1 Motivation

2 Preliminaries
   - Definitions
   - Three examples

3 Problems
   - Sphere Packing Problem
   - Covering Problem
   - Quantization Problem
   - Channel Coding Problem

4 Relation
   - Probability of Error versus VNR
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 $\beta$ such that any two vectors of $\Lambda$ have distance at least $\beta$. 

---

**Motivation**

**Preliminaries**

- Problem
  - 
- Problem
  - 
- Problem
  - 
- Problem
  - 

**Problems**

- Problem
  - 
- Problem
  - 
- Problem
  - 
- Problem
  -

**Relation**

- 
- 
- 

**Definitions**

**Definition**

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

---

**Lattice Coding I: From Theory To Application**

Amin Sakzad
Definitions

Definition

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

Definition

An infinite discrete set \( \Lambda \subseteq \mathbb{R}^n \) is called a lattice if \( \Lambda \) is a group under addition in \( \mathbb{R}^n \).
Every lattice is generated by the integer combination of some linearly independent vectors $g_1, \ldots, g_m \in \mathbb{R}^n$, i.e.,

$$\Lambda = \{ u_1 g_1 + \cdots + u_m g_m : u_1, \ldots, u_m \in \mathbb{Z} \}.$$
Every lattice is generated by the integer combination of some linearly independent vectors $g_1, \ldots, g_m \in \mathbb{R}^n$, i.e.,

$$\Lambda = \{u_1 g_1 + \cdots + u_m g_m : u_1, \ldots, u_m \in \mathbb{Z}\}.$$ 

**Definition**

The $m \times n$ matrix $G = (g_1, \ldots, g_m)$ which has the generator vectors as its rows is called a generator matrix of $\Lambda$. A lattice is called full rank if $m = n$. 

Lattice Coding I: From Theory To Application

Amin Sakzad
Every lattice is generated by the integer combination of some linearly independent vectors $g_1, \ldots, g_m \in \mathbb{R}^n$, i.e.,

$$\Lambda = \{u_1 g_1 + \cdots + u_m g_m : u_1, \ldots, u_m \in \mathbb{Z}\}.$$

**Definition**

The $m \times n$ matrix $G = (g_1, \ldots, g_m)$ which has the generator vectors as its rows is called a **generator matrix** of $\Lambda$. A lattice is called **full rank** if $m = n$.

Note that

$$\Lambda = \{x = uG : u \in \mathbb{Z}^n\}.$$
Definition

The Gram matrix of $\Lambda$ is

$$M = GG^T.$$
Definition

The Gram matrix of $\Lambda$ is

$$M = GG^T.$$ 

Definition

The minimum distance of $\Lambda$ is defined by

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

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

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

$$\det[GG^T]^{\frac{1}{2}}.$$
Definition

The **coding gain** of a lattice $\Lambda$ is defined as:

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

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

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

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

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

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

**Barens-Wall Lattices**

- Let $G = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.
- Let $G \otimes^m$ denote the $m$-fold Kronecker (tensor) product of $G$. 

$Lattice Coding I: From Theory To Application$
Let \( G \) denote the \( m \)-fold Kronecker (tensor) product of \( G \).

A basis matrix for Barens-Wall lattice \( BW_n \), \( n = 2^m \), can be formed by selecting the rows of matrices \( G \otimes m, \ldots, 2^{\lfloor \frac{m}{2} \rfloor} G \otimes m \) which have a square norm equal to \( 2^{m-1} \) or \( 2^m \).
Let

\[ G = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}. \]

Let \( G \otimes m \) denote the \( m \)-fold Kronecker (tensor) product of \( G \).

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

\[ d_{\min}(\mathcal{BW}_n) = \sqrt{\frac{n}{2}} \] and \( \det(\mathcal{BW}_n) = \left( \frac{n}{2} \right)^{n/4} \), which confirms that \( \gamma(\mathcal{BW}_n) = \sqrt{\frac{n}{2}} \).
For $n \geq 3$, $D_n$ can be represented by the following basis matrix:

$$
G = \begin{pmatrix}
-1 & -1 & 0 & \cdots & 0 \\
1 & -1 & 0 & \cdots & 0 \\
0 & 1 & -1 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & -1
\end{pmatrix}.
$$
For $n \geq 3$, $\mathcal{D}_n$ can be represented by the following basis matrix:

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

We have $\det(\mathcal{D}_n) = 2$ and $d_{\text{min}}(\mathcal{D}_n) = \sqrt{2}$, 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 $\Lambda$. 
Let us put a sphere of radius $\rho = d_{\min}(\Lambda)/2$ at each lattice point $\Lambda$.

**Definition**

The *density* of $\Lambda$ 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 $\Lambda$ is then $\delta = \frac{\Lambda}{V_n}$.

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

---

Lattice Coding I: From Theory To Application

Amin Sakzad
Definition

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

Definition

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

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

Definition

The **Hermite's constant** $\gamma_n$ is the highest attainable coding gain of an $n$-dimensional lattice.
Find the densest lattice packing of equal nonoverlapping, solid spheres (or balls) in $n$-dimensional space.
Summary of Well-Known Results

For large \( n \)'s we have

\[
\frac{1}{2\pi e} \leq \frac{\gamma_n}{n} \leq \frac{1.744}{2\pi e},
\]
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 suppose a set of spheres of radius $R$ covers $\mathbb{R}^n$. 
Let us suppose a set of spheres of radius $R$ covers $\mathbb{R}^n$.

**Definition**

The *thickness* of $\Lambda$ is defined as

$$\Theta(\Lambda) = \frac{R^n V_n}{\det(\Lambda)}$$
Let us suppose a set of spheres of radius $R$ covers $\mathbb{R}^n$

**Definition**

The *thickness* of $\Lambda$ is defined as

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

**Definition**

The *normalized thickness* of $\Lambda$ 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 $A_n^*$).*
- *Davenport’s Construction of thin lattice coverings, (thinner than $A_n^*$ for $n \leq 200$).*
**Definition**

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

\[
\nu(x) = \{ v \in \mathbb{R}^n : \| v - x \| \leq \| v - y \|, \forall y \in A \}.
\]
**Quantization Problem**

<table>
<thead>
<tr>
<th>Motivation</th>
<th>Preliminaries</th>
<th>Problems</th>
</tr>
</thead>
</table>

**Definition**

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

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

We simply denote $\nu(0)$ by $\nu$. 

---

*Lattice Coding I: From Theory To Application*  
Amin Sakzad
**Definition**

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

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

A good quantizer attempts to minimize the mean squared error of quantization.
finds and $n$-dimentional lattice $\Lambda$ for which

$$G(\nu) = \frac{1}{n} \int_{\nu} x \cdot x dx \left/ \det(\nu)^{1+\frac{2}{n}} \right.$$ 

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

$$G_n \to \frac{1}{2\pi e}.$$
The optimum lattice quantizers are only known for dimensions 1 to 3.

As $n \rightarrow \infty$, we have

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

It is worth remarking that the best n-dimensional quantizers presently known are always the duals of the best packings known.
For two points $x$ and $y$ in $\mathbb{F}_q^n$ the Hamming distance is defined as

$$d(x, y) = \| \{ i : x_i \neq y_i \} \|.$$
Definition

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

$$d(x, y) = \|\{i : x_i \neq y_i\}\|.$$ 

Definition

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

$$d_{\text{min}}(C) = \min_{x \neq y \in C} d(x, y).$$
Suppose that $x$, which is in a constellation $A$, is sent,

$y = x + z$ is received, where the components of $z$ are i.i.d. based on $\mathcal{N}(0, \sigma^2)$,

The **probability of error** is defined as

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

Definition

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

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

Definition

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

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

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

**Definition**

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

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

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 $\Lambda$ is

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

Definition

The capacity of an AWGN channel with noise variance $\sigma^2$ 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.
**Capacity**

**Definition**

The *capacity* of an AWGN channel with noise variance $\sigma^2$ 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 $\sigma^2$ is

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

Approaching Capacity

**Capacity-Achieving Codes**

**Definition**

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

**Sphere-Bound-Achieving Lattices**

**Definition**

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

Lattice Coding I: From Theory To Application  
Amin Sakzad
**Definition**

The *volume-to-noise ratio* of a lattice \( \Lambda \) over an unconstrained AWGN channel with noise variance \( \sigma^2 \) is defined as

\[
\alpha^2(\Lambda, \sigma^2) = \frac{\det(\Lambda)^2}{2\pi e \sigma^2}.
\]
Definition

The volume-to-noise ratio of a lattice \( \Lambda \) over an unconstrained AWGN channel with noise variance \( \sigma^2 \) 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 \( \text{NLD}(\Lambda) = C_\infty \).
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

- VNR (dB)
- Normalized Error Probability (NEP)

- Sphere bound
- Uncoded system
Thanks for your attention! Friday 18 Oct. Building 72, Room 132.
Thanks for your attention! Friday 18 Oct. Building 72, Room 132.