

An Introduction to Lattices and their Applications in Communications

Frank R. Kschischang

University of Toronto, Canada

Chen Feng

University of British Columbia — Okanagan, Canada

2018 North American School of Information Theory

Texas A&M University

College Station, TX

May 22, 2018

Acknowledgments

- Many thanks to the organizers of NASIT 2018.
- Many thanks to the IEEE Information Theory Society for its ongoing support of student events.
- Many thanks to Roberto Padovani for endowing the Padovani lecture!
- Apologies in advance for errors and omissions, particularly for work left uncited.

Outline

- ① Fundamentals
- ② Packing, Covering, Quantization, Modulation
- ③ Lattices and Linear Codes
- ④ Asymptopia
- ⑤ Communications Applications



Part 1: Lattice Fundamentals

Notation

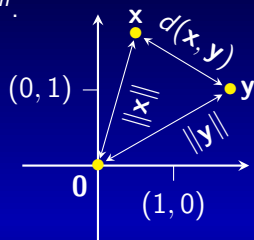
- \mathbb{C} : the **complex numbers** (a field)
- \mathbb{R} : the **real numbers** (a field)
- \mathbb{Z} : the **integers** (a ring)
- X^n : the **n -fold Cartesian product** of set X with itself;
 $X^n = \{(x_1, \dots, x_n) : x_1 \in X, x_2 \in X, \dots, x_n \in X\}$. If X is a field, then the elements of X^n are **row vectors**.
- $X^{m \times n}$: the $m \times n$ **matrices** with entries from X .
- If $(G, +)$ is a group with identity 0, then $G^* \triangleq G \setminus \{0\}$ denotes the **nonzero elements** of G .

Euclidean Space

Lattices are **discrete subgroups** (under vector addition) of finite-dimensional Euclidean spaces such as \mathbb{R}^n .

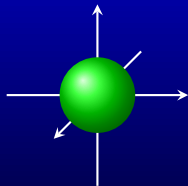
In \mathbb{R}^n we have

- an **inner product**: $\langle \mathbf{x}, \mathbf{y} \rangle \triangleq \sum_{i=1}^n x_i y_i$
- a **norm**: $\|\mathbf{x}\| \triangleq \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle}$
- a **metric**: $d(\mathbf{x}, \mathbf{y}) \triangleq \|\mathbf{x} - \mathbf{y}\|$



- Vectors \mathbf{x} and \mathbf{y} are **orthogonal** if $\langle \mathbf{x}, \mathbf{y} \rangle = 0$.
- A **ball** centered at the origin in \mathbb{R}^n is the set

$$\mathcal{B}_r = \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\| \leq r\}.$$



- If \mathcal{R} is any subset of \mathbb{R}^n , the **translation of \mathcal{R} by \mathbf{x}** is, for any $\mathbf{x} \in \mathbb{R}^n$, the set $\mathbf{x} + \mathcal{R} = \{\mathbf{x} + \mathbf{y} : \mathbf{y} \in \mathcal{R}\}$.

Lattices

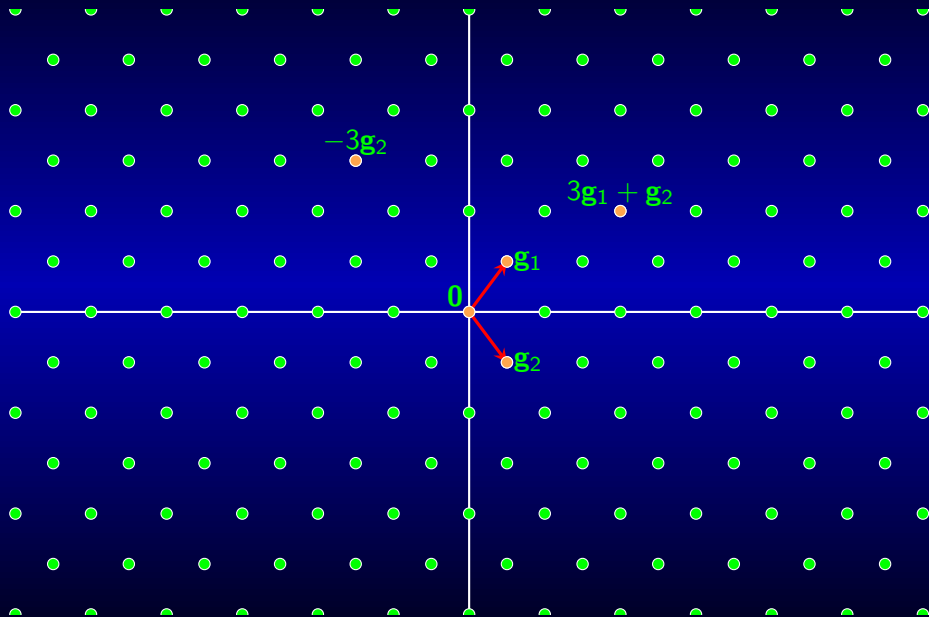
Definition

Given m linearly independent (row) vectors $\mathbf{g}_1, \dots, \mathbf{g}_m \in \mathbb{R}^n$, the **lattice** Λ generated by them is defined as the set of all integer linear combinations of the \mathbf{g}_i 's:

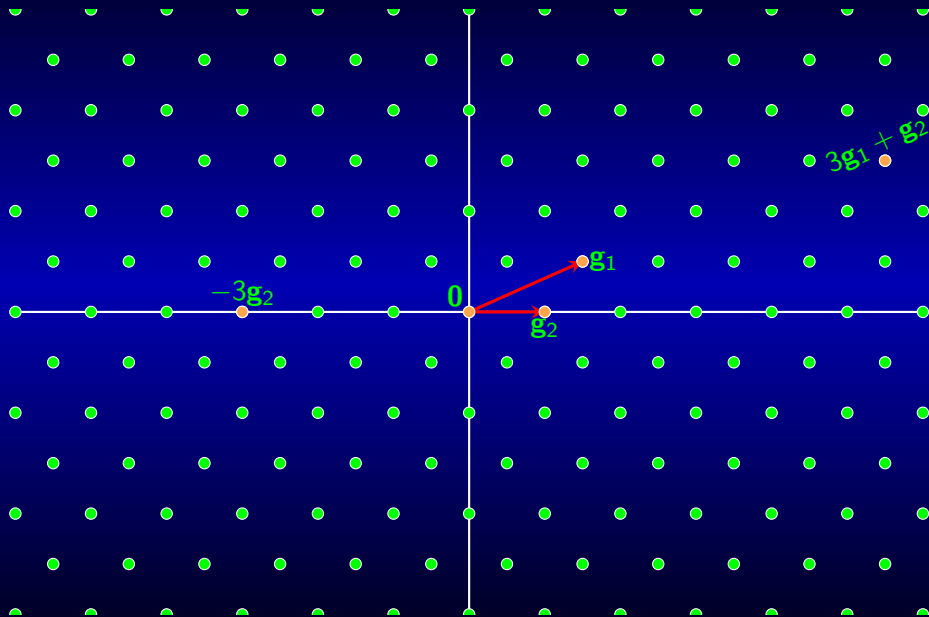
$$\Lambda(\mathbf{g}_1, \dots, \mathbf{g}_m) \triangleq \left\{ \sum_{i=1}^m c_i \mathbf{g}_i : c_1 \in \mathbb{Z}, c_2 \in \mathbb{Z}, \dots, c_m \in \mathbb{Z} \right\}.$$

- $\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_m$: the **generators** of Λ
- n : the **dimension** of Λ
- m : the **rank** of Λ
- We will focus only on full-rank lattices ($m = n$) in this tutorial.

Example: $\Lambda \left(\left(\frac{1}{2}, \frac{2}{3} \right), \left(\frac{1}{2}, -\frac{2}{3} \right) \right)$



Example: $\Lambda \left(\left(\frac{3}{2}, \frac{2}{3} \right), (1, 0) \right)$



Generator Matrix

Definition

A **generator matrix** \mathbf{G}_Λ for a lattice $\Lambda \subseteq \mathbb{R}^n$ is a matrix whose rows generate Λ :

$$\mathbf{G}_\Lambda = \begin{bmatrix} \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_n \end{bmatrix} \in \mathbb{R}^{n \times n} \text{ and } \Lambda = \{\mathbf{c}\mathbf{G}_\Lambda : \mathbf{c} \in \mathbb{Z}^n\}.$$

Example:

$$G_1 = \begin{bmatrix} 1/2 & 2/3 \\ 1/2 & -2/3 \end{bmatrix} \text{ and } G_2 = \begin{bmatrix} 3/2 & 2/3 \\ 1 & 0 \end{bmatrix}$$

generate the previous examples.

By definition, a generator matrix is *full rank*.

When do \mathbf{G} and \mathbf{G}' Generate the Same Lattice?

Recall that a matrix $\mathbf{U} \in \mathbb{Z}^{n \times n}$ is said to be **unimodular** if $\det(\mathbf{U}) \in \{1, -1\}$. If \mathbf{U} is unimodular, then $\mathbf{U}^{-1} \in \mathbb{Z}^{n \times n}$ and \mathbf{U}^{-1} is also unimodular. (\mathbf{U} is unimodular $\leftrightarrow \det(\mathbf{U})$ is a unit.)

Theorem

Two generator matrices $\mathbf{G}, \mathbf{G}' \in \mathbb{R}^{n \times n}$ generate the same lattice if and only if there exists a unimodular matrix $\mathbf{U} \in \mathbb{Z}^{n \times n}$ such that $\mathbf{G}' = \mathbf{U}\mathbf{G}$.

(In any commutative ring R , for any matrix $\mathbf{A} \in R^{n \times n}$, we have $\mathbf{A} \operatorname{adj}(\mathbf{A}) = \det(\mathbf{A})\mathbf{I}_n$, where $\operatorname{adj}(\mathbf{A})$, the **adjugate** of \mathbf{A} is given by $[\operatorname{adj}(\mathbf{A})]_{i,j} = (-1)^{i+j} \mathbf{M}_{j,i}$ where $\mathbf{M}_{j,i}$ is the minor of \mathbf{A} obtained by deleting the j th row and i th column of \mathbf{A} . Note that $\operatorname{adj}(\mathbf{A}) \in R^{n \times n}$. The matrix \mathbf{A} is invertible (in $R^{n \times n}$) if and only if $\det(\mathbf{A})$ is an invertible element (a unit) of R , in which case $\mathbf{A}^{-1} = (\det(\mathbf{A}))^{-1} \operatorname{adj}(\mathbf{A})$. cf. **Cramer's rule.**)

Proof

For “ \Rightarrow ”: Assume that \mathbf{G} and \mathbf{G}' generate the same lattice. Then there are integer matrices \mathbf{V} and \mathbf{V}' such that

$$\mathbf{G}' = \mathbf{V}\mathbf{G} \text{ and } \mathbf{G} = \mathbf{V}'\mathbf{G}'.$$

Hence,

$$\mathbf{G}' = \mathbf{V}\mathbf{V}'\mathbf{G}' = (\mathbf{V}\mathbf{V}')\mathbf{G}',$$

from which it follows that $\mathbf{V}\mathbf{V}'$ is the identity matrix. However, since $\det(\mathbf{V})$ and $\det(\mathbf{V}')$ are integers and the determinant function is multiplicative, we have $\det(\mathbf{V})\det(\mathbf{V}') = 1$. Thus $\det(\mathbf{V})$ is a unit in \mathbb{Z} and so \mathbf{V} is unimodular.

For “ \Leftarrow ”: Assume that $\mathbf{G}' = \mathbf{U}\mathbf{G}$ for a unimodular matrix \mathbf{U} , let Λ be generated by \mathbf{G} and let Λ' be generated by \mathbf{G}' . An element $\lambda' \in \Lambda'$ can be written, for some $\mathbf{c} \in \mathbb{Z}^n$ as $\lambda' = \mathbf{c}\mathbf{G}' = \mathbf{c}\mathbf{U}\mathbf{G} = \mathbf{c}'\mathbf{G} \in \Lambda$, which shows, since $\mathbf{c}' = \mathbf{c}\mathbf{U} \in \mathbb{Z}^n$, that $\Lambda' \subseteq \Lambda$. On the other hand, we have $\mathbf{G} = \mathbf{U}^{-1}\mathbf{G}'$ and a similar argument shows that $\Lambda \subseteq \Lambda'$.

Lattice Determinant

Definition

The **determinant**, $\det(\Lambda)$, of a full-rank lattice Λ is given as

$$\det(\Lambda) = |\det(\mathbf{G}_\Lambda)|$$

where \mathbf{G}_Λ is any generator matrix for Λ .

- Note that, in view of the previous theorem, this is an **invariant** of the lattice Λ , i.e., the determinant of Λ is independent of the choice of \mathbf{G}_Λ .
- As we will now see, this invariant has a geometric significance.

Fundamental Region

Definition

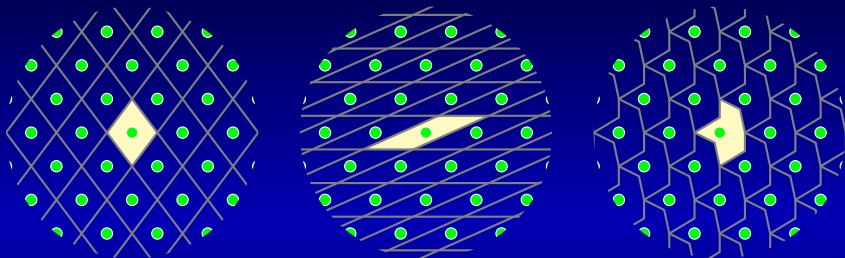
A set $\mathcal{R} \subseteq \mathbb{R}^n$ is called a **fundamental region** of a lattice $\Lambda \subseteq \mathbb{R}^n$ if the following conditions are satisfied:

- 1 $\mathbb{R}^n = \bigcup_{\lambda \in \Lambda} (\lambda + \mathcal{R})$.
- 2 For every $\lambda_1, \lambda_2 \in \Lambda$ with $\lambda_1 \neq \lambda_2$, $(\lambda_1 + \mathcal{R}) \cap (\lambda_2 + \mathcal{R}) = \emptyset$.

In other words, the translates of a fundamental region \mathcal{R} by lattice points form a disjoint covering (or **tiling**) of \mathbb{R}^n .

- A fundamental region \mathcal{R} cannot contain two points \mathbf{x}_1 and \mathbf{x}_2 whose difference is a nonzero lattice point, since if $\mathbf{x}_1 - \mathbf{x}_2 = \lambda \in \Lambda$, $\lambda \neq \mathbf{0}$, for $\mathbf{x}_1, \mathbf{x}_2 \in \mathcal{R}$, we would have $\mathbf{x}_1 \in \mathbf{0} + \mathcal{R}$ and $\mathbf{x}_1 = \mathbf{x}_2 + \lambda \in \lambda + \mathcal{R}$, contradicting Property 2.
- Algebraically, the points of a fundamental region form a complete system of coset representatives of the cosets of Λ in \mathbb{R}^n .

Fundamental Regions for $\Lambda((1/2, 2/3), (1/2, -2/3))$



- Each shaded fundamental region serves as a **tile**; the union of translates of a tile by all lattice points forms a disjoint covering of \mathbb{R}^2 .
- Fundamental regions need not be connected sets.

Fundamental Parallelepiped

Definition

The **fundamental parallelepiped** of a generating set $\mathbf{g}_1, \dots, \mathbf{g}_n \in \mathbb{R}^n$ for a lattice Λ is the set

$$\mathcal{P}(\mathbf{g}_1, \dots, \mathbf{g}_n) \triangleq \left\{ \sum_{i=1}^n a_i \mathbf{g}_i : (a_1, \dots, a_n) \in [0, 1)^n \right\}.$$



$$\mathcal{P}\left(\left(\frac{1}{2}, \frac{2}{3}\right), \left(\frac{1}{2}, -\frac{2}{3}\right)\right)$$



$$\mathcal{P}\left(\left(\frac{3}{2}, \frac{2}{3}\right), (1, 0)\right)$$

Their Volume = $\det(\Lambda)$

Proposition

Given a lattice Λ , the fundamental parallelepiped of every generating set for Λ has the same volume, namely $\det(\Lambda)$.

Proof: Let $\mathbf{g}_1, \dots, \mathbf{g}_n$ form the rows of a generator matrix \mathbf{G} . Then, by change of variables,

$$\begin{aligned}\text{Vol}(\mathcal{P}(\mathbf{g}_1, \dots, \mathbf{g}_n)) &= \text{Vol}(\{\mathbf{a}\mathbf{G} : \mathbf{a} \in [0, 1]^n\}) \\ &= \text{Vol}([0, 1]^n) \cdot |\det(\mathbf{G})| \\ &= |\det(\mathbf{G})| \\ &= \det(\Lambda)\end{aligned}$$

All Fundamental Regions Have the Same Volume

Proposition

More generally, every fundamental region \mathcal{R} of Λ has the same volume, namely $\det(\Lambda)$.

Proof (by picture):



Proof (by mapping): translate each point of \mathcal{R} by some lattice vector to a unique point of \mathcal{P} . Partition \mathcal{R} into “pieces” $\mathcal{R}_1, \mathcal{R}_2, \dots$ translated by the same vector. If the pieces each have a well-defined volume, then $\text{Vol}(\mathcal{R}) = \sum_i \text{Vol}(\mathcal{R}_i)$, and the result follows since volume is translation invariant and the union of the translated pieces is \mathcal{P} .

Voronoi Region

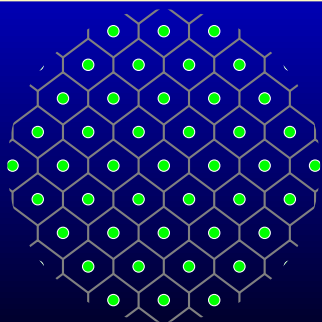
Definition

Given a lattice $\Lambda \subseteq \mathbb{R}^n$ and a point $\lambda \in \Lambda$, a **Voronoi region** of λ is defined as

$$\mathcal{V}(\lambda) = \{\mathbf{x} \in \mathbb{R}^n : \forall \lambda' \in \Lambda, \lambda' \neq \lambda, \|\mathbf{x} - \lambda\| \leq \|\mathbf{x} - \lambda'\|\},$$

where ties are broken systematically.

The Voronoi region of $\mathbf{0}$ is often called the Voronoi region of the lattice and it is denoted by $\mathcal{V}(\Lambda)$.



Nearest-Neighbor Quantizer

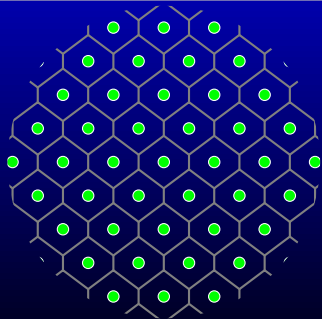
Definition

A **nearest neighbor quantizer** $Q_{\Lambda}^{(NN)} : \mathbb{R}^n \rightarrow \Lambda$ associated with a lattice Λ maps a vector to the closest lattice point

$$Q_{\Lambda}^{(NN)}(\mathbf{x}) = \arg \min_{\lambda \in \Lambda} \|\mathbf{x} - \lambda\|,$$

where ties are broken systematically.

- The inverse image $[Q_{\Lambda}^{(NN)}]^{-1}(\lambda)$ is a Voronoi region of λ .
- $Q_{\Lambda}^{(NN)}(\mathbf{x})$ may be difficult to compute for arbitrary $\mathbf{x} \in \mathbb{R}^n$.

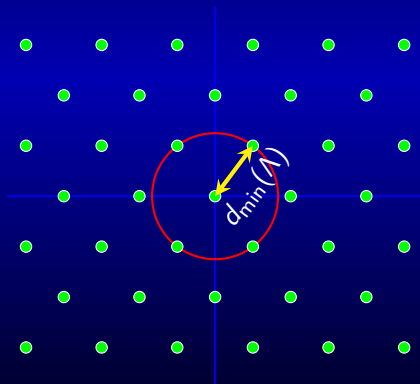


Minimum Distance

Definition

The **minimum distance** of a lattice $\Lambda \subseteq \mathbb{R}^n$ is defined as

$$d_{\min}(\Lambda) = \min_{\lambda \in \Lambda^*} \|\lambda\|.$$



Fact:

$$d_{\min}(\Lambda) > 0$$

Proof: exercise.

Successive Minima

Recall that \mathcal{B}_r denotes the n -dimensional ball of radius r centered at the origin: $\mathcal{B}_r \triangleq \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\| \leq r\}$.

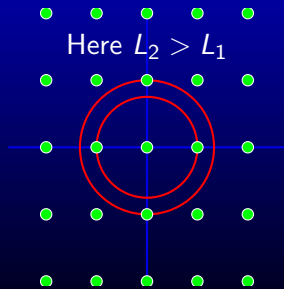
Definition

For a lattice $\Lambda \subset \mathbb{R}^n$, let

$L_i(\Lambda) \triangleq \min\{r : \mathcal{B}_r \text{ contains at least } i \text{ linearly indep. lattice vectors}\}$.

Then $L_1 \leq L_2 \leq \dots \leq L_n$ are the **successive minima** of Λ .

- We have $L_1(\Lambda) = d_{\min}(\Lambda)$.
- Note that $L_n(\Lambda)$ contains n linearly independent lattice vectors by definition, but these may *not* generate Λ ! (Example: $2\mathbb{Z}^5 \cup (1, 1, 1, 1, 1) + 2\mathbb{Z}^5$ has $L_1 = \dots = L_5 = 2$, but the 5 linearly independent vectors in \mathcal{B}_2 generate only $2\mathbb{Z}^5$.)



A Quick Recap

As subgroups of \mathbb{R}^n , lattices have both algebraic and geometric properties.

- Algebra: closed under subtraction (forms a subgroup)
- Geometry: fundamental regions (fundamental parallelepiped, Voronoi region), (positive) minimum distance, successive minima
- Because lattices have positive minimum distance, they are **discrete** subgroups of \mathbb{R}^n , i.e., surrounding the origin is an open ball containing just one lattice point (the origin itself).
- The converse is also true: a discrete subgroup of \mathbb{R}^n is necessarily a lattice.

Dual Lattice

Definition

The **dual** of a full-rank lattice $\Lambda \subset \mathbb{R}^n$ is the set

$$\Lambda^\perp = \{\mathbf{x} \in \mathbb{R}^n : \forall \boldsymbol{\lambda} \in \Lambda, \langle \mathbf{x}, \boldsymbol{\lambda} \rangle \in \mathbb{Z}\},$$

i.e., the set of vectors in \mathbb{R}^n having *integral* inner-product with every lattice vector.

Fact

If Λ has generator matrix $\mathbf{G} \in \mathbb{R}^{n \times n}$, then Λ^\perp has generator matrix $(\mathbf{G}^{-1})^T$, where the inverse is taken in $\mathbb{R}^{n \times n}$.

Theorem

$$\det(\Lambda) \cdot \det(\Lambda^\perp) = 1.$$

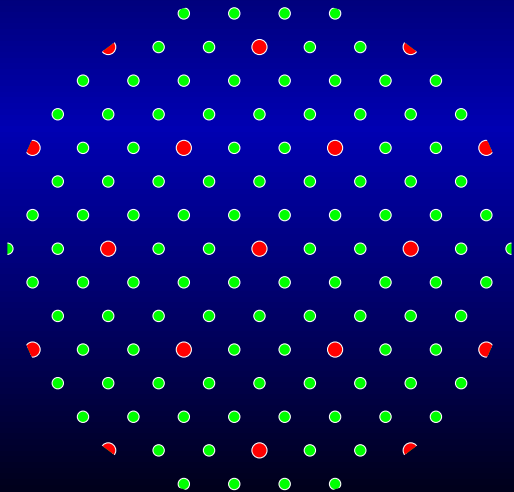
Proof: follows from the fact that $\det(\mathbf{G}^{-1}) = (\det \mathbf{G})^{-1}$.

Remark: the generator matrix for Λ^\perp serves as a **parity-check matrix** for Λ .

Nested Lattices

Definition

A **sublattice** Λ' of Λ is a subset of Λ , which itself is a lattice. A pair of lattices (Λ, Λ') is called **nested** if Λ' is a sublattice of Λ .



Λ is called the **fine lattice**
while Λ' is called the
coarse lattice.

$$\Lambda' \subseteq \Lambda$$

Nested Lattices: Nesting Matrix

Let Λ and Λ' have generator matrices \mathbf{G}_Λ and $\mathbf{G}_{\Lambda'}$, respectively. If $\Lambda' \subseteq \Lambda$, every vector of Λ' is generated as some integer linear combination of the rows of \mathbf{G}_Λ .

Definition

In particular, the generator matrices $\mathbf{G}_{\Lambda'}$ and \mathbf{G}_Λ must satisfy

$$\mathbf{G}_{\Lambda'} = \mathbf{J}\mathbf{G}_\Lambda,$$

for some matrix $\mathbf{J} \in \mathbb{Z}^{n \times n}$, called a **nesting matrix**.

- Given \mathbf{G}_Λ and $\mathbf{G}_{\Lambda'}$, \mathbf{J} is unique.
- $|\det(\mathbf{J})|$ is an invariant: $\det(\Lambda') = |\det(\mathbf{J})| \det(\Lambda)$

Nested Lattices: Diagonal Nesting

Theorem

Let $\Lambda' \subset \Lambda$ be a nested lattice pair. Then there exist generator matrices \mathbf{G}_Λ and $\mathbf{G}_{\Lambda'}$ for Λ and Λ' , respectively, such that

$$\mathbf{G}_{\Lambda'} = \text{diag}(c_1, \dots, c_n) \mathbf{G}_\Lambda$$

with $c_1 \mid c_2 \mid \dots \mid c_n$.

Here c_1, \dots, c_n are the **invariant factors** of the nesting matrix.

Smith Normal Form

The Smith normal form is a canonical form for matrices with entries in a principal ideal domain (PID).

Definition

Let \mathbf{A} be a nonzero $m \times n$ matrix over a PID. There exist invertible $m \times m$ and $n \times n$ matrices \mathbf{P}, \mathbf{Q} such that the product

$$\mathbf{PAQ} = \text{diag}(r_1, \dots, r_k), \quad k = \min\{m, n\}$$

and the diagonal elements $\{r_i\}$ satisfy $r_i \mid r_{i+1}$ for $1 \leq i < k$. This product is the **Smith normal form** of \mathbf{A} .

The elements $\{r_i\}$ are unique up to multiplication by a unit and are called the **invariant factors** of \mathbf{A} .

Diagonal Nesting Follows from Smith Normal Form

For some $\mathbf{J} \in \mathbb{Z}^{n \times n}$, let

$$\mathbf{G}_{\Lambda'} = \mathbf{J}\mathbf{G}_{\Lambda}.$$

Then, for some $n \times n$ unimodular matrices \mathbf{U} and \mathbf{V} , we have

$$\mathbf{U}\mathbf{J}\mathbf{V} = \mathbf{D} = \text{diag}(c_1, c_2, \dots, c_n),$$

or, equivalently,

$$\mathbf{J} = \mathbf{U}^{-1}\mathbf{D}\mathbf{V}^{-1}.$$

Thus

$$\mathbf{G}_{\Lambda'} = \mathbf{J}\mathbf{G}_{\Lambda} = \mathbf{U}^{-1}\mathbf{D}\mathbf{V}^{-1}\mathbf{G}_{\Lambda}$$

or

$$(\mathbf{U}\mathbf{G}_{\Lambda'}) = \mathbf{D}(\mathbf{V}^{-1}\mathbf{G}_{\Lambda}).$$

Nested Lattices: Labels and Enumeration

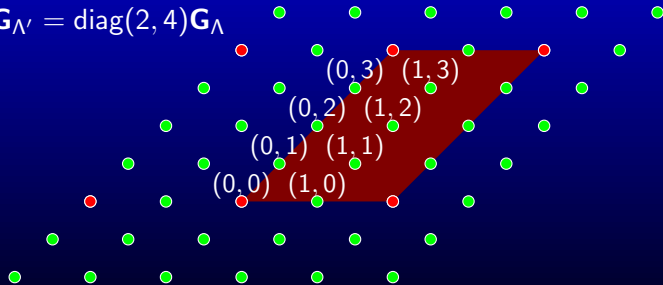
With a diagonal nesting in which $\mathbf{G}_{\Lambda'} = \mathbf{J}\mathbf{G}_{\Lambda}$ with $\mathbf{J} = \text{diag}(c_1, c_2, \dots, c_n)$, we get a useful labelling scheme for lattice vectors in the fundamental parallelepiped of Λ' : each such point is of the form

$$(a_1, a_2, \dots, a_n)\mathbf{G}_{\Lambda}$$

where

$$0 \leq a_1 < c_1, 0 \leq a_2 < c_2, \dots, 0 \leq a_n < c_n.$$

E.g., $\mathbf{G}_{\Lambda'} = \text{diag}(2, 4)\mathbf{G}_{\Lambda}$

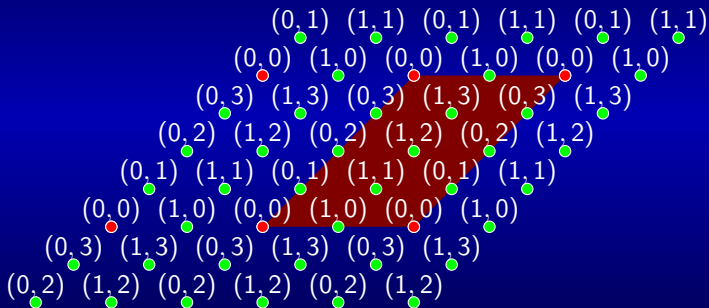


Note that there are $\det(\mathbf{J}) = \prod_{i=1}^n c_i$ labelled points.

Nested Lattices: Linear Labelling

If we periodically extend the labels to *all* the lattice vectors, then the labels are **linear** in $\mathbb{Z}_{c_1} \times \mathbb{Z}_{c_2} \times \cdots \times \mathbb{Z}_{c_n}$, i.e.,

$$\ell(\boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2) = \ell(\boldsymbol{\lambda}_1) + \ell(\boldsymbol{\lambda}_2).$$



Stated more algebraically,

$$\Lambda/\Lambda' \simeq \mathbb{Z}_{c_1} \times \mathbb{Z}_{c_2} \times \cdots \times \mathbb{Z}_{c_n}.$$

Complex Lattices

The theory of lattices extends to \mathbb{C}^n , where we have many choices for what is meant by an “integer.” Generally we take the ring R of integers as a subring of \mathbb{C} forming a principal ideal domain.

Examples:

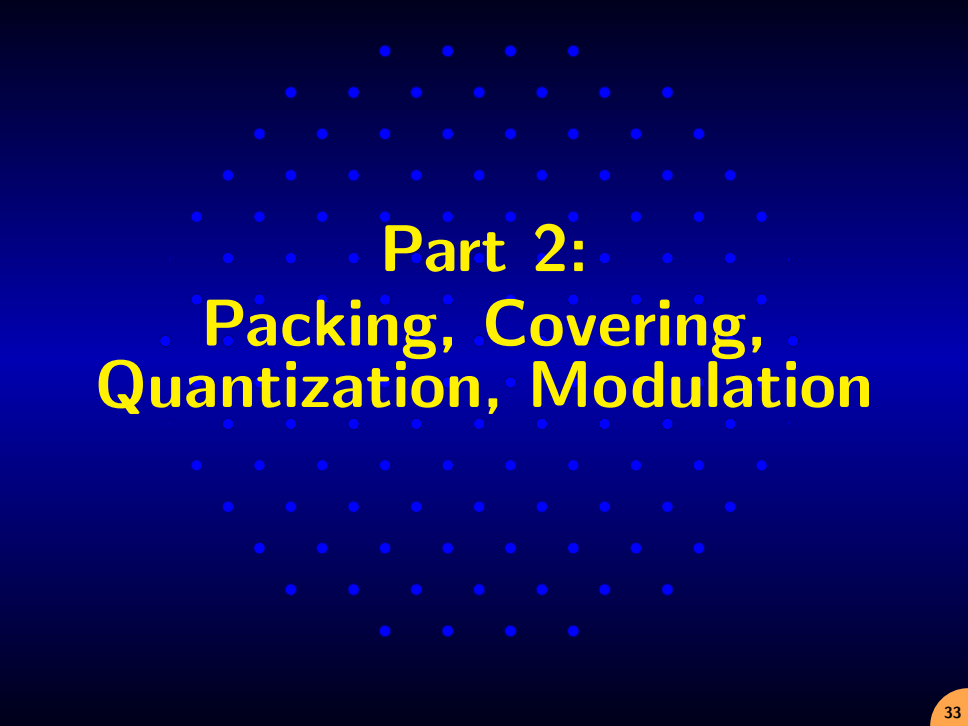
- $R = \{a + bi : a, b \in \mathbb{Z}\}$ (Gaussian integers)
- $R = \{a + be^{2\pi i/3} : a, b \in \mathbb{Z}\}$ (Eisenstein integers)

Definition

Given m linearly independent (row) vectors $\mathbf{g}_1, \dots, \mathbf{g}_m \in \mathbb{C}^n$, the **complex lattice** Λ generated by them is defined as the set of all R -linear combinations of the \mathbf{g}_i 's:

$$\Lambda(\mathbf{g}_1, \dots, \mathbf{g}_m) \triangleq \left\{ \sum_{i=1}^m c_i \mathbf{g}_i : c_1 \in R, c_2 \in R, \dots, c_m \in R \right\}.$$

(In engineering applications, complex lattices are suited for QAM modulation.)



Part 2:
**Packing, Covering,
Quantization, Modulation**

Balls in High Dimensions

Recall that $\mathcal{B}_r = \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\| \leq r\}$ is the n -dimensional ball of radius r centered at the origin.

- \mathcal{B}_1 is the unit-radius ball
- $\mathcal{B}_r = r\mathcal{B}_1 = \{r\mathbf{x} : \mathbf{x} \in \mathcal{B}_1\}$
- $\text{Vol}(\mathcal{B}_r) = r^n \text{Vol}(\mathcal{B}_1) \triangleq r^n V_n$, where V_n is the volume of \mathcal{B}_1
- Easy to show that $V_1 = 2$, $V_2 = \pi$, $V_3 = \frac{4}{3}\pi$
- In general, $V_n = \frac{\pi^{n/2}}{(n/2)!}$, where the factorial $(n/2)!$ for odd n is

$$(n/2)! = \Gamma\left(1 + \frac{n}{2}\right) = \sqrt{\pi} \frac{1}{2} \frac{3}{2} \cdots \frac{n}{2}.$$

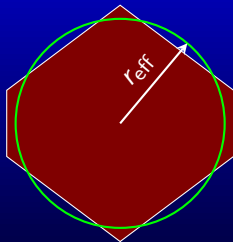
- In fact, $V_n \approx (2\pi e/n)^{n/2}$ and $\lim_{n \rightarrow \infty} nV_n^{2/n} = 2\pi e$.

Effective Radius of a Lattice

Definition

The **effective radius** of a lattice Λ is the radius of a ball of volume $\det(\Lambda)$:

$$r_{\text{eff}}(\Lambda) = \left(\frac{\det(\Lambda)}{V_n} \right)^{1/n}.$$



Sphere Packing

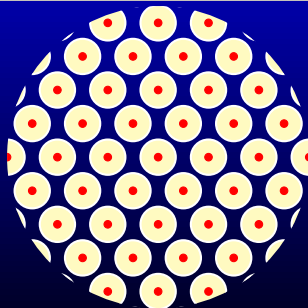
Definition

A lattice $\Lambda \subset \mathbb{R}^n$ is said to **pack** \mathcal{B}_r if

$$\lambda_1, \lambda_2 \in \Lambda, \lambda_1 \neq \lambda_2 \rightarrow (\lambda_1 + \mathcal{B}_r) \cap (\lambda_2 + \mathcal{B}_r) = \emptyset.$$

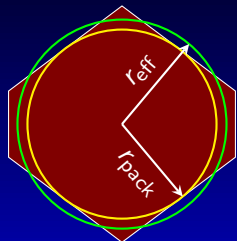
The **packing radius** of Λ is

$$r_{\text{pack}}(\Lambda) \triangleq \sup\{r : \Lambda \text{ packs } \mathcal{B}_r\}.$$



Packing Efficiency

It is easy to see that $r_{\text{pack}}(\Lambda)$ is the inner radius of the Voronoi region $\mathcal{V}(\Lambda)$, i.e., the radius of the smallest (open) ball contained in \mathcal{V} . Clearly, $r_{\text{pack}}(\Lambda) \leq r_{\text{eff}}(\Lambda)$, with equality if and only if the Voronoi region itself is a ball.



Definition

The **packing efficiency** of a lattice Λ is

$$\rho_{\text{pack}}(\Lambda) = \frac{r_{\text{pack}}(\Lambda)}{r_{\text{eff}}(\Lambda)}.$$

- Clearly, $0 < \rho_{\text{pack}}(\Lambda) \leq 1$.
- $\rho_{\text{pack}}(\Lambda)$ is invariant to scaling, i.e., $\rho_{\text{pack}}(\alpha\Lambda) = \rho_{\text{pack}}(\Lambda)$ for all $\alpha \neq 0$.

- the **packing density** $= \frac{\text{Vol}(\mathcal{B}_{r_{\text{pack}}(\Lambda)})}{\text{Vol}(\mathcal{V}(\Lambda))} = \rho_{\text{pack}}^n(\Lambda)$

Packing Efficiency (Cont'd)

- The densest 2-dimensional lattice is the hexagonal lattice with efficiency $\sqrt{\pi/2\sqrt{3}} \approx 0.9523$
- The densest 3-dimensional lattice is the face-centered cubic lattice with efficiency $\sqrt[3]{\pi/3\sqrt{2}} \approx 0.9047$
- The densest lattices are known for all dimensions up to eight, and in 24 dimensions, but are still unknown for most higher dimensions. (cf 2016 breakthrough result of Maryna Viazovska showing that E_8 forms the densest *packing* in 8 dimensions, and, with coauthors, that the Leech lattice Λ_{24} has the same property in 24 dimensions.)
- The Minkowski-Hlawka Theorem guarantees that in each dimension there exists a lattice whose packing efficiency is at least $1/2$:

$$\max_{\Lambda \subset \mathbb{R}^n} \rho_{\text{pack}}(\Lambda) \geq 1/2$$

Sphere Covering

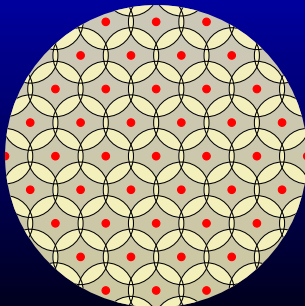
Definition

A lattice $\Lambda \subset \mathbb{R}^n$ is said to **cover** \mathbb{R}^n with \mathcal{B}_r if

$$\bigcup_{\lambda \in \Lambda} (\lambda + \mathcal{B}_r) = \mathbb{R}^n.$$

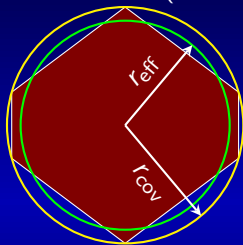
The **covering radius** of Λ is

$$r_{\text{cov}}(\Lambda) \triangleq \min\{r : \Lambda \text{ covers } \mathbb{R}^n \text{ with } \mathcal{B}_r\}.$$



Covering Efficiency

It is easy to see that $r_{\text{cov}}(\Lambda)$ is the outer radius of the Voronoi region $\mathcal{V}(\Lambda)$, i.e., the radius of the smallest (closed) ball containing \mathcal{V} .



Definition

The **covering efficiency** of a lattice Λ is

$$\rho_{\text{cov}}(\Lambda) = \frac{r_{\text{cov}}(\Lambda)}{r_{\text{eff}}(\Lambda)}.$$

- Clearly, $\rho_{\text{cov}}(\Lambda) \geq 1$.
- $\rho_{\text{cov}}(\Lambda)$ is invariant to scaling.

Covering Efficiency (Cont'd)

- The best 2-dimensional covering lattice is the hexagonal lattice with $\rho_{\text{cov}}(\Lambda) \approx 1.0996$.
- The best 3-dimensional covering lattice is not the densest one: it is the body-centered cubic lattice with $\rho_{\text{cov}}(\Lambda) \approx 1.1353$.
- A result of Rogers shows that there exists a sequence of lattices Λ_n of increasing dimension n such that $\rho_{\text{cov}}(\Lambda) \rightarrow 1$, as $n \rightarrow \infty$.

Quantization

Definition

A **lattice quantizer** is a map $Q_\Lambda : \mathbb{R}^n \rightarrow \Lambda$ for some lattice $\Lambda \subset \mathbb{R}^n$.

- If we use the nearest-neighbor quantizer $Q_\Lambda^{(NM)}$, then the quantization error $\mathbf{x}_e \triangleq \mathbf{x} - Q_\Lambda^{(NM)}(\mathbf{x}) \in \mathcal{V}(\Lambda)$.
- Suppose that \mathbf{x}_e is uniformly distributed over the Voronoi region $\mathcal{V}(\Lambda)$, then the **second moment per dimension** is given as

$$\sigma^2(\Lambda) = \frac{1}{n} E[\|\mathbf{x}_e\|^2] = \frac{1}{n \det(\Lambda)} \int_{\mathcal{V}(\Lambda)} \|\mathbf{x}_e\|^2 d\mathbf{x}_e.$$

- Clearly, the smaller is $\sigma^2(\Lambda)$, the better is the quantizer.

Quantization: Figure of Merit

Definition

A figure of merit of the nearest-neighbor lattice quantizer is the **normalized second moment**, given as

$$G(\Lambda) = \frac{\sigma^2(\Lambda)}{\det(\Lambda)^{2/n}}.$$

- $G(\Lambda)$ is invariant to scaling.
- Let G_n denote the minimum possible value of $G(\Lambda)$ over all lattices in \mathbb{R}^n . Then, since $G(\mathbb{Z}^n) = 1/12$, we have $G_n \leq 1/12$.

Quantization: Figure of Merit (Cont'd)

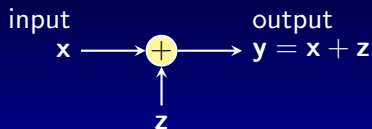
Q: What is a lower bound on G_n ?

A: An n -dimensional ball of a given volume minimizes the second moment. The corresponding quantity G_n^* is monotonically decreasing with n , and approaches $\frac{1}{2\pi e}$ as $n \rightarrow \infty$. Hence

$$\frac{1}{12} \geq G_n \geq G_n^* > \frac{1}{2\pi e}.$$

- There exists a sequence of lattices Λ_n of increasing dimension n such that $G(\Lambda_n) \rightarrow \frac{1}{2\pi e}$, as $n \rightarrow \infty$.

Modulation: AWGN channel



An additive-noise channel is given by the input/output relation

$$\mathbf{y} = \mathbf{x} + \mathbf{z},$$

where the noise \mathbf{z} is independent of the input \mathbf{x} .

In the AWGN channel case, \mathbf{z} is a white (i.i.d.) Gaussian noise with zero mean and variance σ^2 whose pdf is given by

$$f_Z(\mathbf{z}) = \frac{1}{(2\pi\sigma^2)^{n/2}} e^{-\frac{\|\mathbf{z}\|^2}{2\sigma^2}}.$$

Modulation: Error Probability

Suppose that (part of) a lattice Λ is used as a codebook; then the transmitted signal $\mathbf{x} \in \Lambda$.

Since the pdf decreases monotonically with $\|\mathbf{z}\|$, given a received vector \mathbf{y} , it is natural to decode \mathbf{x} as the closest lattice point:

$$\hat{\mathbf{x}} = \arg_{\boldsymbol{\lambda} \in \Lambda} \min \|\mathbf{y} - \boldsymbol{\lambda}\| = \mathcal{Q}_{\Lambda}^{(MM)}(\mathbf{y}).$$

The error probability is thus defined as

$$P_e(\Lambda, \sigma^2) \triangleq \Pr[\mathbf{z} \notin \mathcal{V}(\Lambda)]$$

- $P_e(\Lambda, \sigma^2)$ increases monotonically with the noise variance σ^2
- For some target error probability $0 < \epsilon < 1$, let $\sigma^2(\epsilon) =$ value of σ^2 such that $P_e(\Lambda, \sigma^2)$ is equal to ϵ .

Modulation: Figure of Merit

Definition (Normalized volume to noise ratio)

The **normalized volume to noise ratio** of a lattice Λ , at a target error probability P_e , $0 < P_e < 1$, is defined as

$$\mu(\Lambda, P_e) = \frac{\det(\Lambda)^{2/n}}{\sigma^2(P_e)}.$$

- $\mu(\Lambda, P_e)$ is invariant to scaling.
- The lower, the better.

Modulation: Figure of Merit (Cont'd)

- The minimum possible value of $\mu(\Lambda, P_e)$ over all lattices in \mathbb{R}^n is denoted by $\mu_n(P_e)$. Clearly, $\mu_n(P_e) \leq \mu(\mathbb{Z}^n, P_e)$.

Q: What is a lower bound on $\mu_n(P_e)$?

A: An n -dimensional ball contains more probability mass of an AWGN vector than any other body of the same volume. The corresponding quantity $\mu_n^*(P_e)$ is monotonically decreasing with n for $0 < P_e < P_e^{\text{th}} \approx 0.03$, and it approaches $2\pi e$, as $n \rightarrow \infty$, for all $0 < P_e < 1$.

- Hence,

$$2\pi e < \mu_n^*(P_e) \leq \mu_n(P_e) \leq \mu(\mathbb{Z}^n, P_e).$$

- There exists a sequence of lattices Λ_n of increasing dimension n such that for all $0 < P_e < 1$, $\mu(\Lambda_n, P_e) \rightarrow 2\pi e$, as $n \rightarrow \infty$.

Fun Facts about Lattices (Lifted from the Pages of [Zamir,2014])

- The seventeenth century astronomer Johannes Kepler conjectured that the face-centered cubic lattice forms the best sphere-packing in three dimensions. While Gauss showed that no other *lattice* packing is better, the perhaps harder part—of excluding non-lattice packings—remained open until a full (computer-aided) proof was given in 1998 by Hales.
- The optimal sphere packings in 2 and 3 dimensions are lattice packings—could this be the case in higher dimensions as well? This remains a mystery. (But not in dimensions 8 and 24!)
- The early twentieth century mathematician Hermann Minkowski used lattices to relate n -dimensional geometry with number theory—an area he called “the geometry of numbers.” The Minkowski-Hlawka theorem (conjectured by Minkowski and proved by Hlawka in 1943) will play the role of Shannon’s random coding technique in Part 4.
- Some of the stronger (post-quantum) public-key algorithms today use lattice-based cryptography.



Part 3: Lattices and Linear Codes

Fields

Definition

Recall that a **field** is a triple $(\mathbb{F}, +, \cdot)$ with the properties that

- 1 $(\mathbb{F}, +)$ forms an abelian group with identity 0,
- 2 (\mathbb{F}^*, \cdot) forms an abelian group with identity 1,
- 3 for all $x, y, z \in \mathbb{F}$, $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$, i.e., multiplication ' \cdot ' distributes over addition ' $+$ '.

Roughly speaking, fields enjoy all the usual familiar arithmetic properties of real numbers, including addition, subtraction, multiplication and division (by nonzero elements), the product of nonzero elements is nonzero, etc.

- \mathbb{R} and \mathbb{C} form (infinite) fields under real and complex arithmetic, respectively.
- \mathbb{Z} does not form a field (since most elements don't have multiplicative inverses).

Finite Fields

Definition

A field with a finite number of elements is called a **finite field**.

- $\mathbb{F}_p = \{0, 1, \dots, p-1\}$ forms a field under integer arithmetic modulo p , where p is a prime.
- $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$ does not form field under integer arithmetic modulo m , when m is composite, since if $m = ab$ with $1 < a < m$ then $ab = 0 \pmod{m}$, yet a and b are nonzero elements of \mathbb{Z}_m . Such “zero divisors” cannot be present in a field.

The following facts are well known:

- A q -element finite field \mathbb{F}_q exists if and only if $q = p^m$ for a prime integer p and a positive integer m . Thus there are finite fields of order 2, 3, 4, 5, 7, 8, 9, 11, 13, 16, \dots , but none of order 6, 10, 12, 14, 15, \dots
- Any two finite fields of the same order are isomorphic; thus we refer to *the* finite field \mathbb{F}_q of order q .

The Vector Space \mathbb{F}_q^n

The set of n -tuples

$$\mathbb{F}_q^n = \{(x_1, \dots, x_n) : x_1 \in \mathbb{F}_q, \dots, x_n \in \mathbb{F}_q\}$$

forms a **vector space** over \mathbb{F}_q with

- 1 **vector addition** defined componentwise

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n)$$

- 2 **scalar multiplication** defined, for any scalar $a \in \mathbb{F}_q$ and any vector $\mathbf{x} \in \mathbb{F}_q^n$, via $a\mathbf{x} = (ax_1, \dots, ax_n)$.

- Any subset of $C \subseteq \mathbb{F}_q^n$ forming a vector space under the operations inherited from \mathbb{F}_q^n , is called a **subspace** of \mathbb{F}_q^n .
- A set of vectors $\{\mathbf{v}_1, \dots, \mathbf{v}_k\} \subseteq \mathbb{F}_q^n$ is called **linearly independent** if the only solution to the equation $\mathbf{0} = a_1\mathbf{v}_1 + \dots + a_n\mathbf{v}_n$ in unknown scalars a_1, \dots, a_n is the trivial one (with $a_1 = \dots = a_n = 0$).

Dimension

- If C is a subspace of \mathbb{F}_q^n , then the number of elements in any maximal subset of C of linearly independent vectors is an invariant called the **dimension** of C .
- For example, \mathbb{F}_q^n has dimension n .
- If C is a subspace of \mathbb{F}_q^n of dimension k , then $0 \leq k \leq n$.

Linear Block Codes over \mathbb{F}_q

Definition

An (n, k) **linear code** over \mathbb{F}_q is a k -dimensional subspace of \mathbb{F}_q^n .

The parameter n is called the **block length**, and k is the **dimension**. The elements of a code are called *codewords*. For example, $\{000, 111\}$ is a $(3,1)$ linear code over \mathbb{F}_2 .

Let $\mathcal{B} = \{\mathbf{g}_1, \dots, \mathbf{g}_k\}$ be a maximal linearly independent subset of an (n, k) linear code C . Then \mathcal{B} is a **basis** having the property that each element \mathbf{v} of C has a unique representation as a linear combination

$$\mathbf{v} = \sum_{i=1}^k a_i \mathbf{g}_i$$

for some scalars $a_1, \dots, a_k \in \mathbb{F}_q$.

By counting the number of distinct choices for a_1, \dots, a_k , we find that an (n, k) linear code over \mathbb{F}_q has q^k codewords.

Generator Matrices

Definition

A **generator matrix** for an (n, k) linear code C over \mathbb{F}_q is a matrix $\mathbf{G} \in \mathbb{F}_q^{k \times n}$ given as

$$\mathbf{G} = \begin{bmatrix} \mathbf{g}_1 \\ \mathbf{g}_2 \\ \vdots \\ \mathbf{g}_k \end{bmatrix}$$

where $\{\mathbf{g}_1, \dots, \mathbf{g}_k\}$ is any basis for C .

The code C itself is then the **row space** of \mathbf{G} , i.e.,

$$C = \{\mathbf{u}\mathbf{G} : \mathbf{u} \in \mathbb{F}_q^k\},$$

and \mathbf{G} is said to **generate** C .

Two different generator matrices \mathbf{G}_1 and \mathbf{G}_2 generate the same code C if $\mathbf{G}_2 = \mathbf{U}\mathbf{G}_1$ for some invertible matrix $\mathbf{U} \in \mathbb{F}_q^{k \times k}$, or equivalently if \mathbf{G}_2 can be obtained from \mathbf{G}_1 by a sequence of elementary row operations.

Systematic Form

A canonical generator matrix for a code C is obtained (using Gauss-Jordan elimination) by reducing any generator matrix \mathbf{G} of C to its unique reduced row echelon form \mathbf{G}_{RREF} .

In some cases, \mathbf{G}_{RREF} takes the form, called **systematic form**,

$$\mathbf{G}_{\text{RREF}} = [\mathbf{I}_k \mid \mathbf{P}]$$

where \mathbf{I}_k is the $k \times k$ identity matrix, and \mathbf{P} is some $k \times (n - k)$ matrix.

If $\mathbf{v} = \mathbf{u}\mathbf{G}$, with \mathbf{G} in systematic form, then $\mathbf{v} = (\mathbf{u}, \mathbf{u}\mathbf{P})$.

When \mathbf{G} used as an encoder, mapping a message \mathbf{u} to a codeword $\mathbf{v} = \mathbf{u}\mathbf{G}$, then, when \mathbf{G} is in systematic form, the message \mathbf{u} appears in the first k positions of every codeword.

(More generally, if \mathbf{G}_{RREF} is used as an encoder, the components of the message \mathbf{u} appears in k fixed locations, corresponding to the pivot columns of \mathbf{G}_{RREF} , of every codeword.)

Dual Codes

We may define an “inner-product” in \mathbb{F}_q^n via $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^n x_i y_i$.

Definition

The dual C^\perp of a linear code C over \mathbb{F}_q is the set

$$C^\perp = \{\mathbf{v} \in \mathbb{F}_q^n : \forall \mathbf{c} \in C, \langle \mathbf{v}, \mathbf{c} \rangle = 0\}.$$

- The dual of an (n, k) linear code is an $(n, n - k)$ linear code.
- A generator matrix \mathbf{H} for C^\perp is called a **parity-check matrix** for C and must satisfy $\mathbf{GH}^T = \mathbf{0}^{k \times (n-k)}$ for every generator matrix \mathbf{G} of C .
- Equivalently, we may write

$$C = \{\mathbf{c} \in \mathbb{F}_q^n : \mathbf{cH}^T = \mathbf{0}\},$$

displaying C as the k -dimensional solution space of a system of $n - k$ homogenous equations in n unknowns.

Computing \mathbf{H} from \mathbf{G}

When C has a generator matrix \mathbf{G} in systematic form

$$\mathbf{G} = [\mathbf{I} \mid \mathbf{P}]$$

then it is easy to verify (by multiplication) that

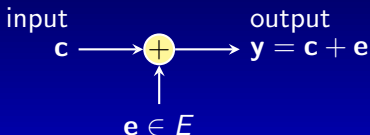
$$\mathbf{H} = [-\mathbf{P}^T \mid \mathbf{I}]$$

is a parity-check matrix for C .

More generally, any given \mathbf{G} can be reduced to \mathbf{G}_{RREF} . If \mathbf{P} is the matrix obtained from \mathbf{G}_{RREF} by deleting its pivot columns, then a parity-check matrix \mathbf{H} is obtained by distributing the columns of $-\mathbf{P}^T$ (in order) among the k columns corresponding to pivots of \mathbf{G}_{RREF} , and distributing the columns of the identity matrix \mathbf{I}_{n-k} (in order) among the remaining columns.

Error-Correcting Capability under Additive Errors

Let C be a linear (n, k) code over \mathbb{F}_q . Let $E \subset \mathbb{F}_q^n$ be a general set of error patterns, and suppose that when $\mathbf{c} \in C$ is sent, an adversary may add any vector $\mathbf{e} \in E$, so that $\mathbf{y} = \mathbf{c} + \mathbf{e}$ is received.



When $\mathbf{c}_1 \in C$ is sent, the adversary can cause **confusion** at the receiver (more than one possible explanation for \mathbf{y}) if and only if there are error patterns $\mathbf{e}_1, \mathbf{e}_2 \in E$ and another codeword $\mathbf{c}_2 \in C$, $\mathbf{c}_2 \neq \mathbf{c}_1$, satisfying

$$\mathbf{c}_1 + \mathbf{e}_1 = \mathbf{c}_2 + \mathbf{e}_2 \Leftrightarrow \mathbf{c}_1 - \mathbf{c}_2 = \mathbf{e}_2 - \mathbf{e}_1$$

Since C is linear, $\mathbf{c}_1 - \mathbf{c}_2$ is in C^* and hence the adversary can cause confusion if and only if E contains two error patterns whose *difference* is a nonzero codeword.

Error-Correcting Capability (cont'd)

Theorem

Let $E \subset \mathbb{F}_q^n$ be a set of error patterns and let $\Delta E = \{\mathbf{e}_1 - \mathbf{e}_2 : \mathbf{e}_1, \mathbf{e}_2 \in E\}$. An adversary restricted to adding patterns of E to codewords of a linear code C cannot cause confusion at the receiver if and only if $\Delta E \cap C^* = \emptyset$.

Example: if E consists of the all-zero pattern and all patterns of Hamming weight one, then ΔE consists of the all-zero pattern and all patterns of Hamming weight one or two. Thus a linear code C is single-error-correcting if and only if it contains no nonzero codewords of weight smaller than 3.

Linear Codes: A Quick Summary

A linear (n, k) code over the finite field \mathbb{F}_q is a k -dimensional subspace of \mathbb{F}_q^n . Such a code C is specified by giving:

- a generator matrix \mathbf{G} whose rows form a basis for C ; or
- a parity-check matrix \mathbf{H} whose rows form a basis for the dual code C^\perp .

Then

$$C = \{\mathbf{u}\mathbf{G} : \mathbf{u} \in \mathbb{F}_q^k\} = \{\mathbf{c} \in \mathbb{F}_q^n : \mathbf{c}\mathbf{H}^T = \mathbf{0}\}.$$

Every (n, k) linear code over \mathbb{F}_q contains q^k distinct codewords.

A linear code C can correct every additive error pattern in a set E if and only if $\Delta E \cap C^* = \emptyset$, where $\Delta E = \{\mathbf{e}_1 - \mathbf{e}_2 : \mathbf{e}_1, \mathbf{e}_2 \in E\}$.

From Codes to Lattices: Construction A

Definition

The **modulo- p -reduction** of an integer vector $\mathbf{v} = (v_1, \dots, v_n) \in \mathbb{Z}^n$ is the vector

$$\mathbf{v} \bmod p = (v_1 \bmod p, \dots, v_n \bmod p) \in \mathbb{F}_p^n$$

where $\mathbb{F}_p^n = \{0, 1, \dots, p-1\}$ and $s \bmod p = r$ if $s = qp + r$ with $0 \leq r < p$. [Here we think of r simultaneously as an integer residue *and* as an element of \mathbb{F}_p , with the obvious correspondence.]

Definition (Modulo- p Lattices)

The **Construction A lifting** of a linear (n, k) code C over \mathbb{F}_p is the lattice

$$\Lambda_C = \{\mathbf{x} \in \mathbb{Z}^n : \mathbf{x} \bmod p \in C\};$$

such a lattice is sometimes called a **modulo- p lattice**.

Properties

Properties of a modulo- p lattice Λ_C :

- 1 $p\mathbb{Z}^n \subseteq \Lambda_C \subseteq \mathbb{Z}^n$.
- 2 For a linear (n, k) code C over \mathbb{F}_p , $\det(\Lambda_C) = p^{n-k}$.
- 3 Let \mathbf{G} be a generator matrix of C and \mathbf{I}_n be the $n \times n$ identity matrix, then Λ_C is spanned by the extended $n \times (n+k)$ generator matrix

$$\mathbf{G}_{\Lambda_C} = \begin{bmatrix} \mathbf{G} \\ p\mathbf{I}_n \end{bmatrix}. \quad (1)$$

- 4 If the generator matrix \mathbf{G} is of the systematic form $\mathbf{G} = [\mathbf{I}_k \ \mathbf{P}_{k \times (n-k)}]$, then the extended generator matrix (1) can be reduced to a standard $n \times n$ generator matrix for Λ_C

$$\mathbf{G}_{\Lambda_C} = \begin{bmatrix} \mathbf{I}_k & \mathbf{P}_{k \times (n-k)} \\ 0 & p\mathbf{I}_{n-k} \end{bmatrix}.$$

Nested Construction A

Consider two linear codes C_1, C_2 over \mathbb{F}_p with $C_2 \subset C_1$. By lifting the nested codes to \mathbb{R}^n using Construction A, we generate nested Construction A lattices

$$\Lambda_{C_1} = \{\mathbf{x} \in \mathbb{Z}^n \mid \mathbf{x} \bmod p \in C_1\}, \text{ and}$$

$$\Lambda_{C_2} = \{\mathbf{x} \in \mathbb{Z}^n \mid \mathbf{x} \bmod p \in C_2\}.$$

Properties

Properties of nested-Construction-A lattices $\Lambda_{C_1}, \Lambda_{C_2}$:

- 1 $p\mathbb{Z}^n \subseteq \Lambda_{C_2} \subset \Lambda_{C_1} \subseteq \mathbb{Z}^n$.
- 2 Let C_i be a linear (n, k_i) code over \mathbb{F}_p , then $\det(\Lambda_{C_i}) = p^{n-k_i}$.
- 3 There exist generator matrices $\mathbf{G}_{\Lambda_{C_1}}$ and $\mathbf{G}_{\Lambda_{C_2}}$ such that

$$\mathbf{G}_{\Lambda_{C_2}} = \text{diag}(1, \dots, 1, \underbrace{p, \dots, p}_{k_1 - k_2}) \mathbf{G}_{\Lambda_{C_1}}$$

Property 3 is an example of the “diagonal nesting” theorem of Part 1, which follows from the Smith normal form of the nesting matrix \mathbf{J} that relates $\mathbf{G}_{\Lambda_{C_2}}$ and $\mathbf{G}_{\Lambda_{C_1}}$. Used is the fact that $\det(\mathbf{J}) = p^{k_1 - k_2}$, which forces the invariant factors of \mathbf{J} to be $(1, 1, \dots, 1, p, p, \dots, p)$.

Other Constructions

- A myriad of other constructions for lattices exist; see Conway and Sloane's *SPLAG* for Construction B and Construction D.
- There are a host of number-theoretic constructions for lattices (some of them useful in space-time coding); see papers by J.-C. Belfiore, E. Viterbo, M. O. Damen, among many others.
- There are so-called “low-density lattice codes”; see papers by N. Sommer, M. Feder, O. Shalvi, and others.

For our purposes in this tutorial, Construction A will suffice.



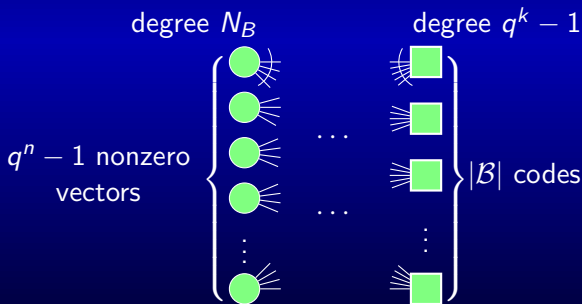
Part 4: Asymptopia

Balanced Families

Definition

A family \mathcal{B} of (n, k) linear codes over a finite field \mathbb{F} is called **balanced** if every nonzero vector in \mathbb{F}^n appears in the same number, N_B , of codes from \mathcal{B} .

For example, the set of *all* linear (n, k) codes is a balanced family.



Edge balance: $(q^n - 1)N_B = (q^k - 1)|\mathcal{B}|$

Basic Averaging Lemma

Basic averaging lemma

Let $f : \mathbb{F}_q^n \rightarrow \mathbb{C}$ be an arbitrary complex-valued function. Then

$$\frac{1}{|\mathcal{B}|} \sum_{C \in \mathcal{B}} \sum_{\mathbf{w} \in C^*} f(\mathbf{w}) = \frac{q^k - 1}{q^n - 1} \sum_{\mathbf{v} \in (\mathbb{F}_q^n)^*} f(\mathbf{v}). \quad (2)$$

Proof: Label each edge of the bipartite graph incident on circular node v with $f(v)$. Summing the labels over all edges incident on circular nodes is equivalent to summing over all edges incident on square nodes, which implies that

$$N_B \sum_{\mathbf{v} \in (\mathbb{F}_q^n)^*} f(\mathbf{v}) = \sum_{C \in \mathcal{B}} \sum_{\mathbf{w} \in C^*} f(\mathbf{w}).$$

Then (2) follows by substituting for N_B from the edge-balance condition.

First Application: Gilbert-Varshamov-like Bound

Let $A \subset \mathbb{F}_q^n$ be given, and, for $\mathbf{v} \in (\mathbb{F}_q^n)^*$, define

$$f(\mathbf{v}) = \begin{cases} 1 & \text{if } \mathbf{v} \in A, \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$\sum_{\mathbf{v} \in (\mathbb{F}_q^n)^*} f(\mathbf{v}) = |A^*| \text{ and } \sum_{\mathbf{w} \in C^*} f(\mathbf{w}) = \underbrace{|C^* \cap A|}_{\text{intersection count}},$$

for any code C of length n .

The basic averaging lemma for any balanced family \mathcal{B} of (n, k) linear codes gives

$$\underbrace{\frac{1}{|\mathcal{B}|} \sum_{C \in \mathcal{B}} |C^* \cap A|}_{\text{avg. intersection count}} = \frac{q^k - 1}{q^n - 1} |A^*|$$

First Application (cont'd)

Now if

$$\frac{q^k - 1}{q^n - 1} |A^*| < 1$$

then the average intersection count is < 1 . But since $|C^* \cap A|$ is an integer, this would mean that \mathcal{B} contains at least one code with $C^* \cap A = \emptyset$.

- Setting $A = \Delta E$, we see that if $\frac{q^k - 1}{q^n - 1} |\Delta E^*| < 1$, or more loosely if

$$|\Delta E| < q^{n-k},$$

then \mathcal{B} contains at least one (n, k) linear code that can correct all additive errors in a set E .

- For example setting E to a Hamming ball yields (essentially) the Gilbert-Varshamov bound.

Constructing mod- p Lattices of Constant Volume

It is natural to construct a family of lattices in fixed dimension n , with a fixed determinant V_f , using lifted (n, k) codes with fixed k , where $0 < k < n$. **Free parameter:** p .

Unscaled Construction A, lifting code C over \mathbb{F}_p , gives

$$\underbrace{p\mathbb{Z}^n}_{\det=p^n} \subset \underbrace{\Lambda_C}_{\det=p^{n-k}} \subset \underbrace{\mathbb{Z}^n}_{\det=1}$$

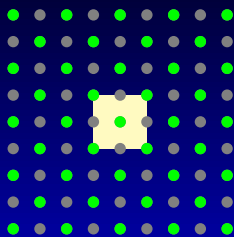
We scale everything by $\gamma > 0$, where $\gamma^n p^{n-k} = V_f$ (\dagger).

- From (\dagger), as $p \rightarrow \infty$ we must have $\gamma \rightarrow 0$.
- Since $(\gamma p)^n = p^k V_f$, we have $\gamma p \rightarrow \infty$ as $p \rightarrow \infty$.

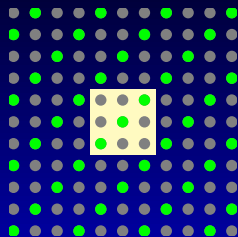
After scaling by γ we have:

$$\underbrace{\gamma p \mathbb{Z}^n}_{\det=(\gamma p)^n \rightarrow \infty} \subset \underbrace{\gamma \Lambda_C}_{\det=V_f} \subset \underbrace{\gamma \mathbb{Z}^n}_{\det=\gamma^n \rightarrow 0}$$

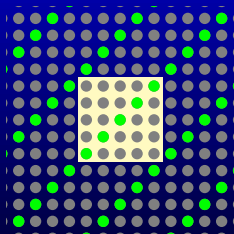
Example: Lifting $\langle(1, 1)\rangle \bmod p$ with fixed V_f



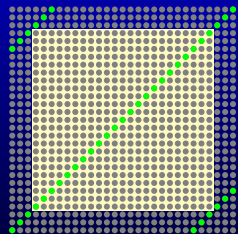
$p = 2$



$p = 3$

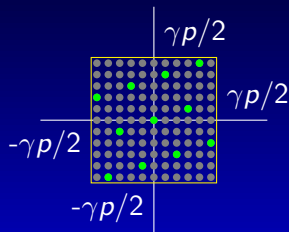


$p = 5$



$p = 23$

Yellow-shaded region: $\mathcal{V}(\gamma p \mathbb{Z}^2)$



General case

As $p \rightarrow \infty$:

- fine lattice $\gamma \mathbb{Z}^n$ grows increasingly “fine”
- Voronoi region of coarse lattice $\gamma p \mathbb{Z}^n$ grows increasingly large

Minkowski-Hlawka Theorem

Minkowski-Hlawka Theorem

Let f be a Riemann integrable function $\mathbb{R}^n \rightarrow \mathbb{R}$ of bounded support (i.e., $f(\mathbf{v}) = 0$ if $\|\mathbf{v}\|$ exceeds some bound). For $0 < k < n$, let \mathcal{B}_p be a balanced family of linear (n, k) codes over \mathbb{F}_p . Then, for any fixed V_f , the approximation

$$\frac{1}{|\mathcal{B}_p|} \sum_{C \in \mathcal{B}_p} \sum_{\mathbf{w} \in \gamma \Lambda_C^*} f(\mathbf{w}) \approx V_f^{-1} \int_{\mathbb{R}^n} f(\mathbf{v}) d\mathbf{v}$$

becomes exact in the limit as $p \rightarrow \infty$, $\gamma \rightarrow 0$ with $\gamma^n p^{n-k} = V_f$ fixed.

Minkowski-Hlawka Theorem: A Proof

Let \mathcal{V} be the Voronoi region of $\gamma p \mathbb{Z}^n$. Then, when p is sufficiently large (so that $\text{supp}(f) \subseteq \mathcal{V}$),

$$\frac{1}{|\mathcal{B}_p|} \sum_{C \in \mathcal{B}_p} \sum_{\mathbf{w} \in \gamma \Lambda_C^*} f(\mathbf{w}) = \frac{1}{|\mathcal{B}_p|} \sum_{C \in \mathcal{B}_p} \sum_{\mathbf{w} \in (\gamma \Lambda_C^* \cap \mathcal{V})} f(\mathbf{w}) \quad \text{supp}(f) \subseteq \mathcal{V}$$

$$= \frac{p^k - 1}{p^n - 1} \sum_{\mathbf{v} \in ((\gamma \mathbb{Z}^n)^* \cap \mathcal{V})} f(\mathbf{v}) \quad \text{averaging lemma}$$

$$= \frac{p^k - 1}{p^n - 1} \gamma^{-n} \sum_{\mathbf{v} \in ((\gamma \mathbb{Z}^n)^* \cap \mathcal{V})} f(\mathbf{v}) \gamma^n \quad \text{multiply by unity}$$

$$\rightarrow p^{k-n} \gamma^{-n} \int_{\mathbb{R}^n} f(\mathbf{v}) d\mathbf{v} \quad \text{sum} \rightarrow \text{integral}$$

$$= V_f^{-1} \int_{\mathbb{R}^n} f(\mathbf{v}) d\mathbf{v}.$$

Minkowski-Hlawka Theorem: Equivalent Form

Theorem

Let E be a bounded subset of \mathbb{R}^n that is Jordan-measurable (i.e., $\text{Vol}(E)$ is the Riemann integral of the indicator function of E); let k be an integer such that $0 < k < n$ and let V_f be a positive real number. Then the approximation

$$\frac{1}{|\mathcal{B}_p|} \sum_{C \in \mathcal{B}_p} |\gamma \Lambda_C^* \cap E| \approx \text{Vol}(E)/V_f$$

where \mathcal{B}_p is any balanced family of linear (n, k) codes over \mathbb{F}_p , becomes exact in the limit $p \rightarrow \infty$, $\gamma \rightarrow 0$ with $\gamma^n p^{n-k} = V_f$ fixed.

Proof of “ \Rightarrow ”: Let f be the indicator function for E (i.e., $f(v) = 1$ if $v \in E$ and $f(v) = 0$ otherwise). (The other direction is left as an exercise.)

Note: if $\text{Vol}(E)/V_f < 1$ then there exists a lattice Λ with $\det(\Lambda) = V_f$ and $|\Lambda^* \cap E| = 0$.

“Good” Lattices

To illustrate the application of the Minkowski-Hlawka Theorem, we now show that “good” lattices exist for packing and modulation in n dimensions (**existence**) and that, as $n \rightarrow \infty$, a random choice (from an appropriate ensemble) is highly likely to be good (**concentration**).

Goodness for Packing

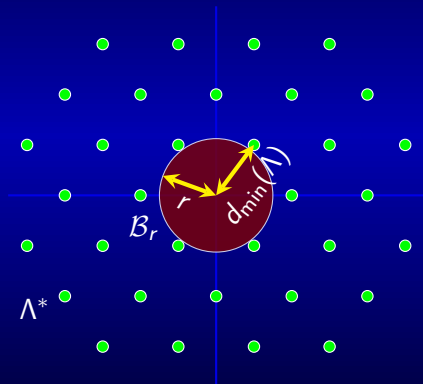
Theorem

For any $n > 1$ and any $\epsilon > 0$, there exists a lattice Λ_n of dimension n such that

$$\rho_{\text{pack}}(\Lambda_n) = \frac{r_{\text{pack}}(\Lambda_n)}{r_{\text{eff}}(\Lambda_n)} \geq \frac{1}{2(1 + \epsilon)}.$$

Lower Bound on Packing Radius

$$|\Lambda^* \cap \mathcal{B}_r| = 0 \Rightarrow d_{\min}(\Lambda) \geq r \Rightarrow r_{\text{pack}}(\Lambda) \geq r/2$$



Goodness for Packing: A Proof

For any $n > 1$ and any $\epsilon > 0$, let \mathcal{B}_r be the ball with

$$\text{Vol}(\mathcal{B}_r) = r^n V_n = V_f / (1 + \epsilon)^n < V_f.$$

Then,

$$\frac{1}{|\mathcal{B}|} \sum_{C \in \mathcal{B}} |\gamma \Lambda_C^* \cap \mathcal{B}_r| \rightarrow \text{Vol}(\mathcal{B}_r) / V_f < 1.$$

Hence, there exists a lattice Λ_n with $|\Lambda_n^* \cap \mathcal{B}_r| = 0$. This means that

$$r_{\text{pack}}(\Lambda_n) \geq r/2.$$

On the other hand, $r_{\text{eff}}(\Lambda_n) = \sqrt[n]{V_f / V_n} = r(1 + \epsilon)$. Hence,

$$\rho_{\text{pack}}(\Lambda_n) = \frac{r_{\text{pack}}(\Lambda_n)}{r_{\text{eff}}(\Lambda_n)} \geq \frac{1}{2(1 + \epsilon)}.$$

From Existence to Concentration

Concentration for Large n

Let Λ_n be a random lattice of dimension n uniformly distributed over $\{\gamma\Lambda_C^* \mid C \in \mathcal{B}\}$. Then,

$$\Pr[\Lambda_n \text{ is good for packing}] \rightarrow 1,$$

as $n \rightarrow \infty$.

Proof: Recall that $\frac{1}{|\mathcal{B}|} \sum_{C \in \mathcal{B}} |\gamma\Lambda_C^* \cap \mathcal{B}_r| \rightarrow (1/(1+\epsilon))^n$, as $p \rightarrow \infty$. Consider the random variable $|\Lambda_n^* \cap \mathcal{B}_r|$, where Λ_n is uniform over $\{\gamma\Lambda_C^* \mid C \in \mathcal{B}\}$. By Markov's inequality,

$$\Pr[|\Lambda_n^* \cap \mathcal{B}_r| \geq 1] \leq \frac{E[|\Lambda_n^* \cap \mathcal{B}_r|]}{1} = \frac{1}{|\mathcal{B}|} \sum_{C \in \mathcal{B}} |\gamma\Lambda_C^* \cap \mathcal{B}_r|.$$

Hence, $\Pr[|\Lambda_n^* \cap \mathcal{B}_r| \geq 1] \rightarrow 0$, as $n \rightarrow \infty$.

Goodness for Modulation

Recall that the **normalized volume to noise ratio** of a lattice Λ , at a target error probability P_e , $0 < P_e < 1$, is defined as

$$\mu(\Lambda, P_e) = \frac{\det(\Lambda)^{2/n}}{\sigma^2(P_e)}.$$

Theorem

There exists a sequence of lattices Λ_n such that for all $0 < P_e < 1$, $\mu(\Lambda_n, P_e) \rightarrow 2\pi e$, as $n \rightarrow \infty$.

(Suboptimal) Decoding Rule

Consider a specific (non-random) lattice Λ .

Fix a decoding radius r . Given $\mathbf{y} \in \mathbb{R}^n$, decode to a lattice point $\lambda \in \Lambda$ if

❶ $\|\mathbf{y} - \lambda\| \leq r$, and

❷ no *other* lattice point $\lambda' \in \Lambda$, $\lambda' \neq \lambda$, satisfies $\|\mathbf{y} - \lambda'\| \leq r$;

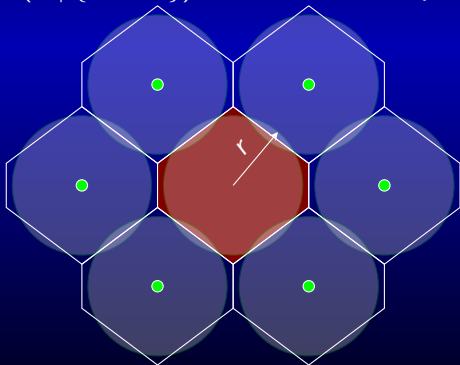
otherwise, declare an error.

Upper Bound on the Error Probability

For a specific (non-random) lattice Λ , the error probability $P_e(\Lambda)$ is upper bounded by

$$P_e(\Lambda) \leq \Pr[\mathbf{z} \notin \mathcal{B}_r] + \int_{\mathcal{B}_r} f_r(\mathbf{v}) |\Lambda^* \cap (\mathbf{v} + \mathcal{B}_r)| d\mathbf{v},$$

where $f_r(\mathbf{v}) = f_z(\mathbf{v} \mid \{\mathbf{z} \in \mathcal{B}_r\})$ is the conditional pdf.



Average Error Probability \bar{P}_e

$$\begin{aligned}\bar{P}_e &\triangleq \frac{1}{|\mathcal{B}|} \sum_{C \in \mathcal{B}} P_e(\gamma \wedge C) \\ &\leq \Pr[\mathbf{z} \notin \mathcal{B}_r] + \frac{1}{|\mathcal{B}|} \sum_{C \in \mathcal{B}} \int_{\mathcal{B}_r} f_r(\mathbf{v}) |(\gamma \wedge C)^* \cap (\mathbf{v} + \mathcal{B}_r)| d\mathbf{v} \\ &= \Pr[\mathbf{z} \notin \mathcal{B}_r] + \int_{\mathcal{B}_r} f_r(\mathbf{v}) \left(\frac{1}{|\mathcal{B}|} \sum_{C \in \mathcal{B}} |(\gamma \wedge C)^* \cap (\mathbf{v} + \mathcal{B}_r)| \right) d\mathbf{v} \\ &\rightarrow \Pr[\mathbf{z} \notin \mathcal{B}_r] + \int_{\mathcal{B}_r} f_r(\mathbf{v}) (\text{Vol}(\mathcal{B}_r)/V_f) d\mathbf{v} \\ &= \Pr[\mathbf{z} \notin \mathcal{B}_r] + \text{Vol}(\mathcal{B}_r)/V_f\end{aligned}$$

The typical “noise radius” $r_{\text{noise}} = \sqrt{n\sigma^2}$.

Claim:

If $r_{\text{noise}} = \frac{r_{\text{eff}}}{1+\epsilon}$ for some $\epsilon > 0$, then $\bar{P}_e \rightarrow 0$, as $n \rightarrow \infty$.

Average Error Probability \bar{P}_e (Cont'd)

Proof of the Claim: On the last slide we had

$$\bar{P}_e \leq \Pr[\mathbf{z} \notin \mathcal{B}_r] + \text{Vol}(\mathcal{B}_r)/V_f.$$

If $r_{\text{noise}} = r_{\text{eff}}/(1 + \epsilon)$, then there exist $\epsilon_1, \epsilon_2 > 0$ such that

$$r_{\text{noise}} = \frac{r_{\text{eff}}}{(1 + \epsilon_1)(1 + \epsilon_2)}.$$

Now, we set $r = r_{\text{eff}}/(1 + \epsilon_1)$. Then $r_{\text{noise}} = r/(1 + \epsilon_2)$,

$$\frac{\text{Vol}(\mathcal{B}_r)}{V_f} = \left(\frac{r}{r_{\text{eff}}}\right)^n = \left(\frac{1}{1 + \epsilon_1}\right)^n, \text{ and}$$

$$\begin{aligned}\Pr[\mathbf{z} \notin \mathcal{B}_r] &= \Pr[\|\mathbf{z}\| > r] \\ &= \Pr[\|\mathbf{z}\|^2/n > r^2/n] \\ &= \Pr[\|\mathbf{z}\|^2/n > \sigma^2(1 + \epsilon_2)^2].\end{aligned}$$

Note that both terms $\rightarrow 0$, as $n \rightarrow \infty$.

Goodness for Modulation: A Proof

Recall that the normalized volume to noise ratio

$$\mu(\Lambda, P_e) = \frac{\det(\Lambda)^{2/n}}{\sigma^2(P_e)}.$$

For any target error probability $\delta > 0$, if we set $r_{\text{noise}} = r_{\text{eff}}/(1 + \epsilon)$ for some $\epsilon > 0$, then $\bar{P}_e \leq \delta$ for sufficiently large n . Hence, there exists a lattice Λ_n with $P_e(\Lambda_n) \leq \delta$ and $\sigma^2(\delta) \geq r_{\text{noise}}^2/n$.

Therefore,

$$\mu(\Lambda_n, \delta) = \frac{V_f^{2/n}}{\sigma^2(\delta)} \leq \frac{V_f^{2/n}}{r_{\text{noise}}^2/n} = nV_n^{2/n} \frac{r_{\text{eff}}^2}{r_{\text{noise}}^2} \rightarrow 2\pi e(1 + \epsilon)^2.$$

The theorem follows because we can make ϵ arbitrarily small.

From Existence to Concentration

Concentration for Large n

Let Λ_n be a random lattice of dimension n uniformly distributed over $\{\gamma\Lambda_C^* \mid C \in \mathcal{B}\}$. Then,

$$\Pr[\Lambda_n \text{ is good for modulation}] \rightarrow 1,$$

as $n \rightarrow \infty$.

Proof: For any target error probability $\delta > 0$ and any large $L > 0$, if we set $r_{\text{noise}} = r_{\text{eff}}/(1 + \epsilon)$ for some $\epsilon > 0$, then $\bar{P}_e \leq \delta/L$ for sufficiently large n .

Consider the random variable $P_e(\Lambda_n)$, where Λ_n is uniform over $\{\gamma\Lambda_C^* \mid C \in \mathcal{B}\}$. By Markov's inequality,

$$\Pr[P_e(\Lambda_n) \geq \delta] \leq \frac{E[P_e(\Lambda_n)]}{\delta} = \frac{\bar{P}_e}{\delta} \leq \frac{1}{L}.$$

Hence, with probability at least $1 - 1/L$, Λ_n has $P_e(\Lambda_n) \leq \delta$ and $\sigma^2(\delta) \geq r_{\text{noise}}^2/n$.

Simultaneous Goodness

Theorem

Let Λ_n be a random lattice of dimension n uniformly distributed over $\{\gamma\Lambda_C^* \mid C \in \mathcal{B}\}$. Then for any $0 < P_e < 1$ and any $\epsilon > 0$,

$$\Pr \left[\rho_{\text{pack}}(\Lambda_n) \geq \frac{1}{2(1+\epsilon)} \text{ and } \mu(\Lambda_n, P_e) \leq 2\pi e(1+\epsilon) \right] \rightarrow 1$$

as $n \rightarrow \infty$.

Proof: a union-bound argument.

Goodness of Nested Lattices

- Previously, the use of the Minkowski-Hlawka Theorem, together with a balanced family of linear codes, proves the existence and concentration of “good” lattices.
- This naturally extends to nested lattices, if nested Construction A is applied to some appropriate linear-code ensemble.
- For example, let \mathcal{B} be the set of all linear (n, k) codes, and let \mathcal{B}' be the set of all linear (n, k') codes with $k' < k$. Then, for all possible linear codes $C_1 \in \mathcal{B}$, $C_2 \in \mathcal{B}'$ with $C_2 \subset C_1$, we generate corresponding nested-Construction-A lattices Λ_{C_1} and Λ_{C_2} .
- This ensemble allows us to prove the existence and concentration of “good” nested lattices for packing and modulation.

Nested Lattices Good for (Almost) Everything

In fact, with a refined argument, one can prove that, with high probability, both Λ_n and Λ'_n are simultaneously good for packing, modulation, covering, and quantization.

Remark 1: goodness for covering implies goodness for quantization

Remark 2: in order to prove goodness for covering, we need some constraints on k and k' of the underlying linear codes. This is beyond the scope of this tutorial.

Practical Ensembles of Lattices

For linear codes, practical ensembles include Turbo codes, LDPC codes, Polar codes, Spatially-Coupled LDPC codes.

What about their lattice versions?

- LDPC Lattices: M.-R. Sadeghi, A. H. Banihashemi, and D. Panario, 2006
- Low-Density Lattice Codes: N. Sommer, M. Feder, and O. Shalvi, 2008
- Low-Density Integer Lattices: N. Di Pietro, J. J. Boutros, G. Zémor, and L. Brunel, 2012
- Turbo Lattices: A. Sakzad, M.-R. Sadeghi, and D. Panario, 2012
- Polar Lattices: Y. Yan, C. Ling, and X. Wu, 2013
- Spatially-Coupled Low-Density Lattices: A. Vem, Y.-C. Huang, K. Narayanan, and H. Pfister, 2014

Towards a Unified Framework

A unified framework

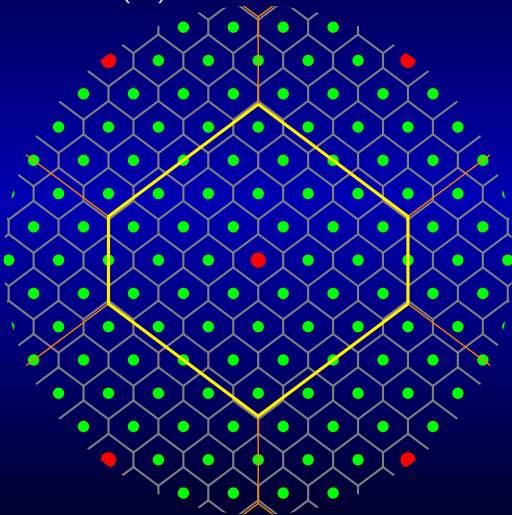
It is possible to generalize the balanced families to “almost balanced” families so that goodness of some (practical) linear codes over \mathbb{F}_p implies goodness of lattices.

For goodness of linear LDPC codes, see, e.g.,

- U. Erez and G. Miller. The ML decoding performance of LDPC ensembles over \mathbb{Z}_q . *IEEE Trans. Inform. Theory*, **51**:1871–1879, May 2005.
- G. Como and F. Fagnani. Average spectra and minimum distances of LDPC codes over abelian groups. *SIAM J. Discrete Math.*, **23**:19–53, 2008.
- S. Yang, T. Honold, Y. Chen, Z. Zhang, and P. Qiu. Weight distributions of regular LDPC codes over finite fields. *IEEE Trans. Inform. Theory*, **57**:7507–7521, Nov. 2011.

Nested Lattice Codes — Voronoi Constellations

For $\Lambda' \subset \Lambda$, define a finite codebook—a Voronoi constellation—via $\Lambda \cap \mathcal{V}(\Lambda')$.



- Λ is the “fine lattice”
- Λ' is the “shaping lattice”
- The points of the constellation are coset representatives of Λ/Λ' ; it is often convenient to have a “linear labelling” achieved via diagonal nesting.

Encoding

Encoding is convenient when we have diagonal nesting (as is always possible), and

$$\mathbf{G}_{\Lambda'} = \text{diag}(c_1, c_2, \dots, c_n) \mathbf{G}_{\Lambda}$$

Then we encode a message $m \in \mathbb{Z}_{c_1} \times \mathbb{Z}_{c_2} \times \dots \times \mathbb{Z}_{c_n}$ to $m\mathbf{G}_{\Lambda}$, subtracting the nearest point of Λ' , i.e.,

$$m \mapsto m\mathbf{G}_{\Lambda} \bmod \Lambda' \triangleq m\mathbf{G}_{\Lambda} - \mathcal{Q}_{\Lambda'}^{(NN)}(m\mathbf{G}_{\Lambda}).$$

The result is always a point in $\mathcal{V}(\Lambda')$.

Encoding with a Random Dither

Let \mathbf{u} be continuously and uniformly distributed over $\mathcal{V}(\Lambda')$. (In transmission applications, \mathbf{u} is pseudorandom and known to both transmitter and receiver.) We add \mathbf{u} to $\boldsymbol{\lambda} \in \Lambda$ prior to implementing the mod Λ' operation.

Purpose of dither: to control the average power

Let

$$\begin{aligned}\mathbf{x} &= [\boldsymbol{\lambda} + \mathbf{u}] \bmod \Lambda' \\ &= \boldsymbol{\lambda} + \mathbf{u} - \mathcal{Q}_{\Lambda'}^{\text{NN}}(\boldsymbol{\lambda} + \mathbf{u})\end{aligned}$$

Clearly, $\mathbf{x} \in \mathcal{V}(\Lambda')$, and we will now show that in fact \mathbf{x} is uniformly distributed and hence has

$$\frac{1}{n} E[\|\mathbf{x}\|^2] = \sigma^2(\Lambda').$$

The Role of the Random Dither

Crypto Lemma

If the dither \mathbf{u} is uniform over the Voronoi region $\mathcal{V}(\Lambda')$ and independent of $\boldsymbol{\lambda}$, then $\mathbf{x} = [\boldsymbol{\lambda} + \mathbf{u}] \bmod \Lambda'$ is uniform over $\mathcal{V}(\Lambda')$, independent of $\boldsymbol{\lambda}$.

Hence, $\frac{1}{n} E[\|\mathbf{x}\|^2] = \sigma^2(\Lambda')$.

In practice one often uses a non-random dither chosen to achieve a transmitted signal with zero mean.

Decoding

A sensible (though suboptimal) decoding rule at the output of a Gaussian noise channel:

- Given \mathbf{y} , map $\mathbf{y} - \mathbf{u}$ to the nearest point of the fine lattice Λ .
- Reduce mod Λ' if necessary.

$$\hat{\lambda} = Q_{\Lambda}^{\text{NN}}(\mathbf{y} - \mathbf{u}) \bmod \Lambda'$$

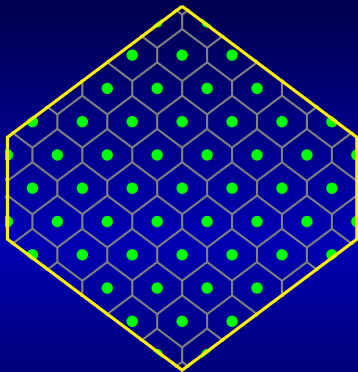
Understanding the decoding: Let $\lambda' = Q_{\Lambda'}^{\text{NN}}(\lambda + \mathbf{u})$. Then,

$$\begin{aligned}\mathbf{y} - \mathbf{u} &= \mathbf{x} + \mathbf{z} - \mathbf{u} \\ &= \underbrace{\lambda + \mathbf{u} - \lambda'}_{\mathbf{x}} + \mathbf{z} - \mathbf{u} \\ &= \lambda + \mathbf{z} - \lambda'\end{aligned}$$

Hence, $\hat{\lambda} = \lambda$ if and only if $Q_{\Lambda}^{\text{NN}}(\mathbf{z}) \in \Lambda'$. Therefore,

$$\Pr[\hat{\lambda} \neq \lambda] = \Pr[Q_{\Lambda}^{\text{NN}}(\mathbf{z}) \notin \Lambda'] \leq \Pr[Q_{\Lambda}^{\text{NN}}(\mathbf{z}) \neq \mathbf{0}] = \Pr[\mathbf{z} \notin \mathcal{V}(\Lambda)].$$

Rate



$$R = \frac{1}{n} \log_2 \frac{\det(\Lambda')}{\det(\Lambda)}$$

Rate versus SNR

$$\begin{aligned} R &= \frac{1}{n} \log_2 \frac{\det(\Lambda')}{\det(\Lambda)} \\ &= \frac{1}{2} \log_2 \left(\frac{\det(\Lambda')^{2/n}}{\det(\Lambda)^{2/n}} \right) \\ &= \frac{1}{2} \log_2 \left(\frac{\sigma^2(\Lambda')/G(\Lambda')}{\sigma^2(P_e) \cdot \mu(\Lambda, P_e)} \right) \\ &= \frac{1}{2} \log_2 \left(\frac{\sigma^2(\Lambda')}{\sigma^2(P_e)} \right) - \frac{1}{2} \log_2 (G(\Lambda') \cdot \mu(\Lambda, P_e)) \\ &= \frac{1}{2} \log_2 \left(\frac{P}{N} \right) - \underbrace{\frac{1}{2} \log_2 (2\pi e G(\Lambda'))}_{\text{shaping loss}} - \underbrace{\frac{1}{2} \log_2 \left(\frac{\mu(\Lambda, P_e)}{2\pi e} \right)}_{\text{coding loss}}. \end{aligned}$$

Summary of Nested Lattice Codes


For a specific nested lattice code with $\Lambda' \subset \Lambda$,

$$R = \frac{1}{2} \log_2 \left(\frac{P}{N} \right) - \underbrace{\frac{1}{2} \log_2 (2\pi e G(\Lambda'))}_{\text{shaping loss}} - \underbrace{\frac{1}{2} \log_2 \left(\frac{\mu(\Lambda, P_e)}{2\pi e} \right)}_{\text{coding loss}}.$$

If Λ' is good for quantization (i.e., $G(\Lambda') \rightarrow \frac{1}{2\pi e}$) and Λ is good for modulation (i.e., $\mu(\Lambda, P_e) \rightarrow 2\pi e$), then both losses $\rightarrow 0$.

Recall that $G(\mathbb{Z}^n) = 1/12$. Hence, the uncoded transmission has a shaping loss of $\frac{1}{2} \log_2(2\pi e/12) \approx 0.254$.

Compared to $R = \frac{1}{2} \log_2 \left(1 + \frac{P}{N} \right)$, what about the “1+” term? – see Part 5!



Part 5: Applications in Communications

Outline

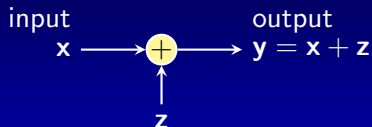
- ① AWGN Channel Coding
- ② Dirty-Paper Coding
- ③ Two-Way Relay Channel
- ④ Compute-and-Forward
- ⑤ Successive Compute-and-Forward

Outline

- ① AWGN Channel Coding
- ② Dirty-Paper Coding
- ③ Two-Way Relay Channel
- ④ Compute-and-Forward
- ⑤ Successive Compute-and-Forward

See appendix!

AWGN Channel Coding



$\mathbf{y} = \mathbf{x} + \mathbf{z}$, where $\mathbf{z}_i \sim \mathcal{N}(0, N)$, independent components, and independent of \mathbf{x} .

Average power constraint: $\frac{1}{n}E[\|\mathbf{x}\|^2] \leq P$.

$$C_{\text{AWGN}} = \frac{1}{2} \log_2 \left(1 + \frac{P}{N} \right)$$

Key Intuition (Erez&Zamir'04)

Intuition: consider $Y = X + Z$, where $X \sim \mathcal{N}(0, 1)$ and $Z \sim \mathcal{N}(0, 10)$. Taking Y as an estimate of X would give us an MSE ten times larger than the variance of X !

If we use αY as an estimate, then the estimation error is

$$\alpha Y - X = \alpha(X + Z) - X = (\alpha - 1)X + \alpha Z,$$

with $\text{MSE}(\alpha) = (\alpha - 1)^2 \cdot 1 + \alpha^2 \cdot 10$.

In fact, the optimal α^* (i.e., the MMSE coefficient) is $1/11$, and

$$\text{MSE}(\alpha^*) = 110/121 < 1.$$

This shows the value of **prior information**!

Lesson Learned: we should use prior information in decoding!

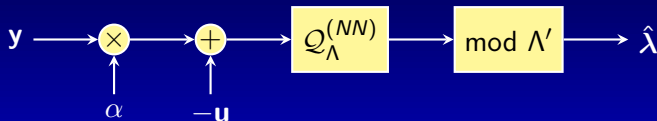
Encoding with a Random Dither

The encoding is the same as before.

$$\begin{aligned}\mathbf{x} &= [\boldsymbol{\lambda} + \mathbf{u}] \bmod \Lambda' \\ &= \boldsymbol{\lambda} + \mathbf{u} - \mathcal{Q}_{\Lambda'}^{\text{NN}}(\boldsymbol{\lambda} + \mathbf{u})\end{aligned}$$

Clearly, $\mathbf{x} \in \mathcal{V}(\Lambda')$ and $\frac{1}{n}E[\|\mathbf{x}\|^2] = \sigma^2(\Lambda')$.

Decoding with the MMSE Estimator



$$\hat{\lambda} = \mathcal{Q}_{\Lambda}^{\text{NN}}(\alpha \mathbf{y} - \mathbf{u}) \text{ mod } \Lambda',$$

where α is the MMSE coefficient.

Note that when $\alpha = 1$, it reduces to our previous case.

Error Probability

Let $\lambda' = \mathcal{Q}_{\Lambda'}^{\text{NN}}(\lambda + \mathbf{u})$. Then,

$$\begin{aligned}\alpha \mathbf{y} - \mathbf{u} &= \alpha(\mathbf{x} + \mathbf{z}) - \mathbf{u} \\ &= \alpha(\underbrace{\lambda + \mathbf{u} - \lambda'}_{\mathbf{x}} + \mathbf{z}) - \mathbf{u} \\ &= \lambda + (\alpha - 1)(\lambda + \mathbf{u} - \lambda') + \alpha \mathbf{z} - \lambda' \\ &= \lambda + \underbrace{(\alpha - 1)\mathbf{x} + \alpha \mathbf{z} - \lambda'}_{\mathbf{n}_\alpha}\end{aligned}$$

Hence, $\hat{\lambda} = \lambda$ if and only if $\mathcal{Q}_{\Lambda}^{\text{NN}}(\mathbf{n}_\alpha) \in \Lambda'$. Therefore,

$$\begin{aligned}P_e &\triangleq \Pr[\hat{\lambda} \neq \lambda] \\ &= \Pr[\mathcal{Q}_{\Lambda}^{\text{NN}}(\mathbf{n}_\alpha) \notin \Lambda'] \\ &\leq \Pr[\mathcal{Q}_{\Lambda}^{\text{NN}}(\mathbf{n}_\alpha) \neq \mathbf{0}] \\ &= \Pr[\mathbf{n}_\alpha \notin \mathcal{V}(\Lambda)].\end{aligned}$$

The Role of the MMSE Estimator

The effective channel noise is \mathbf{n}_α (instead of \mathbf{z}), and the second moment per dimension of \mathbf{n}_α is

$$\begin{aligned}\sigma^2(\mathbf{n}_\alpha) &\triangleq \frac{1}{n} E[\|\mathbf{n}_\alpha\|^2] \\ &= (\alpha - 1)^2 \sigma^2(\mathbf{x}) + \alpha^2 \sigma^2(\mathbf{z}) \\ &= (\alpha - 1)^2 P + \alpha^2 N.\end{aligned}$$

The optimal $\alpha^* = P/(P + N)$, and

$$\sigma^2(\mathbf{n}_{\alpha^*}) = \frac{PN}{P + N} < \min\{P, N\}.$$

Now, the achievable rate

$$R = \frac{1}{2} \log_2 \left(\frac{P}{\sigma^2(\mathbf{n}_{\alpha^*})} \right) = \frac{1}{2} \log_2 \left(\frac{P}{\frac{PN}{P+N}} \right) = \frac{1}{2} \log_2 \left(1 + \frac{P}{N} \right).$$

Caution

Previous argument is heuristic, since \mathbf{n}_{α^*} is not Gaussian...
To address this issue, we only need to prove that

$$\Pr[\|\mathbf{n}_{\alpha^*}\|^2/n > \sigma^2(\mathbf{n}_{\alpha^*})(1 + \epsilon_2)^2] \rightarrow 0,$$

as $n \rightarrow \infty$.

This can be done with some additional steps.

Conclusion

- ① Fundamentals
- ② Packing, Covering, Quantization, Modulation
- ③ Lattices and Linear Codes
- ④ Asymptopia
- ⑤ Communications Applications

Lattices give a *structured* approach to Gaussian information theory problems, though the asymptotic results are still based on random-(linear)-coding arguments.

Much work can be done in applying these tools to new problems, and searching for constructions having tractable implementation complexity.

Fundamentals of Lattices

- 1 J. W. H. Cassels. *An Introduction to the Geometry of Numbers*. Springer, 1971.
- 2 J. H. Conway and N. J. A. Sloane. *Sphere Packings, Lattices and Groups*. Springer-Verlag, New York, 3rd Ed., 1999.
- 3 P. M. Gruber and C. G. Lekkerkerker. *Geometry of Numbers*. North-Holland Mathematical Library, Vol. 37, 1987.
- 4 D. Micciancio and S. Goldwasser. *Complexity of Lattice Problems: A Cryptographic Perspective*. Kluwer, 2002.
- 5 V. Vaikuntanathan. *Lattices in Computer Science*. Class notes at the University of Toronto.
- 6 R. Zamir. *Lattice Coding for Signals and Networks*. Cambridge University Press, Cambridge, 2014.
- 7 M. Viazovska, “The sphere packing problem in dimension 8,” arxiv.org/abs/1603.04246.

Bibliography (Cont'd)

Asymptotically-Good Lattices

- 1 U. Erez, S. Litsyn, and R. Zamir. Lattices which are good for (almost) everything. *IEEE Trans. Inform. Theory*, **51**:3401–3416, Oct. 2005.
- 2 G. D. Forney, M. D. Trott, and S.-Y. Chung. Sphere-bound-achieving coset codes and multilevel coset codes. *IEEE Trans. Inform. Theory*, **46**:820–850, May 2000.
- 3 H. A. Loeliger. Averaging bounds for lattices and linear codes. *IEEE Trans. Inform. Theory*, **43**:1767–1773, Nov. 1997.
- 4 O. Ordentlich and U. Erez. A simple proof for the existence of good pairs of nested lattices. In *Proc. of IEEEI*, 2012.
- 5 N. D. Pietro. *On Infinite and Finite Lattice Constellations for the Additive White Gaussian Noise Channel*. PhD Thesis, 2014.
- 6 C. A. Rogers. *Packing and Covering*. Cambridge University Press, Cambridge, 1964.

Bibliography (Cont'd)

Applications of Lattices

- 1 U. Erez, S. Shamai (Shitz), and R. Zamir. Capacity and lattice strategies for cancelling known interference. *IEEE Trans. Inform. Theory*, **51**:3820–3833, Nov. 2005.
- 2 U. Erez and R. Zamir. Achieving $1/2 \log(1 + \text{SNR})$ on the AWGN channel with lattice encoding and decoding. *IEEE Trans. Inform. Theory*, **50**:2293–2314, Oct. 2004.
- 3 B. Nazer and M. Gastpar. Compute-and-forward: harnessing interference through structured codes. *IEEE Trans. Inform. Theory*, **57**:6463–6486, Oct. 2011.
- 4 M. P. Wilson, K. Narayanan, H. Pfister, and A. Sprintson. Joint physical layer coding and network coding for bidirectional relaying. *IEEE Trans. Inform. Theory*, **56**:5641–5654, Nov. 2010.

Bibliography (Cont'd)

More on Applications of Lattices

- 1 C. Feng, D. Silva, and F. R. Kschischang. An algebraic approach to physical-layer network coding. *IEEE Trans. Inform. Theory*, **59**:7576–7596, Nov. 2013.
- 2 W. Nam, S.-Y. Chung, and Y. H. Lee. Capacity of the Gaussian two-way relay channel to within 1/2 bit. *IEEE Trans. Inform. Theory*, **56**:5488–5494, Nov. 2010.
- 3 B. Nazer. Successive compute-and-forward. In *Proc. of IZS*, 2012.
- 4 R. Zamir, S. Shamai, and U. Erez. Nested linear/lattice codes for structured multiterminal binning. *IEEE Trans. Inform. Theory*, **48**:1250–1276, Jun. 2002.
- 5 J. Zhu and M. Gastpar. Gaussian multiple access via compute-and-forward. *IEEE Trans. Inform. Theory*, **63**:2678–2695, 2017.

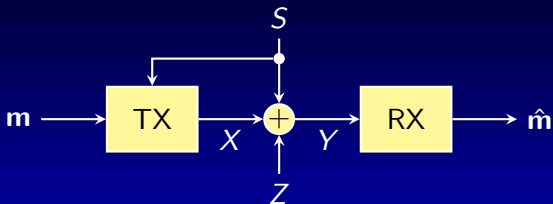


Appendix: Further Schemes

Outline

- ① AWGN Channel Coding
- ② Dirty-Paper Coding
- ③ Two-Way Relay Channel
- ④ Compute-and-Forward
- ⑤ Successive Compute-and-Forward

Dirty-Paper Coding



In the dirty-paper channel $Y = X + S + Z$, where Z is an unknown additive noise, and S is an interference signal known to the transmitter but not to the receiver.

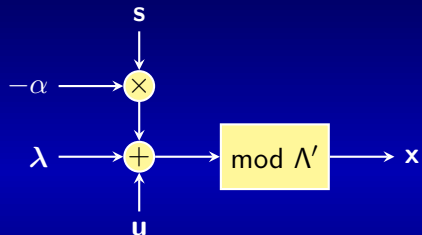
The channel input satisfies an average power constraint:

$$E\|\mathbf{x}\|^2 \leq nP.$$

If S and Z are statistically independent Gaussian variables, then the channel capacity

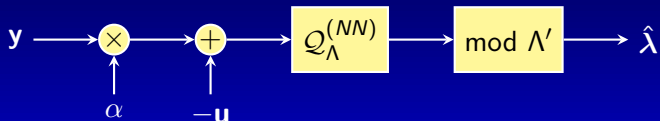
$$C_{\text{DP}} = C_{\text{AWGN}} = \frac{1}{2} \log_2 \left(1 + \frac{P}{N} \right).$$

Encoding



$$\mathbf{x} = [\boldsymbol{\lambda} + \mathbf{u} - \alpha \mathbf{s}] \bmod \Lambda'$$

Decoding



$$\hat{\lambda} = Q_{\Lambda}^{\text{NN}}(\alpha \mathbf{y} - \mathbf{u}) \bmod \Lambda',$$

where α is the MMSE coefficient.

Error Probability

Let $\lambda' = Q_{\Lambda'}^{\text{NN}}(\lambda + \mathbf{u} - \alpha \mathbf{s})$. Then,

$$\begin{aligned}\alpha \mathbf{y} - \mathbf{u} &= \alpha(\mathbf{x} + \mathbf{s} + \mathbf{z}) - \mathbf{u} \\ &= \alpha(\underbrace{\lambda + \mathbf{u} - \alpha \mathbf{s} - \lambda'}_{\mathbf{x}} + \mathbf{s} + \mathbf{z}) - \mathbf{u} \\ &= \lambda + (\alpha - 1)(\lambda + \mathbf{u} - \alpha \mathbf{s} - \lambda') + \alpha \mathbf{z} - \lambda' \\ &= \lambda + \underbrace{(\alpha - 1)\mathbf{x} + \alpha \mathbf{z} - \lambda'}_{\mathbf{n}_\alpha}\end{aligned}$$

Once again, $\hat{\lambda} = \lambda$ if and only if $Q_{\Lambda}^{\text{NN}}(\mathbf{n}_\alpha) \in \Lambda'$. Therefore,

$$P_e \triangleq \Pr[\hat{\lambda} \neq \lambda] \leq \Pr[\mathbf{n}_\alpha \notin \mathcal{V}(\Lambda)].$$

Achievable Rate

Recall that $\mathbf{n}_\alpha = (\alpha - 1)\mathbf{x} + \alpha\mathbf{z}$ with

$$\sigma^2(\mathbf{n}_\alpha) = (\alpha - 1)^2 P + \alpha^2 N.$$

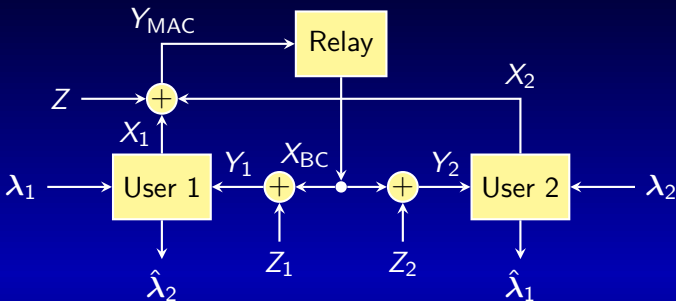
Once again, the optimal $\alpha^* = P/(P + N)$ and

$$\sigma^2(\mathbf{n}_{\alpha^*}) = \frac{PN}{P + N}.$$

Hence, the achievable rate

$$R = \frac{1}{2} \log_2 \left(\frac{P}{\sigma^2(\mathbf{n}_{\alpha^*})} \right) = \frac{1}{2} \log_2 \left(1 + \frac{P}{N} \right).$$

Gaussian Two-Way Relay Channel



$$Y_{MAC} = X_1 + X_2 + Z \quad Y_1 = X_{BC} + Z_1 \quad Y_2 = X_{BC} + Z_2$$

where $Z \sim \mathcal{N}(0, N)$, $Z_1 \sim \mathcal{N}(0, N_1)$, and $Z_2 \sim \mathcal{N}(0, N_2)$.

Average power constraints:

$$\frac{1}{n}E[\|\mathbf{x}_1\|^2] \leq P_1, \quad \frac{1}{n}E[\|\mathbf{x}_2\|^2] \leq P_2, \quad \text{and} \quad \frac{1}{n}E[\|\mathbf{x}_{BC}\|^2] \leq P_{BC}.$$

For simplicity, we first consider the symmetric case $P_1 = P_2 = P_{BC}$ and $N_1 = N_2 = N$.

Transmission Strategy

Two-phase transmission strategy:

- 1 1st phase: the relay recovers

$$\lambda = [\lambda_1 + \lambda_2] \pmod{\Lambda'}$$

from the received signal \mathbf{y}_{MAC} .

- 2 2nd phase: the relay broadcasts λ to both nodes.
- 3 Clearly, $\lambda_1 = [\lambda - \lambda_2] \pmod{\Lambda'}$ and $\lambda_2 = [\lambda - \lambda_1] \pmod{\Lambda'}$.

1st Phase

Encoding:

$$\mathbf{x}_1 = [\boldsymbol{\lambda}_1 + \mathbf{u}_1] \pmod{\Lambda'}$$

$$\mathbf{x}_2 = [\boldsymbol{\lambda}_2 + \mathbf{u}_2] \pmod{\Lambda'}$$

Decoding:

$$\hat{\boldsymbol{\lambda}} = \mathcal{Q}_{\Lambda}^{\text{NN}}(\alpha \mathbf{y} - \mathbf{u}_1 - \mathbf{u}_2) \pmod{\Lambda'}$$

1st Phase: Error Probability

Let $\lambda'_i = \mathcal{Q}_{\Lambda'}^{\text{NN}}(\lambda_i + \mathbf{u}_i)$ for $i = 1, 2$. Then,

$$\begin{aligned}\alpha \mathbf{y} - \mathbf{u}_1 - \mathbf{u}_2 &= \alpha(\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{z}) - \mathbf{u}_1 - \mathbf{u}_2 \\ &= \alpha\left(\sum_i \underbrace{(\lambda_i + \mathbf{u}_i - \lambda'_i)}_{\mathbf{x}_i} + \mathbf{z}\right) - \mathbf{u}_1 - \mathbf{u}_2 \\ &= \lambda_1 + \lambda_2 + (\alpha - 1) \sum_i (\lambda_i + \mathbf{u}_i - \lambda'_i) + \alpha \mathbf{z} - \lambda'_1 - \lambda'_2 \\ &= \lambda_1 + \lambda_2 + \underbrace{(\alpha - 1)(\mathbf{x}_1 + \mathbf{x}_2)}_{\mathbf{n}_\alpha} + \alpha \mathbf{z} - \lambda'_1 - \lambda'_2.\end{aligned}$$

Note that $\hat{\lambda} = [\lambda_1 + \lambda_2] \bmod \Lambda'$ if and only if $\mathcal{Q}_{\Lambda'}^{\text{NN}}(\mathbf{n}_\alpha) \in \Lambda'$.

Hence,

$$P_e \leq \Pr[\mathbf{n}_\alpha \in \mathcal{V}(\Lambda)].$$

1st Phase: Achievable Rate

Note that

$$\sigma^2(\mathbf{n}_a) = (\alpha - 1)^2 (\sigma^2(\mathbf{x}_1) + \sigma^2(\mathbf{x}_2)) + \alpha^2 \sigma^2(\mathbf{z}) = (\alpha - 1)^2 2P + \alpha^2 N.$$

The optimal $\alpha^* = 2P/(2P + N)$ and

$$\sigma^2(\mathbf{n}_{\alpha^*}) = \frac{2PN}{2P + N}.$$

Hence, the achievable rate

$$R = \frac{1}{2} \log_2 \left(\frac{P}{\sigma^2(\mathbf{n}_{\alpha^*})} \right) = \frac{1}{2} \log_2 \left(\frac{1}{2} + \frac{P}{N} \right).$$

Summary of the Symmetric Case

Since decoding in 1st phase is “harder” than the 2nd phase, we have the following achievable rate

$$R_1 = R_2 = \frac{1}{2} \log_2 \left(\frac{1}{2} + \frac{P}{N} \right).$$

In this case, the cut-set bound = $\frac{1}{2} \log_2 \left(1 + \frac{P}{N} \right)$.

The achievable rate approaches the cut-set bound at high SNR!

Asymmetric Powers

Recall that the channel model is

$$Y_{\text{MAC}} = X_1 + X_2 + Z$$

$$Y_1 = X_{\text{BC}} + Z_1$$

$$Y_2 = X_{\text{BC}} + Z_2$$

where $Z \sim \mathcal{N}(0, N)$, $Z_1 \sim \mathcal{N}(0, N_1)$, and $Z_2 \sim \mathcal{N}(0, N_2)$.

Asymmetric power constraints:

$$\frac{1}{n} E[\|\mathbf{x}_1\|^2] \leq P_1, \frac{1}{n} E[\|\mathbf{x}_2\|^2] \leq P_2, \text{ and } \frac{1}{n} E[\|\mathbf{x}_{\text{BC}}\|^2] \leq P_{\text{BC}}.$$

Symmetric noise variance:

$$N_1 = N_2 = N$$

Key idea: use the same fine lattice at both users but different coarse lattices, each sized to meet its user's power constraint

A Triple of Nested Lattices

$$\Lambda'_1 \subset \Lambda'_2 \subset \Lambda$$

with

$$\sigma^2(\Lambda'_1) = P_1 \text{ and } \sigma^2(\Lambda'_2) = P_2,$$

$$R_1 = \frac{1}{n} \log_2 \frac{\det(\Lambda'_1)}{\det(\Lambda)} \text{ and } R_2 = \frac{1}{n} \log_2 \frac{\det(\Lambda'_2)}{\det(\Lambda)}$$

1st Phase: Encoding

$$\begin{aligned}\mathbf{x}_1 &= [\boldsymbol{\lambda}_1 + \mathbf{u}_1] \bmod \Lambda'_1 \\ \mathbf{x}_2 &= [\boldsymbol{\lambda}_2 + \mathbf{u}_2] \bmod \Lambda'_2\end{aligned}$$

Clearly,

$$\frac{1}{n} E[\|\mathbf{x}_i\|^2] = \sigma^2(\Lambda'_i) = P_i.$$

1st Phase: Decoding

$$\hat{\lambda} = \mathcal{Q}_{\Lambda}^{\text{NN}}(\alpha \mathbf{y} - \mathbf{u}_1 - \mathbf{u}_2) \pmod{\Lambda'_1}$$

To understand the decoding, let $\lambda'_i = \mathcal{Q}_{\Lambda'_i}^{\text{NN}}(\lambda_i + \mathbf{u}_i)$ for $i = 1, 2$.

Then, once again,

$$\alpha \mathbf{y} - \mathbf{u}_1 - \mathbf{u}_2 = \lambda_1 + \lambda_2 + \mathbf{n}_\alpha - \lambda'_1 - \lambda'_2,$$

where

$$\mathbf{n}_\alpha \triangleq (\alpha - 1)(\mathbf{x}_1 + \mathbf{x}_2) + \alpha \mathbf{z}.$$

Let $\lambda = [\lambda_1 + \lambda_2 - \lambda'_2] \pmod{\Lambda'_1}$. Then,

$$\hat{\lambda} = \lambda \text{ if and only if } \mathcal{Q}_{\Lambda}^{\text{NN}}(\mathbf{n}_\alpha) \in \Lambda'_1.$$

1st Phase: Achievable Rates

Note that

$$\sigma^2(\mathbf{n}_a) = (\alpha-1)^2 (\sigma^2(\mathbf{x}_1) + \sigma^2(\mathbf{x}_2)) + \alpha^2 \sigma^2(\mathbf{z}) = (\alpha-1)^2 (P_1 + P_2) + \alpha^2 N.$$

The optimal $\alpha^* = (P_1 + P_2)/(P_1 + P_2 + N)$ and

$$\sigma^2(\mathbf{n}_{\alpha^*}) = \frac{(P_1 + P_2)N}{P_1 + P_2 + N}.$$

Hence, $\boldsymbol{\lambda} = [\boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2 - \boldsymbol{\lambda}'_2] \bmod \Lambda'_1$ can be decoded reliably if

$$R_1 \leq \frac{1}{2} \log_2 \left(\frac{P_1}{\sigma^2(\mathbf{n}_{\alpha^*})} \right) = \frac{1}{2} \log_2 \left(\frac{P_1}{P_1 + P_2} + \frac{P_1}{N} \right)$$

$$R_2 \leq \frac{1}{2} \log_2 \left(\frac{P_2}{\sigma^2(\mathbf{n}_{\alpha^*})} \right) = \frac{1}{2} \log_2 \left(\frac{P_2}{P_1 + P_2} + \frac{P_2}{N} \right)$$

2nd Phase: Coding Scheme

Encoding: The relay sends

$$\lambda = [\lambda_1 + \lambda_2 - \lambda'_2] \pmod{\Lambda'_1}.$$

Decoding: Upon decoding λ , node 1 recovers λ_2 and node 2 recovers λ_1 .

This is feasible, because

$$[\lambda - \lambda_1] \pmod{\Lambda'_2} = \lambda_2$$

and

$$[\lambda - \lambda_2 + \lambda'_2] \pmod{\Lambda'_1} = \lambda_1.$$

2nd Phase: Achievable Rates

$\lambda = [\lambda_1 + \lambda_2 - \lambda'_2] \bmod \Lambda'_1$ can be decoded reliably if

$$R_1, R_2 \leq \frac{1}{2} \log_2 \left(1 + \frac{P_{\text{BC}}}{N} \right).$$

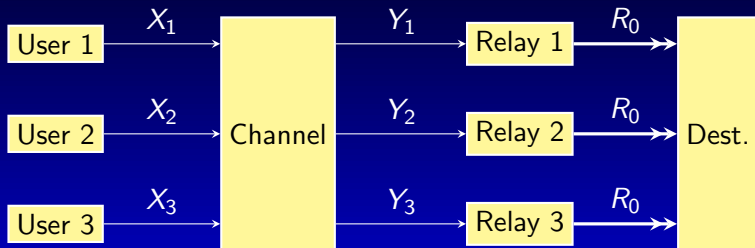
Asymmetric Powers: A Summary

The achievable rate region (R_1, R_2) is the intersection of the previous two regions:

$$R_1 \leq \min \left\{ \frac{1}{2} \log_2 \left(\frac{P_1}{P_1 + P_2} + \frac{P_1}{N} \right), \frac{1}{2} \log_2 \left(1 + \frac{P_{BC}}{N} \right) \right\}$$
$$R_2 \leq \min \left\{ \frac{1}{2} \log_2 \left(\frac{P_2}{P_1 + P_2} + \frac{P_2}{N} \right), \frac{1}{2} \log_2 \left(1 + \frac{P_{BC}}{N} \right) \right\}$$

The above region turns out to be within half a bit of the cut-set bound. See [Nam–Chung–Lee, *IT* 2010].

Compute-and-Forward



$$Y_k = \sum_{\ell=1}^L h_{k\ell} X_{\ell} + Z_k$$

Assume symmetric power constraint, due to $h_{k\ell}$.

Previously, the relay is interested in the sum of the transmitted codewords. Here, we expand the class of functions to include *integer linear combinations* of codewords.

Encoding

For each transmitter ℓ

$$\mathbf{x}_\ell = [\boldsymbol{\lambda}_\ell + \mathbf{u}_\ell] \bmod \Lambda'$$

Relay Decoding

$$\hat{\mathbf{t}}_k = \mathcal{Q}_{\Lambda}^{\text{NN}} \left(\alpha_k \mathbf{y}_k - \sum_{\ell=1}^L a_{k\ell} \mathbf{u}_{\ell} \right) \bmod \Lambda'$$

Error Probability

Let $\boldsymbol{\lambda}'_l = \mathcal{Q}_{\Lambda'}^{\text{NN}}(\boldsymbol{\lambda}_l + \mathbf{u}_l)$ for $l = 1, \dots, L$. Then,

$$\begin{aligned} & \alpha_k \mathbf{y}_k - \sum_{\ell} a_{k\ell} \mathbf{u}_{\ell} \\ &= \alpha_k \left(\sum_{\ell} h_{k\ell} \mathbf{x}_{\ell} + \mathbf{z} \right) - \sum_{\ell} a_{k\ell} \mathbf{u}_{\ell} \\ &= \alpha_k \left(\sum_{\ell} h_{k\ell} \underbrace{(\boldsymbol{\lambda}_{\ell} + \mathbf{u}_{\ell} - \boldsymbol{\lambda}'_{\ell})}_{\mathbf{x}_{\ell}} + \mathbf{z} \right) - \sum_{\ell} a_{k\ell} \mathbf{u}_{\ell} \\ &= \sum_{\ell} a_{k\ell} \boldsymbol{\lambda}_{\ell} + \underbrace{\sum_{\ell} (\alpha_k h_{k\ell} - a_{k\ell}) (\boldsymbol{\lambda}_{\ell} + \mathbf{u}_{\ell} - \boldsymbol{\lambda}'_{\ell})}_{\mathbf{n}_{\alpha_k}} + \alpha_k \mathbf{z} - \sum_{\ell} a_{k\ell} \boldsymbol{\lambda}'_{\ell} \end{aligned}$$

Hence, $\hat{\mathbf{t}}_k = \mathbf{t}_k \triangleq [\sum_{\ell} a_{k\ell} \boldsymbol{\lambda}_{\ell}] \bmod \Lambda'$ if and only if $\mathcal{Q}_{\Lambda'}^{\text{NN}}(\mathbf{n}_{\alpha_k}) \in \Lambda'$.
Therefore, $P_e(\mathbf{t}_k) \leq \Pr[\mathbf{n}_{\alpha_k} \in \mathcal{V}(\Lambda)]$.

Achievable Rate

Recall that $\mathbf{n}_{\alpha_k} = \sum_{\ell} (\alpha_k h_{k\ell} - a_{k\ell}) \mathbf{x}_{\ell} + \alpha_k \mathbf{z}$ with

$$\begin{aligned}\sigma^2(\mathbf{n}_{\alpha_k}) &= \sum_{\ell} (\alpha_k h_{k\ell} - a_{k\ell})^2 \sigma^2(\mathbf{x}_{\ell}) + \alpha_k^2 \sigma^2(\mathbf{z}) \\ &= \sum_{\ell} (\alpha_k h_{k\ell} - a_{k\ell})^2 P + \alpha_k^2 N\end{aligned}$$

The optimal $\alpha_k^* = \frac{P \mathbf{a}_k \mathbf{h}_k^T}{P \|\mathbf{h}_k\|^2 + N}$, where $\mathbf{a}_k = (a_{k1}, \dots, a_{kL})$ and $\mathbf{h}_k = (h_{k1}, \dots, h_{kL})$, and

$$\sigma^2(\mathbf{n}_{\alpha_k^*}) = P \|\mathbf{a}_k\|^2 - \frac{P^2 (\mathbf{a}_k \mathbf{h}_k^T)^2}{P \|\mathbf{h}_k\|^2 + N}.$$

Hence, $\mathbf{t}_k \triangleq [\sum_{\ell} a_{k\ell} \boldsymbol{\lambda}_{\ell}] \bmod \Lambda'$ can be decoded reliably if

$$R \leq \frac{1}{2} \log_2 \left(\frac{P}{\sigma^2(\mathbf{n}_{\alpha_k^*})} \right)$$

Decoding at the Destination

Each relay k sends the label of \mathbf{t}_k to the destination.

The destination solves a system of linear equations of labels \rightarrow

network coding

Decoding at the Destination (Cont'd)

The integer coefficients a_{kl} should be chosen by the relays such that $\mathbf{A} = \{a_{kl}\}$ is full rank over \mathbb{F}_p .

The overall achievable rate

$$R \leq \min \left\{ \frac{1}{2} \log_2 \left(\frac{P}{\sigma^2(\mathbf{n}_{\alpha_1^*})} \right), \dots, \frac{1}{2} \log_2 \left(\frac{P}{\sigma^2(\mathbf{n}_{\alpha_L^*})} \right), R_0 \right\}$$

Finding the Best Integer Coefficients

Problem formulation:

$$\begin{aligned} & \text{maximize} && R \\ & \text{subject to} && \forall k : R \leq \frac{1}{2} \log_2 \left(\frac{P}{\sigma^2(\mathbf{n}_{\alpha_k^*})} \right) \\ & && R \leq R_0 \\ & && \mathbf{A} = \{a_{k\ell}\} \text{ is full rank over } \mathbb{F}_p \end{aligned}$$

A greedy solution: each relay k minimizes $\sigma^2(\mathbf{n}_{\alpha_k^*})$ subject to $\mathbf{a}_k \neq \mathbf{0}$

Finding the Best Integer Coefficients (Cont'd)

Note that

$$\begin{aligned}\sigma^2(\mathbf{n}_{\alpha_k^*}) &= P\|\mathbf{a}_k\|^2 - \frac{P^2(\mathbf{a}_k\mathbf{h}_k^T)^2}{P\|\mathbf{h}_k\|^2 + N} \\ &= \mathbf{a}_k \left(\underbrace{P\mathbf{I}_L - \frac{P^2}{P\|\mathbf{h}_k\|^2 + N}\mathbf{h}_k^T\mathbf{h}_k}_{\mathbf{M}_k} \right) \mathbf{a}_k^T.\end{aligned}$$

Since \mathbf{M}_k is Hermitian and positive definite, it has a unique *Cholesky decomposition* $\mathbf{M}_k = \mathbf{L}_k\mathbf{L}_k^T$. Hence,

$$\sigma^2(\mathbf{n}_{\alpha_k^*}) = \mathbf{a}_k\mathbf{M}_k\mathbf{a}_k^T = \mathbf{a}_k\mathbf{L}_k\mathbf{L}_k^T\mathbf{a}_k^T = \|\mathbf{a}_k\mathbf{L}_k\|^2.$$

So, minimize $\|\mathbf{a}_k\mathbf{L}_k\|$ subject to $\mathbf{a}_k \neq \mathbf{0} \Rightarrow$ shortest vector problem

Compute-and-Forward: A Summary

Achievable rate:

$$R \leq \min_{\mathbf{A}} \left\{ \frac{1}{2} \log_2 \left(\frac{P}{\sigma^2(\mathbf{n}_{\alpha_1^*})} \right), \dots, \frac{1}{2} \log_2 \left(\frac{P}{\sigma^2(\mathbf{n}_{\alpha_L^*})} \right), R_0 \right\},$$

where \mathbf{A} is full rank.

A greedy solution: relay k minimize $\|\mathbf{a}_k \mathbf{L}_k\|$ subject to $\mathbf{a}_k \neq \mathbf{0}$.

Successive Compute-and-Forward

Consider the case of two transmitters and two relays.

Relay k recovers $a_{k1}\lambda_1 + a_{k2}\lambda_2 \pmod{\Lambda'}$ as described before.

However, the matrix

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \text{ is singular.}$$

So, some relay should compute *another* integer linear combination.

A similar analysis, using the same by-now familiar tools, ensues!