Lattice Coding I: From Theory To Application

Amin Sakzad
Dept of Electrical and Computer Systems Engineering
Monash University
amin.sakzad@monash.edu

Oct. 2013

Motivation I: Geometry of Numbers

Initiated by Minkowski and studies convex bodies and integer points in $\mathbb{R}^n$.

1. Diophantine Approximation,
2. Functional Analysis

Examples Approximating real numbers by rationals, sphere packing problem, covering problem, factorizing polynomials, etc.

Motivation II: Telecommunication

1. Channel Coding Problem,
2. Quantization Problem

Examples Signal constellations, space-time coding, lattice-reduction-aided decoders, relaying protocols, etc.

Definition

A set $\Lambda \subseteq \mathbb{R}^n$ of vectors called discrete *if there exist a positive real number β such that any two vectors of Λ have distance at least β.*

Definition

A set $\Lambda \subseteq \mathbb{R}^n$ of vectors called discrete if there exist a positive real number β such that any two vectors of Λ have distance at least β.

Definition

An infinite discrete set $\Lambda \subseteq \mathbb{R}^n$ is called a lattice if Λ is a group under addition in $\mathbb{R}^n$.

Every lattice is generated by the integer combination of some linearly independent vectors $\mathbf{g}_1, \ldots, \mathbf{g}_m \in \mathbb{R}^n$, i.e.,

$$\Lambda = \{u_1\mathbf{g}_1 + \cdots + u_m\mathbf{g}_m : u_1, \ldots, u_m \in \mathbb{Z}\}.$$

Every lattice is generated by the integer combination of some linearly independent vectors $\mathbf{g}_1, \ldots, \mathbf{g}_m \in \mathbb{R}^n$, i.e.,

$$\Lambda = \{u_1\mathbf{g}_1 + \cdots + u_m\mathbf{g}_m : u_1, \ldots, u_m \in \mathbb{Z}\}.$$

Definition

The $m \times n$ matrix $\mathbf{G} = (\mathbf{g}_1, \ldots, \mathbf{g}_m)$ which has the generator vectors as its rows is called a generator matrix of Λ. A lattice is called full rank if $m = n$.

Every lattice is generated by the integer combination of some linearly independent vectors $\mathbf{g}_1, \ldots, \mathbf{g}_m \in \mathbb{R}^n$, i.e.,

$$\Lambda = \{u_1\mathbf{g}_1 + \cdots + u_m\mathbf{g}_m : u_1, \ldots, u_m \in \mathbb{Z}\}.$$

Definition

The $m \times n$ matrix $\mathbf{G} = (\mathbf{g}_1, \ldots, \mathbf{g}_m)$ which has the generator vectors as its rows is called a generator matrix of Λ. A lattice is called full rank if $m = n$.

Note that

$$\Lambda = \{\mathbf{x} = \mathbf{u}\mathbf{G} : \mathbf{u} \in \mathbb{Z}^n\}.$$

Definition

The *Gram matrix* *of* Λ *is*

$$\mathbf{M} = \mathbf{G}\mathbf{G}^T.$$

Definition

The Gram matrix of Λ *is*

$$\mathbf{M} = \mathbf{G}\mathbf{G}^T.$$

Definition

The minimum distance of Λ *is defined by*

$$d_{\min}(\Lambda) = \min\{\|\mathbf{x}\| : \mathbf{x} \in \Lambda \setminus \{\mathbf{0}\}\},$$

where $\|\cdot\|$ *stands for Euclidean norm.*

Definition

The determinate (volume) of an n-dimensional lattice Λ, $\det(\Lambda)$, is defined as

$$\det[\mathbf{G}\mathbf{G}^T]^{\frac{1}{2}}.$$

Definition

The coding gain of a lattice Λ is defined as:

$$\gamma(\Lambda) = \frac{d_{\min}^2(\Lambda)}{\det(\Lambda)^{\frac{2}{n}}}.$$

Geometrically, $\gamma(\Lambda)$ measures the increase in the density of Λ over the lattice $\mathbb{Z}^n$.

Definition

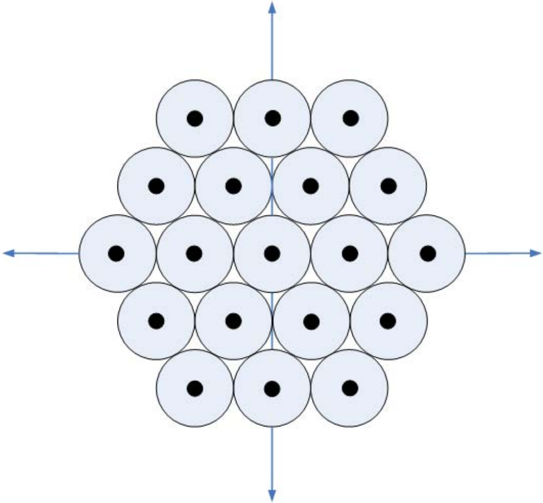
The set of all vectors in $\mathbb{R}^n$ *whose inner product with all elements of* Λ *is an integer form the dual lattice* Λ^*.

Definition

The set of all vectors in $\mathbb{R}^n$ whose inner product with all elements of Λ is an integer form the dual lattice Λ^*.

For a lattice Λ, with generator matrix $\mathbf{G}$, the matrix $\mathbf{G}^{-T}$ forms a basis matrix for Λ^*.

Three examples



Barens-Wall Lattices

- Let

$$\mathbf{G} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Barens-Wall Lattices

- Let

$$\mathbf{G} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

- Let $\mathbf{G}^{\otimes m}$ denote the m-fold Kronecker (tensor) product of $\mathbf{G}$.

Barens-Wall Lattices

- Let

$$\mathbf{G} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

- Let $\mathbf{G}^{\otimes m}$ denote the m-fold Kronecker (tensor) product of $\mathbf{G}$.
- A basis matrix for Barnes-Wall lattice $\mathcal{BW}_n$, $n = 2^m$, can be formed by selecting the rows of matrices $\mathbf{G}^{\otimes m}, \ldots, 2^{\lfloor \frac{m}{2} \rfloor}\mathbf{G}^{\otimes m}$ which have a square norm equal to 2^{m-1} or 2^m.

Barens-Wall Lattices

- Let
$$\mathbf{G} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$
- Let $\mathbf{G}^{\otimes m}$ denote the m-fold Kronecker (tensor) product of $\mathbf{G}$.
- A basis matrix for Barnes-Wall lattice $\mathcal{BW}_n$, $n = 2^m$, can be formed by selecting the rows of matrices $\mathbf{G}^{\otimes m}, \ldots, 2^{\lfloor \frac{m}{2} \rfloor}\mathbf{G}^{\otimes m}$ which have a square norm equal to 2^{m-1} or 2^m.
- $d_{\min}(\mathcal{BW}_n) = \sqrt{\frac{n}{2}}$ and $\det(\mathcal{BW}_n) = (\frac{n}{2})^{\frac{n}{4}}$, which confirms that $\gamma(\mathcal{BW}_n) = \sqrt{\frac{n}{2}}$.

$\mathcal{D}_n$ Lattices

- For $n \geq 3$, $\mathcal{D}_n$ can be represented by the following basis matrix:

$$\mathbf{G} = \begin{pmatrix} -1 & -1 & 0 & \cdots & 0 \\ 1 & -1 & 0 & \cdots & 0 \\ 0 & 1 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -1 \end{pmatrix}.$$

$\mathcal{D}_n$ Lattices

- For $n \geq 3$, $\mathcal{D}_n$ can be represented by the following basis matrix:

$$\mathbf{G} = \begin{pmatrix} -1 & -1 & 0 & \cdots & 0 \\ 1 & -1 & 0 & \cdots & 0 \\ 0 & 1 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -1 \end{pmatrix}.$$

- We have $\det(\mathcal{D}_n) = 2$ and $d_{\min}(\mathcal{D}_n) = \sqrt{2}$, which result in $\gamma(\mathcal{D}_n) = 2^{\frac{n-2}{n}}$.

- Sphere Packing Problem,
- Covering Problem,
- Quantization,
- Channel Coding Problem.

Let us put a sphere of radius $\rho = d_{\min}(\Lambda)/2$ at each lattice point Λ.

Let us put a sphere of radius $\rho = d_{\min}(\Lambda)/2$ at each lattice point Λ.

Definition

The ***density*** *of Λ is defined as*

$$\Delta(\Lambda) = \frac{\rho^n V_n}{\det(\Lambda)},$$

where V_n is the volume of an n-dimensional sphere with radius 1.

Note that

$$V_n = \frac{\pi^{n/2}}{(n/2)!}.$$

Definition

The *kissing number* $\tau(\Lambda)$ *is the number of spheres that touches one sphere.*

Definition

The *kissing number* $\tau(\Lambda)$ *is the number of spheres that touches one sphere.*

Definition

The *center density* *of* Λ *is then* $\delta = \frac{\Delta}{V_n}$*.*

Note that $4\delta(\Lambda)^{2/n} = \gamma(\Lambda)$.

Definition

The kissing number $\tau(\Lambda)$ *is the number of spheres that touches one sphere.*

Definition

The center density of Λ *is then* $\delta = \frac{\Delta}{V_n}$.

Note that $4\delta(\Lambda)^{2/n} = \gamma(\Lambda)$.

Definition

The Hermite's constant γ_n *is the highest attainable coding gain of an* n*-dimensional lattice.*

Lattice Sphere Packing Problem

Find the densest lattice packing of equal nonoverlapping, solid spheres (or balls) in n-dimensional space.

Summary of Well-Known Results

Theorem

- *For large n's we have*

$$\frac{1}{2\pi e} \leq \frac{\gamma_n}{n} \leq \frac{1.744}{2\pi e},$$

Summary of Well-Known Results

Theorem

- *For large n's we have*

$$\frac{1}{2\pi e} \leq \frac{\gamma_n}{n} \leq \frac{1.744}{2\pi e},$$

- *The densest lattice packings are known for dimensions 1 to 8 and $12, 16,$ and 24.*

Let us supose a set of spheres of radius R covers $\mathbb{R}^n$

Let us supose a set of spheres of radius R covers $\mathbb{R}^n$

Definition

The ***thickness*** *of* Λ *is defined as*

$$\Theta(\Lambda) = \frac{R^n V_n}{\det(\Lambda)}$$

Let us supose a set of spheres of radius R covers $\mathbb{R}^n$

Definition

The *thickness* *of* Λ *is defined as*

$$\Theta(\Lambda) = \frac{R^n V_n}{\det(\Lambda)}$$

Definition

The *normalized thickness* *of* Λ *is then* $\theta(\Lambda) = \frac{\Theta}{V_n}$.

Lattice Covering Problem

Ask for the thinnest lattice covering of equal overlapping, solid spheres (or balls) in n-dimensional space.

Summary of Well-Known Results

Theorem

- *The thinnest lattice coverings are known for dimensions* 1 *to* 5, *(all* $\mathcal{A}_n^*$*).*
- *Davenport's Construction of thin lattice coverings, (thinner than* $\mathcal{A}_n^*$ *for* $n \leq 200$*).*

Definition

For any point $\mathbf{x}$ *in a constellation* $\mathcal{A}$ *the Voroni cell* $\nu(\mathbf{x})$ *is defined by the set of points that are at least as close to* $\mathbf{x}$ *as to any other point* $\mathbf{y} \in \mathcal{A}$*, i.e.,*

$$\nu(\mathbf{x}) = \{\mathbf{v} \in \mathbb{R}^n : \|\mathbf{v} - \mathbf{x}\| \leq \|\mathbf{v} - \mathbf{y}\|, \forall \ \mathbf{y} \in \mathcal{A}\}.$$

Definition

For any point $\mathbf{x}$ *in a constellation* $\mathcal{A}$ *the Voroni cell* $\nu(\mathbf{x})$ *is defined by the set of points that are at least as close to* $\mathbf{x}$ *as to any other point* $\mathbf{y} \in \mathcal{A}$*, i.e.,*

$$\nu(\mathbf{x}) = \{\mathbf{v} \in \mathbb{R}^n : \|\mathbf{v} - \mathbf{x}\| \leq \|\mathbf{v} - \mathbf{y}\|, \forall\ \mathbf{y} \in \mathcal{A}\}.$$

We simply denote $\nu(\mathbf{0})$ by ν.

Definition

An n-dimensional quantizer is a set of points chosen in $\mathbb{R}^n$. The input $\mathbf{x}$ is an arbitrary point of $\mathbb{R}^n$; the output is the closest point to $\mathbf{x}$.

Definition

An n-dimensional quantizer is a set of points chosen in $\mathbb{R}^n$. The input $\mathbf{x}$ is an arbitrary point of $\mathbb{R}^n$; the output is the closest point to $\mathbf{x}$.

A good quantizer attempts to minimize the *mean squared error* of quantization.

Lattice Quantizer Problem

finds and n-dimentional lattice Λ for which

$$G(\nu) = \frac{\frac{1}{n}\int_{\nu} \mathbf{x} \cdot \mathbf{x} d\mathbf{x}}{\det(\nu)^{1+\frac{2}{n}}},$$

is a minimum.

Summary of Well-Known Results

Theorem

- *The optimum lattice quantizers are only known for dimensions* 1 *to* 3.
- *As* $n \to \infty$, *we have*

$$G_n \to \frac{1}{2\pi e}.$$

Summary of Well-Known Results

Theorem

- *The optimum lattice quantizers are only known for dimensions* 1 *to* 3.
- *As* $n \to \infty$, *we have*

$$G_n \to \frac{1}{2\pi e}.$$

It is worth remarking that the best n-dimensional quantizers presently known are always the duals of the best packings known.

Definition

For two points $\mathbf{x}$ *and* $\mathbf{y}$ *in* $\mathbb{F}_q^n$ *the* *Hamming distance* *is defined as*

$$d(\mathbf{x}, \mathbf{y}) = \|\{i \colon \mathbf{x}_i \neq \mathbf{y}_i\}\| .$$

Definition

For two points $\mathbf{x}$ *and* $\mathbf{y}$ *in* $\mathbb{F}_q^n$ *the Hamming distance is defined as*

$$d(\mathbf{x},\mathbf{y}) = \|\{i\colon \mathbf{x}_i \neq \mathbf{y}_i\}\|.$$

Definition

A q-ary $(n, M, d_{\min})$ *code* $\mathcal{C}$ *is a subset of* M *points in* $\mathbb{F}_q^n$*, with minimum distance*

$$d_{\min}(\mathcal{C}) = \min_{\mathbf{x}\neq\mathbf{y}\in\mathcal{C}} d(\mathbf{x},\mathbf{y}).$$

Performance Measures I

- Suppose that $\mathbf{x}$, which is in a constellation $\mathcal{A}$, is sent,
- $\mathbf{y} = \mathbf{x} + \mathbf{z}$ is received, where the components of $\mathbf{z}$ are i.i.d. based on $\mathcal{N}(0, \sigma^2)$,
- The probability of error is defined as

$$P_e(\mathcal{A}, \sigma^2) = 1 - \frac{1}{(\sqrt{2\pi}\sigma)^n} \int_{\nu} \exp\left(\frac{-\|\mathbf{x}\|^2}{2\sigma^2} \right) d\mathbf{x}.$$

Performance Measures II

Rate

Definition

The rate $\mathfrak{r}$ *of an* $(n, M, d_{\min})$ *code* $\mathcal{C}$ *is*

$$\mathfrak{r} = \frac{\log_2(M)}{n}.$$

Performance Measures II

Rate

Definition

The rate $\mathfrak{r}$ *of an* $(n, M, d_{\min})$ *code* $\mathcal{C}$ *is*

$$\mathfrak{r} = \frac{\log_2(M)}{n}.$$

The power of a transmission has a close relation with the rate of the code.

Performance Measures II

Rate

Definition

The rate $\mathfrak{r}$ *of an* $(n, M, d_{\min})$ *code* $\mathcal{C}$ *is*

$$\mathfrak{r} = \frac{\log_2(M)}{n}.$$

The power of a transmission has a close relation with the rate of the code.

Normalized Logarithmic Density

Definition

The normalized logarithmic density (NLD) of an n*-dimensional lattice* Λ *is*

$$\frac{1}{n}\log\left(\frac{1}{\det(\Lambda)}\right).$$

Performance Measures III

Capacity

Definition

The capacity of an AWGN channel with noise variance σ^2 is

$$C = \frac{1}{2}\log\left(1 + \frac{P}{\sigma^2}\right),$$

where $\frac{P}{\sigma^2}$ is called the signal-to-noise ratio.

Performance Measures III

Capacity

Definition

The capacity of an AWGN channel with noise variance σ^2 is

$$C = \frac{1}{2}\log\left(1 + \frac{P}{\sigma^2}\right),$$

where $\frac{P}{\sigma^2}$ is called the signal-to-noise ratio.

Generalized Capacity

Definition

The capacity of an "unconstrained" AWGN channel with noise variance σ^2 is

$$C_\infty = \frac{1}{2}\ln\left(\frac{1}{2\pi e\sigma^2}\right).$$

Approaching Capacity

Capacity-Achieving Codes

Definition

A $(n, M, d_{\min})$ code $\mathcal{C}$ is called capacity-achieving for the AWGN channel with noise variance σ^2, if $\mathfrak{r} = C$ when $P_e(\mathcal{C}, \sigma^2) \approx 0$.

Sphere-Bound-Achieving Lattices

Definition

An n-dimensional lattice Λ is called capacity-achieving for the unconstrained AWGN channel with noise variance σ^2, if NLD$(\Lambda) = C_\infty$ when $P_e(\Lambda, \sigma^2) \approx 0$.

Definition

The volume-to-noise ratio of a lattice Λ *over an unconstrained AWGN channel with noise variance* σ^2 *is defined as*

$$\alpha^2(\Lambda, \sigma^2) = \frac{\det(\Lambda)^{\frac{2}{n}}}{2\pi e \sigma^2}.$$

Definition

The volume-to-noise ratio of a lattice Λ over an unconstrained AWGN channel with noise variance σ^2 is defined as

$$\alpha^2(\Lambda, \sigma^2) = \frac{\det(\Lambda)^{\frac{2}{n}}}{2\pi e \sigma^2}.$$

Note that $\alpha^2(\Lambda, \sigma^2) = 1$ is equivalent to $\mathsf{NLD}(\Lambda) = C_\infty$.

Union Bound Estimate

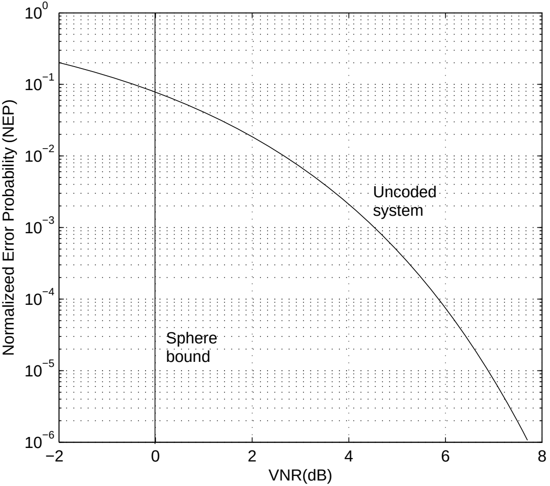
Using the formula of coding gain and $\alpha^2(\Lambda, \sigma^2)$, we obtain an estimate upper bound for the probability of error for a maximum-likelihood decoder:

$$P_e(\Lambda, \sigma^2) \leq \frac{\tau(\Lambda)}{2} \text{erfc}\left(\sqrt{\frac{\pi e}{4}\gamma(\Lambda)\alpha^2(\Lambda, \sigma^2)}\right),$$

where

$$\text{erfc(t)} = \frac{2}{\sqrt{\pi}} \int_t^\infty \exp(-t^2) dt.$$

Probability of Error versus VNR



Thanks for your attention! Friday 18 Oct. Building 72, Room 132.

Thanks for your attention! Friday 18 Oct. Building 72, Room 132.