $[x]$ is the nearest integer to x .

II. PROBLEM FORMULATION

We begin by stating a version of the fat strut problem that is equivalent to the one informally stated in the introduction. Let $\mathbf{a} \in \mathbb{Z}^n$, $\mathbf{a} \neq 0$ be a point in the integer lattice. Consider an infinite cylinder of radius r in \mathbb{R}^n , whose axis contains the points 0 and \mathbf{a} , i.e. the set $\{\mathbf{x} \in \mathbb{R}^n : \min_{t \in \mathbb{R}} \|\mathbf{a}t - \mathbf{x}\| \leq r\}$. The cylinder is said to be a strut if its interior does not contain a lattice point which is not a multiple of \mathbf{a} . It is immediate that a strut has positive radius only if $\mathbf{a} = (a_0, a_1, \dots, a_{n-1})$ is primitive, i.e. $\gcd(\{a_0, a_1, \dots, a_{n-1}\}) = 1$, where $\gcd(\{x, y, z\})$ denotes the greatest common divisor of its integer arguments.

The radius of a fat strut $\mathbf{a} \in \mathbb{Z}^n$ is given by

$$r(\mathbf{a}) := \min_{\mathbf{n} \in \mathbb{Z}^n} \min_{t \in \mathbb{R}} \|\mathbf{a}t - \mathbf{n}\|, \quad (1)$$

where the outer minimization is over vectors \mathbf{n} which are not multiples of \mathbf{a} . The inner minimum in (1) is achieved by the value of t for which $\langle \mathbf{n} - t\mathbf{a}, \mathbf{a} \rangle = 0$ and is equal to the length of the vector obtained by projecting \mathbf{n} into the subspace \mathbf{a}^\perp . The radius of the fat strut \mathbf{a} is therefore equal to the length of the shortest vector in the lattice $\Lambda_{\mathbf{a}}$ obtained by projecting \mathbb{Z}^n into \mathbf{a}^\perp .

Given a lower bound l_0 on the length of a strut, our problem is to determine \mathbf{a} with $\|\mathbf{a}\| > l_0$ such that $r(\mathbf{a})$ is maximized. The main obstacle to solving this problem is determining a basis for $\Lambda_{\mathbf{a}}$, and finding a shortest vector in this lattice. We note that the shortest lattice vector problem is known to be a difficult problem [8], a fact that is used as justification for lattice based cryptosystems.

III. GROUNDWORK

Let $\mathbf{a} = (1, a_1, a_2, \dots, a_{n-1}) \in \mathbb{Z}^n$. Let $\Lambda_{\mathbf{a}}$ be the lattice obtained by projecting \mathbb{Z}^n into the subspace \mathbf{a}^\perp and let $\Lambda_{\mathbf{a}}^*$ denote its dual lattice. The dual of a lattice $\Lambda \subset \mathbb{R}^n$ is the lattice $\Lambda^* := \{\mathbf{x} \in \mathbb{R}^n, \langle \mathbf{x}, \boldsymbol{\lambda} \rangle \in \mathbb{Z} \forall \boldsymbol{\lambda} \in \Lambda\}$. The Gram matrix of Λ^* is the inverse of the Gram matrix of Λ and if Λ has a square generator matrix \mathbf{M} , then the generator matrix for Λ^* is $(\mathbf{M}^{-1})^{tr}$ [3]. In this section (i) we show that $\Lambda_{\mathbf{a}}^* = \mathbb{Z}^n \cap \mathbf{a}^\perp$, (ii) we construct a basis for the lattice $\Lambda_{\mathbf{a}}^*$ and (iii) prove that the minimum distance of a lattice is a continuous function of its Gram matrix.

First consider the lattice obtained by projecting \mathbb{Z}^n into \mathbf{a}^\perp . The resulting lattice $\Lambda_{\mathbf{a}}$ is the set of points $\mathbf{x}\mathbf{P}_{\mathbf{a}}$, where $\mathbf{x} \in \mathbb{Z}^n$ and

$$\mathbf{P}_{\mathbf{a}} := \mathbf{I}_n - \mathbf{a}^t \mathbf{a} / \|\mathbf{a}\|^2 \quad (2)$$

is the corresponding projection matrix. The first row of $\mathbf{P}_{\mathbf{a}}$ can be expressed as an integer linear combination of the remaining $n-1$ rows of $\mathbf{P}_{\mathbf{a}}$ and the lattice $\Lambda_{\mathbf{a}}$ has rank $n-1$; hence the last $n-1$ rows of $\mathbf{P}_{\mathbf{a}}$ are a basis for $\Lambda_{\mathbf{a}}$. It is an interesting fact, and easy to check, that the $(n-1) \times (n-1)$ submatrix formed by excluding the first row and column of $\mathbf{P}_{\mathbf{a}}$ is a Gram matrix for $\Lambda_{\mathbf{a}}$. By direct calculation $\det(\Lambda_{\mathbf{a}}) = 1/\|\mathbf{a}\|^2$, i.e. the volume of a fundamental region of the projected lattice is $1/\|\mathbf{a}\|$. Thus $\Lambda_{\mathbf{a}}^*$, the dual lattice of $\Lambda_{\mathbf{a}}$, has determinant $\|\mathbf{a}\|^2$. Now consider the lattice obtained by the intersection of \mathbb{Z}^n and \mathbf{a}^\perp . The first $n-1$ rows of the unimodular matrix

$$\begin{pmatrix} \mathbf{M}_{\mathbf{a}} \\ -\mathbf{a}/\|\mathbf{a}\|^2 \end{pmatrix} := \begin{pmatrix} -a_1 & 1 & 0 & \dots & 0 \\ -a_2 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ -a_{n-1} & 0 & \dots & 0 & 1 \\ \frac{-1}{\|\mathbf{a}\|^2} & \frac{-a_1}{\|\mathbf{a}\|^2} & \frac{-a_2}{\|\mathbf{a}\|^2} & \dots & \frac{-a_{n-1}}{\|\mathbf{a}\|^2} \end{pmatrix} \quad (3)$$

span \mathbf{a}^\perp , and if $\mathbf{x} \in \mathbb{Z}^n$ lies in \mathbf{a}^\perp , then it can be checked that \mathbf{x} can be written as an integer linear combination of the rows of

2	3	4	5	6	7	8
A_2	D_3	D_4	D_5	E_6	E_7	E_8
$1/\sqrt{12}$	$1/\sqrt{32}$	$1/8$	$1/\sqrt{128}$	$1/\sqrt{192}$	$1/16$	$1/16$

Table I

DIMENSION (ROW 1), LATTICE (ROW 2), CENTER DENSITY Δ/V_n (ROW 3) FOR DENSEST LATTICE PACKINGS [3] IN DIMENSIONS 2 – 8.

$\mathbf{M}_{\mathbf{a}}$. Thus $\mathbf{M}_{\mathbf{a}}$ is a basis for the lattice $\mathbb{Z}^n \cap \mathbf{a}^\perp$, every vector of which has an integer valued inner product with every vector of $\Lambda_{\mathbf{a}}$. Further, $\det(\mathbf{M}_{\mathbf{a}}\mathbf{M}_{\mathbf{a}}^{tr}) = \|\mathbf{a}\|^2$. Thus $\mathbb{Z}^n \cap \mathbf{a}^\perp = \Lambda_{\mathbf{a}}^*$.

To see that the length of the shortest vector in a lattice varies continuously with a Gram matrix \mathbf{G} of the lattice, observe that the length of the shortest vector is $r(\mathbf{G}) := \min_{\mathbf{x} \in \mathbb{Z}^n, \mathbf{x} \neq \mathbf{0}} \mathbf{x}\mathbf{G}\mathbf{x}^{tr}$. For given \mathbf{x} , $\mathbf{x}\mathbf{G}\mathbf{x}^{tr}$ is continuously dependent on \mathbf{G} . This implies that $r(\mathbf{G})$ is a continuous function of \mathbf{G} .

IV. A FUNDAMENTAL CONSTRAINT

The radius of a fat strut $\mathbf{a} \in \mathbb{Z}^n$ is given by

$$r(\mathbf{a}) := \min_{\mathbf{n} \in \mathbb{Z}^n} \min_{t \in \mathbb{R}} \|\mathbf{a}t - \mathbf{n}\|, \quad (4)$$

where the outer minimization is over vectors \mathbf{n} which are not multiples of \mathbf{a} . The inner minimum in (4) is achieved by the value of t for which $\langle \mathbf{n} - t\mathbf{a}, \mathbf{a} \rangle = 0$ and is equal to the length of the vector obtained by projecting \mathbf{n} into the subspace \mathbf{a}^\perp . The radius of the fat strut \mathbf{a} is therefore equal to the length of the shortest vector in the lattice $\Lambda_{\mathbf{a}}$ obtained by projecting \mathbb{Z}^n into \mathbf{a}^\perp . The determinant of $\Lambda_{\mathbf{a}}$ (the square of the volume of a fundamental region) is $\det(\Lambda_{\mathbf{a}}) = 1/\|\mathbf{a}\|^2$, and its packing density is $\Delta = V_{n-1} \|\mathbf{a}\| r(\mathbf{a})^{n-1}$, where V_n is the volume of a unit sphere in \mathbb{R}^n . Thus, the product

$$r(\mathbf{a})^{n-1} \|\mathbf{a}\| \leq \Delta_{n-1} / V_{n-1}, \quad (5)$$

where Δ_n is the highest lattice packing density attainable in \mathbb{R}^n . Thus our design problem can be reduced to one of selecting \mathbf{a} such that $\Lambda_{\mathbf{a}}$ has the largest possible packing density.

The densest lattice packings in dimensions $n \leq 8$ are known and are summarized in Table I, based on Table 1.2 in [3]. For $n = 3$ this table tells us that $\mathbf{a} \in \mathbb{Z}^3$ should be chosen so that $\Lambda_{\mathbf{a}}$ is close to the hexagonal lattice A_2 , which has packing density $\pi/\sqrt{12}$. Similar remarks hold for higher dimensions. However we have an additional constraint, namely that our lattices must be obtained by projecting \mathbb{Z}^n into one lower dimension. Thus it is not clear that the optimal packing densities stated in Table I can be achieved. We settle this question for general integer $n > 2$ by giving an explicit construction.

For dimensions $n \geq 9$, $n \neq 24$, the optimal lattice packing densities are as yet unknown. However, in 1905, Minkowski made a conjecture that there exists a lattice $\Lambda \subset \mathbb{R}^n$, with packing density [3]

$$\Delta \geq \zeta(n)/2^{n-1}, \quad (6)$$

where $\zeta(n) = \sum_{k=1}^{\infty} 1/k^n$ is the Riemann zeta-function. The conjecture was proved by Hlawka in 1944 [6] (see also [4]).

The *Minkowski-Hlawka* theorem is proved by an averaging over a general class of lattices.

An achievability result, very much in the spirit of the Minkowski-Hlawka bound, though using only elementary geometric arguments, was proved in [13]. That result proved the existence of lattices with packing densities that are almost as good as (6), but the ratio of the packing density obtained there to the Minkowski-Hlawka packing density went to zero at the rate $1/\sqrt{n}$ in the limit $n \rightarrow \infty$. Since the publication of that work we have refined the result so that the ratio goes to unity, in the limit of large dimension. This refined result is stated in Sec. VIII.

V. AN EXAMPLE

We illustrate the nature of the calculations involved with a simple example. Let $n = 3$ and let $\mathbf{a} = (1, a, b)$. The lattice $\Lambda_{\mathbf{a}}$, obtained by projecting \mathbb{Z}^n into \mathbf{a}^\perp is the dual of the lattice with basis vectors $\mathbf{v}_a = (-a, 1, 0)$ and $\mathbf{v}_b = (-b, 0, 1)$. Suppose that we wish to choose \mathbf{a} such that $\Lambda_{\mathbf{a}}^*$ is close to a lattice with Gram matrix $(1, P; P, Q)$. The main problem is that $\{\mathbf{v}_a, \mathbf{v}_b\}$ is in general not a reduced basis for $\Lambda_{\mathbf{a}}^*$. Instead we choose to work with the basis $\{\mathbf{v}_a, \tilde{\mathbf{v}}_b = \mathbf{v}_b - \alpha \mathbf{v}_a\}$, for an unknown integer α . The Gram matrix for this basis after normalizing by the $(1, 1)$ term is given by

$$\mathbf{G} = \begin{pmatrix} 1 & \frac{ab}{1+a^2} - \alpha \\ \frac{ab}{1+a^2} - \alpha & \frac{1+b^2}{1+a^2} - \frac{2\alpha ab}{1+a^2} + \alpha^2 \end{pmatrix}. \quad (7)$$

This leads to the following system of simultaneous nonlinear diophantine equations

$$\begin{aligned} P &= \frac{ab}{1+a^2} - \alpha, \\ Q &= \frac{1+b^2}{1+a^2} - \frac{2\alpha ab}{1+a^2} + \alpha^2 \end{aligned} \quad (8)$$

which must be solved approximately in order to obtain a family of solutions $\{a, b, \alpha\}$.

In general, we must solve a system of $\binom{n}{2} - 1$ diophantine equations. We worked out several examples in in dimensions $n > 3$ and also searched for good solutions using a computer. Our findings have led to the lifting construction which is described in the next section.

VI. LIFTING CONSTRUCTION

In this section, we present a general construction for a vector $\mathbf{a} = (1, a_1, a_2, \dots, a_{n-1}) \in \mathbb{Z}^n$ such that the lattice $\Lambda_{\mathbf{a}}^* = \mathbb{Z}^n \cap \mathbf{a}^\perp$, the dual of the projected lattice $\Lambda_{\mathbf{a}}$, approximates Λ_t^* the dual of the target lattice Λ_t . It is assumed, without loss of generality, that a lattice basis is available in triangular form. The construction is presented in the *Lifting* theorem.

Theorem 1: (Lifting Theorem) Let the rows of the lower triangular matrix $\mathbf{M}_t^* = (m_{i,j})$ form a basis for Λ_t^* , the dual of the target lattice $\Lambda_t \in \mathbb{R}^{n-1}$. Let $\mathbf{G}_t^* = (\mathbf{M}_t^* (\mathbf{M}_t^*)^{tr})$ be

the target Gram matrix. Let \mathbf{M}_l^* , be given by

$$\mathbf{M}_l^* = -[w(\mathbf{M}_t^* \ \mathbf{0})] + (\mathbf{0} \ \mathbf{I}_{n-1}) = \begin{pmatrix} -[wm_{1,1}] & 1 & 0 & \dots & 0 \\ -[wm_{2,1}] & -[wm_{2,2}] & 1 & 0\dots & 0 \\ \vdots & \vdots & & \ddots & \\ -[wm_{n-1,1}] & -[wm_{n-1,2}] & \dots & -[wm_{n-1,n-1}] & 1 \end{pmatrix} \quad (9)$$

where $\mathbf{0}$ is the $(n-1) \times 1$ all-zero column vector. Let

$$\tilde{\mathbf{M}}_l^* = \begin{pmatrix} -a_1 & 1 & 0 & \dots & 0 \\ -a_2 & 0 & 1 & 0\dots & 0 \\ \vdots & 0 & 0 & \ddots & \vdots \\ -a_{n-2} & 0 & \dots & 0 & 1 & 0 \\ -a_{n-1} & 0 & 0 & \dots & 0 & 1 \end{pmatrix} \quad (10)$$

be obtained by applying elementary row operations to \mathbf{M}_l^* . The lattice $\Lambda_{\mathbf{a}}^*$, with $\mathbf{a} = (1, a_1, a_2, \dots, a_{n-1})$ has a Gram matrix that converges element-wise to \mathbf{G}_t^* , the given Gram matrix of Λ_t^* , as $w \rightarrow \infty$.

Proof: It follows from (3) and the discussion surrounding it that $\tilde{\mathbf{M}}_l^*$ in (10) is a basis for $\Lambda_{\mathbf{a}}^*$. By construction, $\tilde{\mathbf{M}}_l^*$ is obtained from \mathbf{M}_l^* by elementary row operations. Let $\mathbf{G}_w^* := \mathbf{M}_l^* (\mathbf{M}_l^*)^{tr} / w^2$. Then

$$\mathbf{G}_w^* = \mathbf{G}_t^* + \mathbf{\Gamma}_w / w^2 \quad (11)$$

where the polynomial-in- w entries of the $n \times n$ matrix $\mathbf{\Gamma}_w$ are of highest degree 1. Thus $\mathbf{\Gamma}_w / w^2 \rightarrow 0$ as $w \rightarrow \infty$. ■

A. Formulas

Formulas are given for several well-known target lattices Λ_t with good packing densities.

Target Lattice $\Lambda_t = A_2$: We choose as our basis, the rows of the matrix $[1, 0; 1/2, \sqrt{3}/2]$ (note that A_2 is self-dual). Then $\mathbf{M}_l^* = \begin{pmatrix} -w & 1 & 0 \\ -w/2 & -[w\sqrt{3}/2] & 1 \end{pmatrix} = \begin{pmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \end{pmatrix}$. With w even, and $m = [w\sqrt{3}/2]$ the Gram matrix for the lattice $\Lambda_{\mathbf{a}}^*$ corresponding to the strut $\mathbf{a} = (1, w, mw + w/2)$ converges to $[1, 1/2; 1/2, 1]$.

Target Lattice $\Lambda_t = D_n, n \geq 3$: Applying the Lifting theorem to the following triangular basis for D_n^* , [3],

$$\mathbf{M} = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & & \ddots & 0 & 0 \\ \vdots & & & 1 & 0 \\ 1/2 & 1/2 & \dots & \dots & 1/2 \end{pmatrix} \quad (12)$$

we obtain

$$\mathbf{a}_n = \left(1, 2w, (2w)^2, \dots, (2w)^{n-1}, \frac{w((2w)^n - 1)}{(2w - 1)} \right). \quad (13)$$

Target Lattice $\Lambda_t = E_8$: This is also a self-dual lattice. Using the triangular basis (Equation (99), [3]), $\mathbf{a} =$

$(1, a_1, a_2, \dots, a_8)$ is given by

$$\begin{aligned} a_1 &= 2w; \\ a_2 &= 2w^2 - w; \\ a_i &= w(a_{i-1} - a_{i-2}), \quad i = 3, 4, \dots, 7; \\ a_8 &= (w/2) \left(\sum_{i=1}^7 a_i + 1 \right) \end{aligned} \quad (14)$$

for w even.

Target Lattice $\Lambda_t = \Lambda_{24}$ (**Leech lattice**): From ([3], Fig. 4.12) $\mathbf{a} = (1, a_1, a_2, \dots, a_{24})$ is given by computing a_i , in increasing order of i , according to the rules

$$\begin{aligned} a_1 &= 8w; \\ a_i &= 4w(a_{i-1} + 1), \quad i = 2 - 7, 9 - 11, 13, 17; \\ a_i &= 2w \left(\sum_{j \in S_i} a_j + 1 \right), \quad i = 8, 12, 14, 15, 16, 18, 19, \\ &\quad 20, 21, 22, 23; \\ a_{24} &= w \left(\sum_{i=1}^{23} a_i - 3 \right); \end{aligned} \quad (15)$$

where $S_8 = \{1, 2, \dots, 7\}$, $S_{12} = \{1, 2, 3, 8, 9, 10, 11\}$, $S_{14} = \{1, 4, 5, 8, 9, 12, 13\}$, $S_{15} = \{2k, 1 \leq k \leq 7\}$, $S_{16} = \{3, 4, 7, 8, 11, 12, 15\}$, $S_{18} = \{2, 4, 7, 8, 9, 16, 17\}$, $S_{19} = \{3, 4, 5, 8, 10, 16, 18\}$, $S_{20} = \{1, 4, 6, 8, 11, 16, 19\}$, $S_{21} = \{1, 2, 3, 4, 8, 12, 16, 20\}$, $S_{22} = \{8, 9, 12, 13, 16, 17, 20, 21\}$, $S_{23} = \{2k, k = 4, 5, \dots, 11\}$.

VII. AN APPLICATION TO BANDWIDTH EXPANSION MAPS

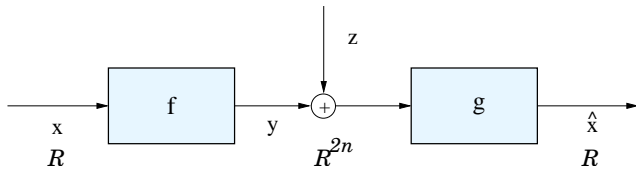


Figure 2. Communication system where the fat strut problem arises.

The fat strut problem arises when attempting to optimize the performance of the communication system illustrated in Fig. 2. This system was studied in [11], [12], and is a model for a non-linear analog communication system studied by Shannon [10]. The codes that we use are related to certain spherical codes which underlie cyclic group codes, studied earlier by Biglieri and Elia [1]. A continuous-alphabet random variable is to be transmitted over an independent vector Gaussian channel of dimension $2n$. An input $x \in [-1/2, 1/2]$ is mapped by an encoder $f: \mathbb{R} \rightarrow \mathbb{R}^{2n}$ to a vector $\mathbf{y} = f(x)$. The mapping is given by $f(x) = \alpha(v_0(x), v_1(x), \dots, v_{n-1}(x))$, where $v_i(x) = (1/\sqrt{n})(\cos \sqrt{n}a_i x, \sin \sqrt{n}a_i x)$, $i = 0, 1, \dots, n-1$, $\alpha \in \mathbb{R}$ is a scale factor chosen to satisfy a power constraint and $\mathbf{a} = (a_0, a_1, \dots, a_{n-1}) \in \mathbb{Z}^n$. The image of $[-1/2, 1/2]$ under f is a curve on a torus contained in a sphere in \mathbb{R}^{2n} . The decoder observes a noisy version of the transmitted signal \mathbf{y} and computes \hat{x} , an estimate of x chosen to minimize $E[(X - \hat{X})^2]$, the reconstruction mean squared error (mse).

The performance of this system is determined by two geometric parameters of the curve, the amount by which the length is increased, or its *stretch*, $\|\dot{f}(x)\| = (2\pi/\sqrt{n})\|\mathbf{a}\|$ (which in this case is independent of x) and its *minimum distance*.

Nonlinear modulation systems exhibit a threshold effect, in which the mse climbs rapidly when the channel signal-to-noise ratio drops below a specific value. A geometrical explanation is that when the noise variance exceeds a threshold value, there is a greater likelihood of demodulating to an incorrect fold of the curve, which leads to large decoding errors. Thus the threshold behavior is affected by the minimum distance of the curve, loosely defined as the minimum distance between distinct folds of the curve in \mathbb{R}^{2n} . Let this minimum distance be denoted by $R(\mathbf{a})$. The minimum distance is related to $r(\mathbf{a})$, the radius of the fat strut \mathbf{a} given in (1) by the following argument.

Let $\mathbf{x} = (x_1, x_2, \dots, x_n)$. Upon defining the map $\Phi(\mathbf{x}) = (v_1(x_1), v_2(x_2), \dots, v_n(x_n))$ it follows that $f(t) = \Phi(\frac{2\pi}{\sqrt{n}}\mathbf{a}t)$. By using the fact that the map $\Phi: \mathbb{R}^n \rightarrow \mathbb{R}^{2n}$ is a local isometry, it was shown in [11] that

$$\frac{4}{n} \sin^2 \left(\frac{\pi r(\mathbf{a})}{2} \right) \leq R^2(\mathbf{a}) \leq 4 \sin^2 \left(\frac{\pi r(\mathbf{a})}{2\sqrt{n}} \right). \quad (16)$$

This suggests that a lower bound on $R(\mathbf{a})$ may be obtained by constraining $r(\mathbf{a})$ from below and leads to the following problem formulation: choose \mathbf{a} such that $\|\mathbf{a}\|$ is maximized subject to $r(\mathbf{a}) > r_0$, for some constraint r_0 . This is precisely the fat strut problem.

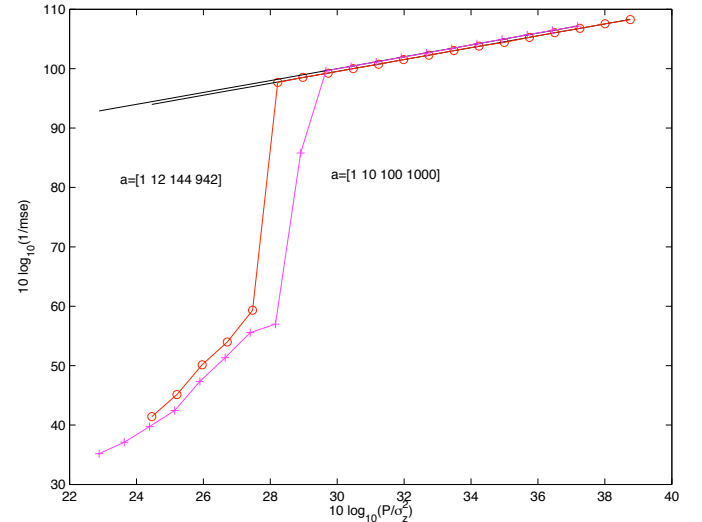


Figure 3. Performance improvement using the lifting construction. We compare the performance of $\mathbf{a}=[1, 12, 144, 942]$, (Equation (13) with $w = 6$), with the exponential sequence $\mathbf{a} = [1, a, a^2, a^3]$, $a = 10$, [11]. P is the transmitted power and σ_z^2 is the noise variance.

A simulation result is provided for $n = 4$, target lattice $\Lambda_t = D_3$, and is compared to the exponential strut $\mathbf{a} = (1, a, a^2, a^3)$. Based on a minimum distance calculation performed in [11] it can be shown that the packing density of the lattice $\Lambda_{\mathbf{a}}$

associated with the exponential strut converges to that of the cubic lattice as $n \rightarrow \infty$. Performance improvements, are clearly seen in Fig. 3. The simulation was based on 40,000 independent trials.

VIII. REFINEMENT OF THE ACHIEVABLE BOUND IN [13]

For general dimensions a nonconstructive lower bound for the packing density of a projected lattice was derived using an averaging argument in [13]. We have since obtained a sharper version of this bound; one that closes the gap between the Minkowski-Hlawka achievable lower bound on lattice packing densities and the packing densities of lattices $\Lambda_{\mathbf{a}}$ that are obtained by projecting \mathbb{Z}^n into \mathbf{a}^\perp . Due to a shortage of space, and to avoid repetition, we will present the sharper result without proof. Details will appear in a full version of the paper that is in preparation.

Let $d(\mathbf{x}, \mathcal{L}_{\mathbf{a}}) := \min_t \|\mathbf{x} - t\mathbf{a}\|$ be the minimum distance between the point \mathbf{x} and the line $\mathcal{L}_{\mathbf{a}} := \{t\mathbf{a}, t \in \mathbb{R}\}$. Given $r > 0$ and $\mathbf{a} \in \mathbb{Z}^n$, let $N(\mathbf{a}, r)$ be the number of primitive vectors \mathbf{x} in \mathbb{Z}^n with length at most $\sqrt{1 + \|\mathbf{a}\|^2}/4$ and $d(\mathbf{x}, \mathcal{L}_{\mathbf{a}}) < r$. Let $\bar{N}(r, l, \delta)$ be the average of $N(\mathbf{a}, \epsilon)$ calculated with a uniform distribution over primitive vectors \mathbf{a} in a shell of thickness $l\delta$ and inner radius $l(1 - \delta)$. If $\bar{N}(r, l, \delta) < 1$ then there exists primitive \mathbf{a} , $\|\mathbf{a}\| \in (l(1 - \delta), l]$ such that $N(\mathbf{a}, r) = 0$. In other words, if $\bar{N}(r, l, \delta) < 1$ a strut exists with length $> l(1 - \delta)$ and radius r .

In [13], it was shown that¹

$$\bar{N}(r, l, \delta) \leq \frac{nV_n}{2} r^{n-1} \frac{l}{2} (1 + o_l(1)). \quad (17)$$

Based on this, the existence of struts which achieve packing densities

$$\Delta_{n-1} \geq \frac{V_{n-1}}{n2^{n-2}V_n} \sim \frac{1}{\sqrt{2\pi n}2^{n-2}} \quad (18)$$

was proved.

Through a refinement of our earlier proof we can show that for large l

$$\bar{N}(r, l, \delta) \leq V_{n-1} \frac{r^{n-1}}{\sqrt{1-r^2}} \frac{l}{2} (1 + o_l(1)). \quad (19)$$

Since a strut of length l and radius r exists if $\bar{N}(r, l, \delta) < 1$, and since we know that $r \rightarrow 0$ as $l \rightarrow \infty$ we are able to establish that lattices with packing density

$$\Delta_{n-1} = 2^{-(n-2)}$$

can be obtained by projecting \mathbb{Z}^n into a subspace orthogonal to a primitive vector in \mathbb{Z}^n whose norm is suitably large. This compares favorably with $\frac{\zeta(n-1)}{2^{n-2}}$, which is the Minkowski-Hlawka bound (6) for the packing density achievable by unrestricted lattices (note that $\zeta(n) \rightarrow 1$ as $n \rightarrow \infty$).

IX. SUMMARY

The *fat strut* problem is posed, motivated by a question in communication theory. A general construction method, referred to as the *lifting construction*, is presented. This

construction gives us a formula for a family of struts which achieve the packing density of a target lattice as the length of the strut grows large. An example illustrating the benefit of this construction in a communication problem is also presented. Finally, a refined non-constructive achievability result is stated.

REFERENCES

- [1] E. Biglieri and M. Elia. Cyclic group codes for the Gaussian channel. *IEEE Trans. Inform. Theory*, 22:624–629, Sept. 1976.
- [2] J. W. S. Cassels. *An Introduction to the Geometry of Numbers*. Springer-Verlag, 1971.
- [3] J. H. Conway and N. J. A. Sloane. *Sphere Packings, Lattices and Groups*. Springer-Verlag, New York, 3rd ed., 1993.
- [4] P. M. Gruber and C. G. Lekkerkerker. *Geometry of Numbers*. North-Holland, Amsterdam, 2nd ed., 1987.
- [5] A. Heppes. Ein satz über gitterförmige kugelpackungen. *Ann. Univ. Sci. Budapest. Eötvös Sect. Math.*, 3–4:89–90, 1960/1961.
- [6] E. Hlawka. Zur geometrie der zahlen. *Math. Zietschr.*, 49:285–312, 1943.
- [7] J. Horváth. Über die durchsichtigkeit gitterförmiger kugelpackungen. *Studia Sci. Math. Hungar.*, 5:421–426, 1970.
- [8] D. Micciancio. The shortest vector in a lattice is hard to approximate to within some constant. *SIAM J. Comput.*, 30:2008–2035, 2001.
- [9] B. Z. Moroz. On the number of primitive lattice points in plain domains. *Mh. Math.*, 99:37–42, 1985.
- [10] C. E. Shannon. Communication in the presence of noise. *Proc. IRE*, 37:30–41, Jan. 1949.
- [11] V. A. Vaishampayan and S. I. R. Costa. Curves on a sphere, shift-map dynamics, and error control for continuous alphabet sources. *IEEE Trans. Inform. Theory*, 49(7):1658–1672, July 2003.
- [12] V. A. Vaishampayan, N. J. A. Sloane and S. I. R. Costa. Dynamical systems, curves and coding for continuous alphabet sources. In *Proceedings, 2002 Information Theory Workshop*, pages 111–114, October 2002.
- [13] N. J. A. Sloane, V. A. Vaishampayan and S. I. R. Costa. Fat Struts: Constructions and a Bound. In *Proceedings, 2009 Information Theory Workshop*, pages 333–337, October 2009.

¹We use the notation $o_l(1)$ when $\lim_{l \rightarrow \infty} o_l(1) = 0$.