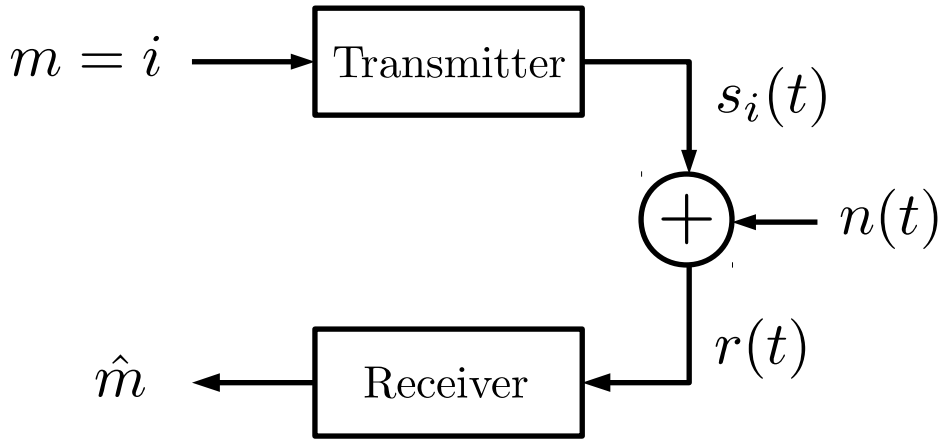
Lattices and Lattice Codes

Trivandrum School on Communication, Coding & Networking

January 27–30, 2017

Lakshmi Prasad Natarajan
Dept. of Electrical Engineering
Indian Institute of Technology Hyderabad
lakshminatarajan@iith.ac.in

Recall – Communications I & II

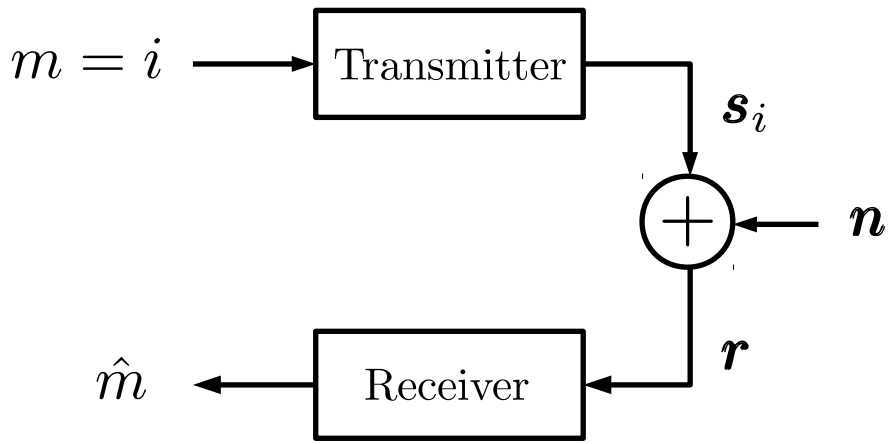


Time duration T

Bandwidth W
(approx. band-limited)

$$R = \frac{\log_2 M}{N}$$

Signal Space Analysis



Dimension N

If $\{\phi_n(t)\}$ chosen
carefully $N \approx 2TW$

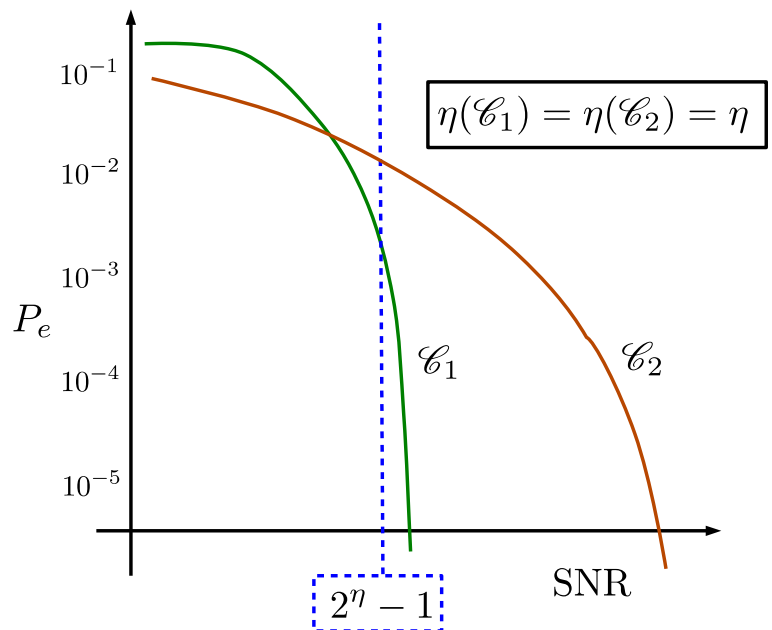
$$\eta = \frac{2\log_2 M}{N}$$

Capacity - Fundamental limit for Digital Communications

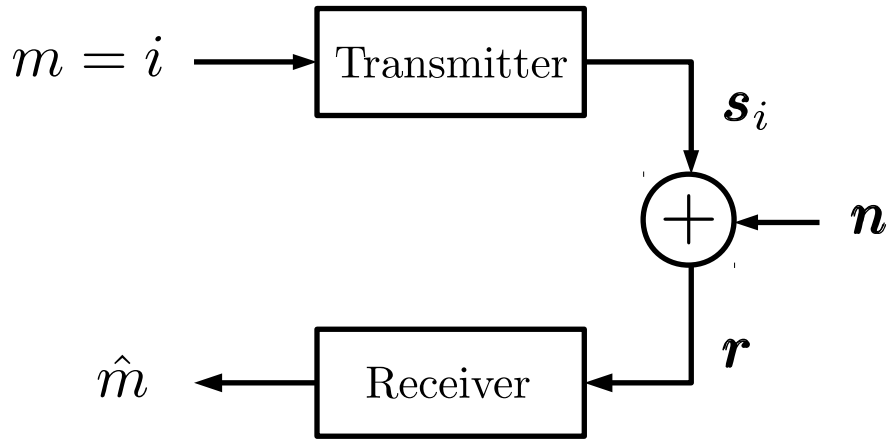
$C(\mathrm{SNR}) = \log_2(1 + \mathrm{SNR})$:
Max. spectral efficiency at a given SNR for reliable communication.

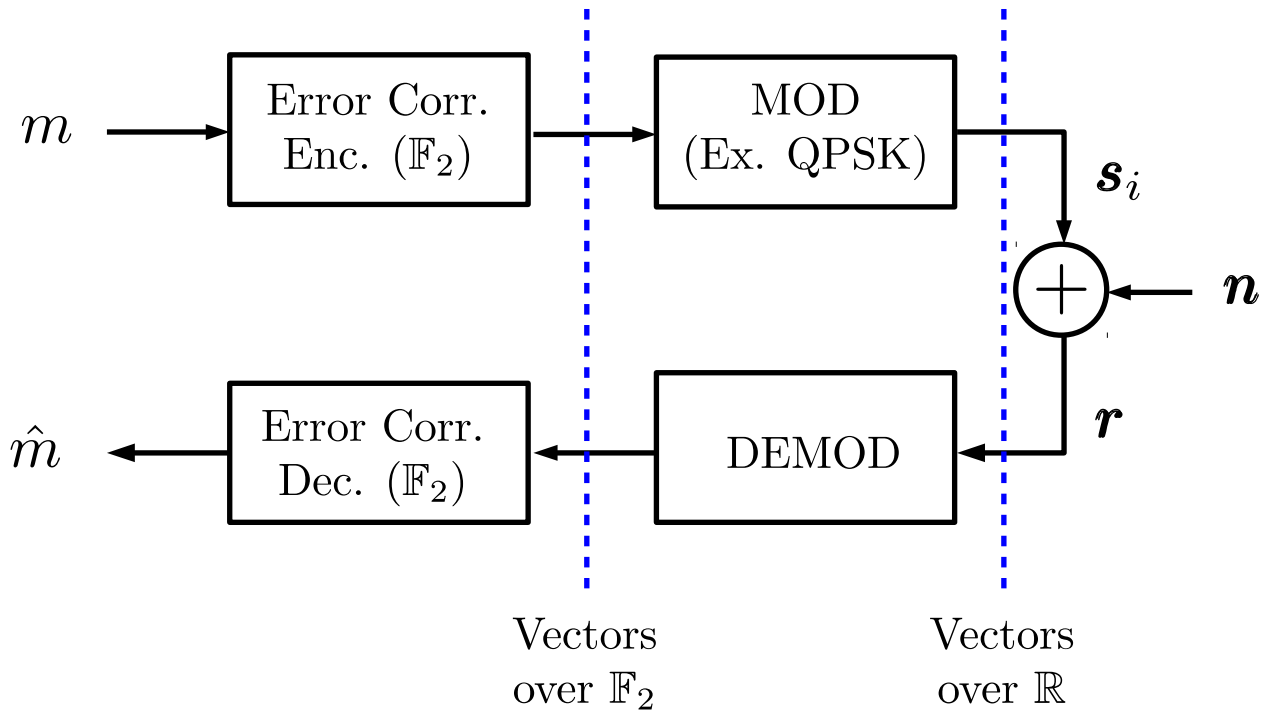
$\mathrm{SNR}^*(\eta) = 2^\eta - 1$:
Min. SNR required for a given η for reliable communication.

A code $\mathscr{C}$ with spectral efficiency η is 'good' if it has negligible P_e for $\mathrm{SNR} > 2^\eta - 1$.



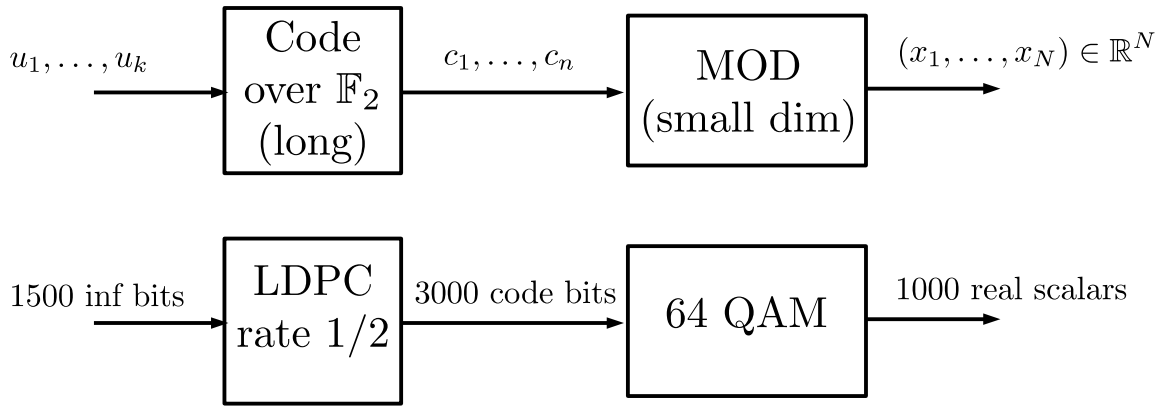
Dr. Lalitha Vadlamani's talk: Coding Theory I & II





How to Design Good Communication Schemes?

1. Combining Long Binary Codes with 'Small' Modulation Schemes

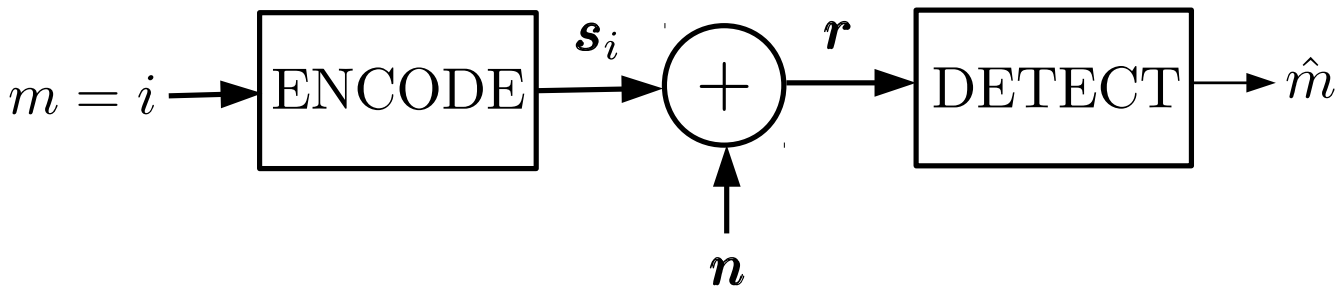


Code of size $M = 2^{1500}$ in $N = 1000$ dimensions

Examples: Bit-interleaved Coded Modulation, Multilevel Codes

2. Directly map messages to points in high-dimensional space $\mathbb{R}^N$
   Examples: Lattice codes, Group codes

This talk: Directly map messages to vectors



- Code (over $\mathbb{R}$) $\mathscr{C} = \{\boldsymbol{s}_1, \ldots, \boldsymbol{s}_M\} \subset \mathbb{R}^N$
- Power $P = \dfrac{1}{N} \cdot \dfrac{\|\boldsymbol{s}_1\|^2 + \cdots + \|\boldsymbol{s}_M\|^2}{M}$
- Noise variance $\sigma^2 = \dfrac{N_o}{2}$ (per dimension)
- Signal to noise ratio $\mathrm{SNR} = \dfrac{P}{\sigma^2} = \dfrac{2P}{N_o}$
- Spectral Efficiency $\eta = \dfrac{2\log_2 M}{N}$ bits/s/Hz (assuming $N = 2TW$)
- Probability of Error $P_e = P(\hat{m} \neq m)$

References

- F. Oggier and E. Viterbo, *Algebraic Number Theory and Code Design for Rayleigh Fading Channels.* Foundations and Trends in Communications and Information Theory, vol. 01, no. 03, 2004.
  - Section 3 of this reference is a primer on lattices.
- J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups.* New York, NY, USA: Springer-Verlag, 1999.
- R. Zamir, *Lattice Coding for Signals and Networks.* Cambridge, UK: Cambridge University Press, 2014.
- G. D. Forney, "Multidimensional constellations. II. Voronoi constellations," *IEEE Journal on Selected Areas in Communications*, vol. 7, no. 6, pp. 941–958, Aug 1989.
- H. A. Loeliger, "Averaging bounds for lattices and linear codes," *IEEE Transactions on Information Theory*, vol. 43, no. 6, pp. 1767-1773, Nov 1997.
- M. P. Wilson, K. Narayanan, H. D. Pfister and A. Sprintson, "Joint Physical Layer Coding and Network Coding for Bidirectional Relaying," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5641-5654, Nov. 2010.

1. Lattices
2. Sphere Packing Problem and Coding for Gaussian Channel
3. Construction A: From Error Correcting Codes to Lattices
4. Nested Lattice Codes/Voronoi Constellations

Lattices

Say $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_m \in \mathbb{R}^N$ are linearly independent column vectors, $m \leq N$.

Definition

The lattice Λ generated by $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_m$ is the set of all integer linear combinations of $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_m$

$$\Lambda = \{z_1\boldsymbol{g}_1 + \cdots + z_m\boldsymbol{g}_m \mid z_i \in \mathbb{Z}\}$$

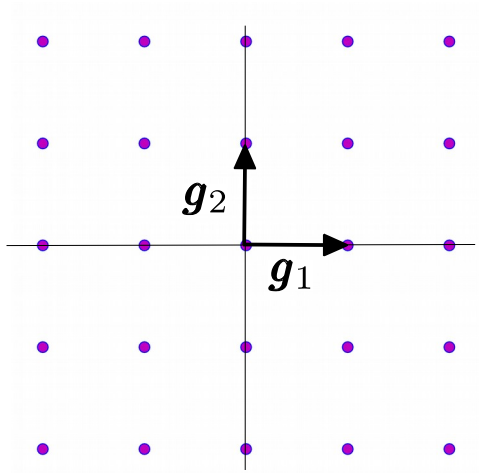
- We will consider only full-rank lattices $m = N$
- The matrix $\boldsymbol{G} = [\boldsymbol{g}_1 \ \boldsymbol{g}_2 \ \cdots \ \boldsymbol{g}_N]$ is a generator matrix for Λ

$$\Lambda = \{\boldsymbol{G}\boldsymbol{z} \mid \boldsymbol{z} \in \mathbb{Z}^N\}$$

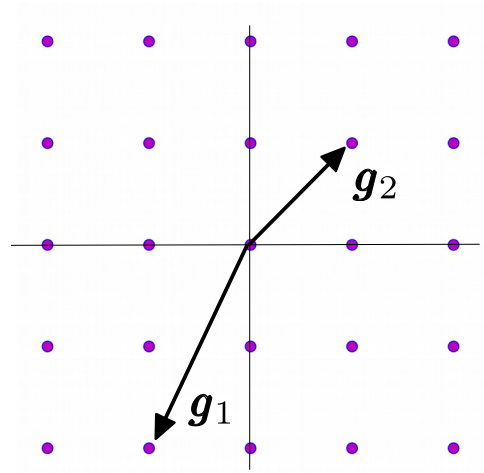
  $\boldsymbol{G} \in \mathbb{R}^{N \times N}$ is square, $\mathrm{rank}(\boldsymbol{G}) = N$, i.e., $\det(\boldsymbol{G}) \neq 0$.
- $\{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_N\}$ forms a basis for Λ.
- Generator matrix $\boldsymbol{G}$ of a lattice Λ is not unique.

Examples of lattices in two dimensions

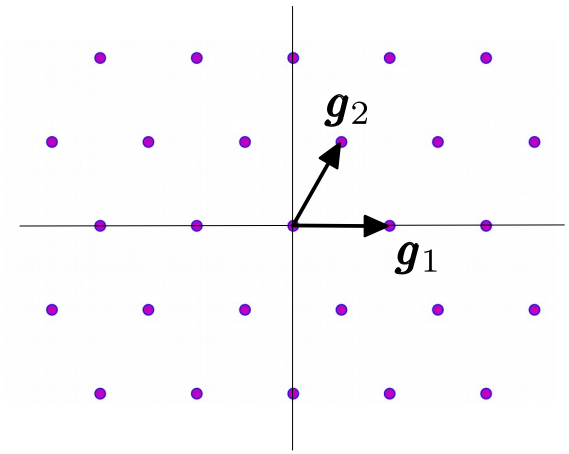
$$\mathbb{Z}^2 = \{(z_1, z_2) \mid z_1, z_2 \in \mathbb{Z}\}$$



$$G = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$



$$G = \begin{bmatrix} -1 & 1 \\ -2 & 1 \end{bmatrix}$$



Hexagonal lattice A_2

$$G = \begin{bmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{bmatrix}$$

"A Lattice of Flowers"
Trivandrum Flower Show, Kanakakunnu Palace Grounds
28 Jan 2017

Algebraic Properties of Lattices

Let $\Lambda \subset \mathbb{R}^N$ be any N-dimensional lattice.

- The all-zero vector $\mathbf{0}$ is a lattice point

$$\mathbf{0} = 0\,\boldsymbol{g}_1 + \cdots + 0\,\boldsymbol{g}_N \in \Lambda$$

- Additive inverse of any lattice point is a lattice point

$$\boldsymbol{\lambda} = z_1\boldsymbol{g}_1 + \cdots + z_N\boldsymbol{g}_N \in \Lambda \quad \Rightarrow \quad -\boldsymbol{\lambda} = -z_1\boldsymbol{g}_1 - \cdots - z_N\boldsymbol{g}_N \in \Lambda$$

- Sum of any two lattice points is also a lattice point

$$\boldsymbol{\lambda}_z = z_1\boldsymbol{g}_1 + \cdots + z_N\boldsymbol{g}_N \quad \text{and} \quad \boldsymbol{\lambda}_u = u_1\boldsymbol{g}_1 + \cdots + u_N\boldsymbol{g}_N$$
$$\boldsymbol{\lambda}_z + \boldsymbol{\lambda}_u = (z_1 + u_1)\boldsymbol{g}_1 + \cdots + (z_N + u_N)\boldsymbol{g}_N \in \Lambda$$

- If $a \in \mathbb{Z}$ and $\boldsymbol{\lambda} \in \Lambda$ then $a\boldsymbol{\lambda} \in \Lambda$.

Properties similar to vector space, but $\mathbb{Z}$ is NOT a field!!

Every lattice Λ is a module over $\mathbb{Z}$

Minimum Distance of a Lattice

Minimum Distance $d_{\min}(\Lambda)$

Smallest distance between any two lattice points

$$d_{\min} = \min_{\boldsymbol{\lambda}_1 \neq \boldsymbol{\lambda}_2} \|\boldsymbol{\lambda}_1 - \boldsymbol{\lambda}_2\|$$

Note that $\boldsymbol{\lambda}_1 - \boldsymbol{\lambda}_2 \in \Lambda$ and $\boldsymbol{\lambda}_1 - \boldsymbol{\lambda}_2 \neq 0$. Hence,

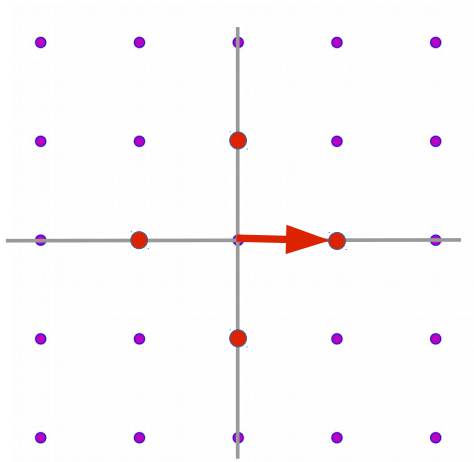
$$d_{\min} = \min_{\boldsymbol{\lambda} \neq 0} \|\boldsymbol{\lambda}\| = \text{ min norm of non-zero lattice points}$$

Note

Λ is invariant to translation by any lattice vector $\boldsymbol{\lambda} \in \Lambda$, $\Lambda = \boldsymbol{\lambda} + \Lambda$

- The distance of any nearest neighbor for any lattice point is $d_{\min}$

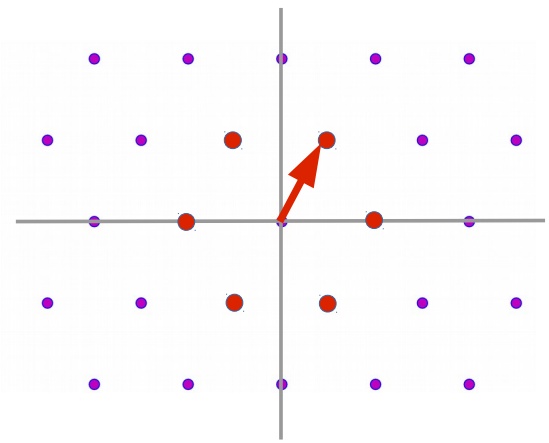
Examples in two dimensions



$$\mathbb{Z}^2 = \{(z_1, z_2) \mid z_1, z_2 \in \mathbb{Z}\}$$

$$\boldsymbol{G} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$d_{\min} = 1$$

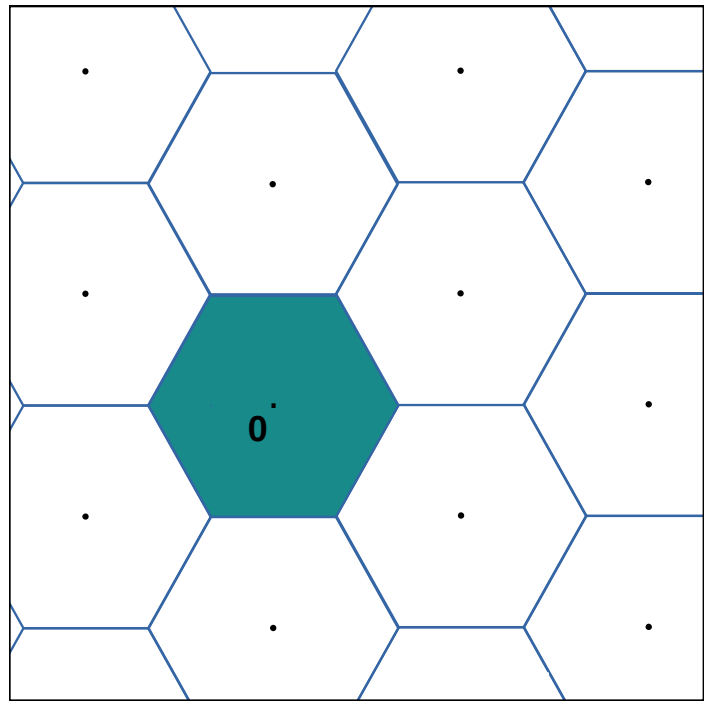


Hexagonal lattice A_2

$$\boldsymbol{G} = \begin{bmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{bmatrix}$$

$$d_{\min} = 1$$

Voronoi Region $\mathcal{V}(\Lambda)$



- Closest vector lattice quantizer
  $Q_\Lambda(\boldsymbol{x}) = \boldsymbol{\lambda}$ if $\boldsymbol{\lambda}$ is the nearest lattice point to $\boldsymbol{x} \in \mathbb{R}^N$
- Fundamental Voronoi region
  $\mathcal{V} = Q_\Lambda^{-1}(\mathbf{0})$ set of all points closer to $\mathbf{0}$ than any other lattice point
- $\boldsymbol{\lambda} + \mathcal{V} = Q_\Lambda^{-1}(\boldsymbol{\lambda})$ all points mapped to $\boldsymbol{\lambda}$ by Q_Λ
- Translates $\{\boldsymbol{\lambda} + \mathcal{V}\}$ of $\mathcal{V}$ are non-intersecting and cover $\mathbb{R}^N$

Volume and Hermite Parameter

Volume of the lattice $V(\Lambda)$

$V(\Lambda) = \mathrm{volume}\big(\mathcal{V}(\Lambda)\big)$ is the volume of the Voronoi region

- If $\boldsymbol{G}$ is a generator matrix, then $V(\Lambda) = |\det(\boldsymbol{G})|$
- This is a lattice invariant, does not depend on the choice of $\boldsymbol{G}$

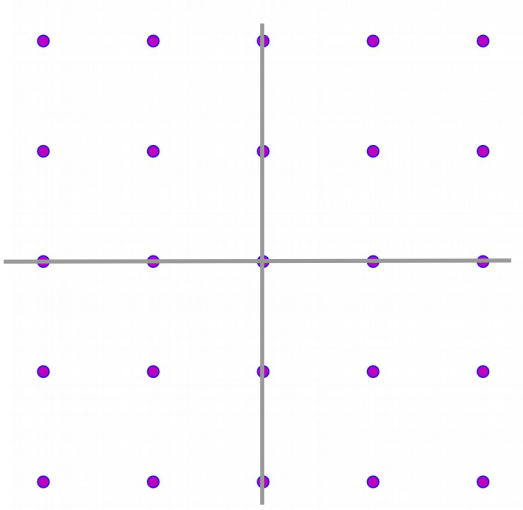
How to measure the density of lattice points

- Number of lattice points per unit volume in $\mathbb{R}^N = 1/V(\Lambda)$
- By simply scaling $\Lambda \to a\Lambda$, we can trivially modify the number of lattice points per unit volume
- We need a measure that is invariant to scaling.

Hermite Parameter $\gamma(\Lambda)$

$$\gamma(\Lambda) = \frac{d^2_{\min}(\Lambda)}{V(\Lambda)^{2/N}}$$

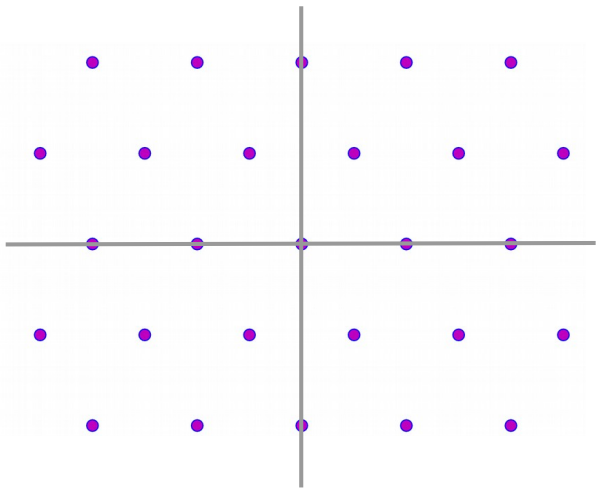
- $\gamma(\Lambda)^{N/2} =$ density when the lattice scaled to unit min distance.
- $\gamma(\Lambda) =$ squared min dist when the lattice is scaled to unit volume.



$$\mathbb{Z}^2 = \{(z_1, z_2) \mid z_1, z_2 \in \mathbb{Z}\}$$

$$\boldsymbol{G} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad d_{\min} = 1, V = 1$$

$$\gamma = 1$$



Hexagonal lattice A_2

$$\boldsymbol{G} = \begin{bmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{bmatrix} \quad d_{\min} = 1, V = \frac{\sqrt{3}}{2}$$

$$\gamma = \frac{2}{\sqrt{3}} \approx 1.15$$

1. Lattices
2. Sphere Packing Problem and Coding for Gaussian Channel
3. Construction A: From Error Correcting Codes to Lattices
4. Nested Lattice Codes/Voronoi Constellations

The Sphere Packing Problem

A sphere packing is an arrangement of infinitely-many non-overlapping identical spheres in the Euclidean space.

- A lattice can be used to pack spheres: place a sphere centered at each lattice point
- Spheres must be non-overlapping: largest spheres that can be packed using Λ have radius

$$r_{\text{pack}} = \frac{d_{\min}}{2}$$

This is called the packing radius of Λ

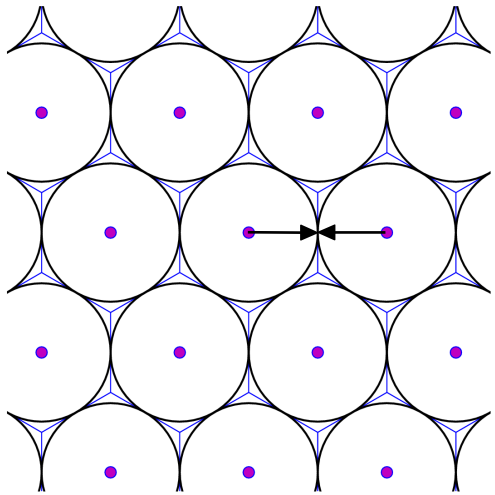
Sphere packing problem

What is the maximum density (number of spheres per unit volume) with which spheres can be packed in $\mathbb{R}^N$?

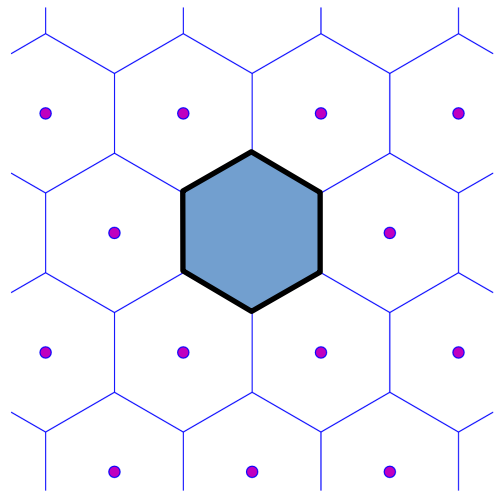
Sphere Packing and Hermite Parameter

Packing radius

$r_{\text{pack}}(\Lambda)$



$\text{Vol}(\Lambda)$



Center Density $\delta(\Lambda) = \dfrac{r_{\text{pack}}^N(\Lambda)}{V(\Lambda)}$

density of spheres when the lattice is scaled to unit packing radius

Using $d_{\min} = 2r_{\text{pack}}$, we obtain $\delta(\Lambda) = \left(\dfrac{\gamma(\Lambda)}{4}\right)^{N/2}$

Best Lattice Sphere Packings

Let γ_N = largest Hermite parameter among all lattices in $\mathbb{R}^N$

Theorem

For all sufficiently large N, we have $\dfrac{N}{2\pi e} \lesssim \gamma_N \lesssim \dfrac{1.744\,N}{2\pi e}$

- Bounds on packing efficiency increase with the dimension N.

Best Lattice Packings for $N \leq 8$

N	1	2	3	4	5	6	7	8
Λ	$\mathbb{Z}$	A_2	D_3	D_4	D_5	E_6	E_7	E_8
γ_N	1	1.15	1.26	1.41	1.52	1.67	1.81	2
κ	2	6	12	24	40	72	126	240

From Lattices to Codes

- A code $\mathscr{C} = \{\boldsymbol{s}_1, \ldots, \boldsymbol{s}_M\}$ for the (vector) Gaussian channel is a finite set of points in $\mathbb{R}^N$.
- Replace the average power constraint with the more stringent 'per-codeword' power constraint:

$$\frac{\|\boldsymbol{s}_i\|^2}{N} \leq P \Rightarrow \|\boldsymbol{s}_i\| \leq \sqrt{NP}$$

- Let $\mathcal{B}$ be the N-dimensional ball of radius $\sqrt{NP}$ centered at $\mathbf{0}$

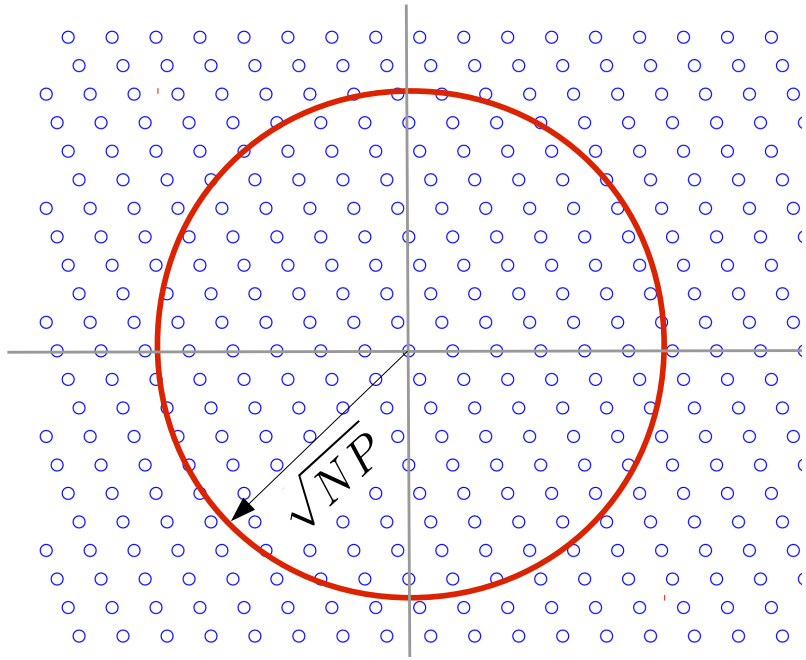
$$\boldsymbol{s}_i \in \mathcal{B} \text{ for } i = 1, \ldots, M$$

Spherically-shaped lattice codes

We can carve an N-dimensional code $\mathscr{C}$ from a lattice Λ by setting

$$\mathscr{C} = \Lambda \cap \mathcal{B}$$

Spherically-Shaped Lattice Codes



Say, we desire to construct a code for given N, P & spectral efficiency η

$$M = |\mathscr{C}| \approx \frac{\mathrm{Vol}(\mathcal{B})}{V(\Lambda)} \quad \Rightarrow \quad V(\Lambda) \approx \mathrm{Vol}(\mathcal{B})\, 2^{-N\eta/2}$$

$$\text{Then } d^2_{\min} = \gamma(\Lambda) \cdot V(\Lambda)^{2/N} \approx \gamma(\Lambda) \cdot \mathrm{Vol}(\mathcal{B})^{2/N}\, 2^{-\eta}$$

To construct a good code, we require Λ to have a large $\gamma(\Lambda)$.

1. Lattices
2. Sphere Packing Problem and Coding for Gaussian Channel
3. Construction A: From Error Correcting Codes to Lattices
4. Nested Lattice Codes/Voronoi Constellations

Prime Fields $\mathbb{F}_p$

Prime fields are finite fields whose cardinality is a prime number.
Let $p \geq 2$ be any prime integer.

Definition

The prime field of cardinality p is the set $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ where addition and multiplication are performed modulo p

- $a \oplus b = (a + b) \bmod p$, and
- $a \otimes b = (a \cdot b) \bmod p$.

- $\mathbb{F}_p$ satisfies all the axioms of a field: existence of additive & multiplicative identities and inverses, distributive law, etc.

Addition in $\mathbb{F}_3 = \{0, 1, 2\}$

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Multiplication in $\mathbb{F}_3 = \{0, 1, 2\}$

$\otimes$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Linear Codes over $\mathbb{F}_p$

Addition of vectors over $\mathbb{F}_p$:

$$\boldsymbol{a} \oplus \boldsymbol{b} = (a_1, \ldots, a_N) \oplus (b_1, \ldots, b_N) = (a_1 \oplus b_1, \ldots, a_N \oplus b_N)$$

Definition

A linear code $\mathcal{C}$ over $\mathbb{F}_p$ of length N is a subspace of $\mathbb{F}_p^N$.

- $|\mathcal{C}| = p^k$, where integer k is the dimension of the code.

Example

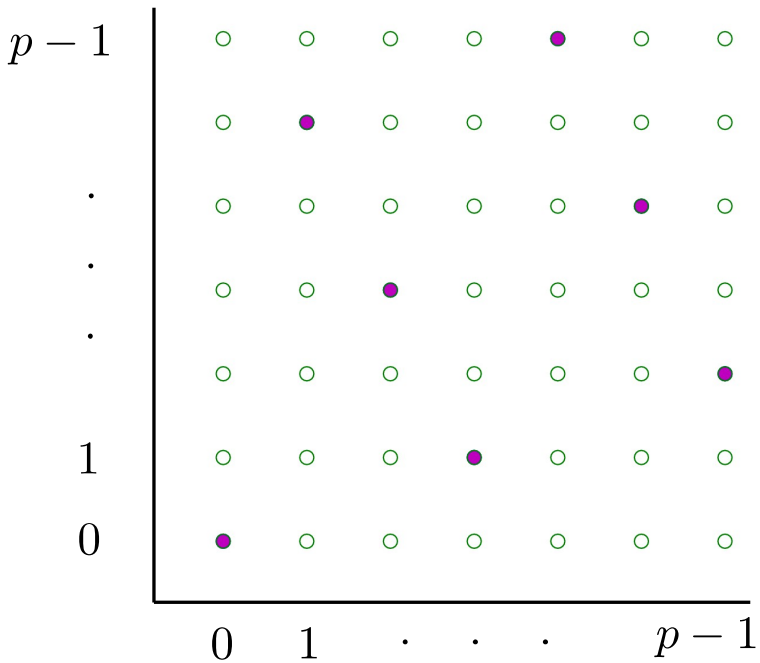
- $N = 5$, $p = 2$ and $\mathcal{C} = \{(0,0,0,0,0), (1,1,1,1,1)\}$.
  This is the repetition code of length 5 over $\mathbb{F}_2$.
- $N = 3$, $p = 3$ and $\mathcal{C} = \{(0,0,0),\ (1,1,1),\ (2,2,2)\}$.
  This is the repetition code of length 3 over $\mathbb{F}_3$.

Lattices from Codes

The linear code $\mathcal{C} \subset \mathbb{F}_p^n$ is closed under addition $\mod p$

$$\boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathcal{C} \Rightarrow (\boldsymbol{c}_1 + \boldsymbol{c}_2) \mod p \in \mathcal{C}$$

Example: $p = 7,\ N = 2$
$\mathcal{C} = \{(0,0), (3,1), (6,2), (2,3), (5,4), (1,5), (4,6)\}$

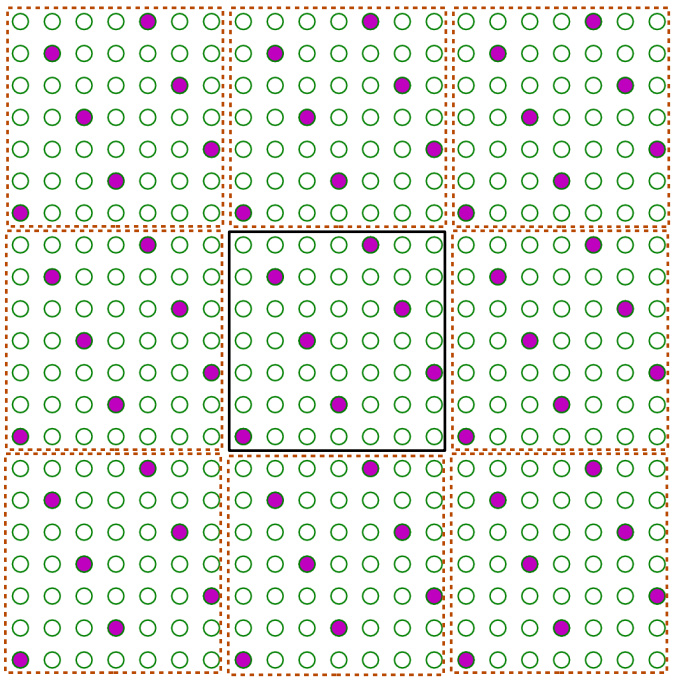


- Embed $\mathcal{C}$ into $\mathbb{R}^N$ using natural map

Create a lattice Λ by tiling copies of $\mathcal{C}$ in $\mathbb{R}^N$

Lattices from Codes: Construction A

$$\Lambda = \mathcal{C} + p\,\mathbb{Z}^N = \cup_{\boldsymbol{u}\in\mathbb{Z}^n}\,(\mathcal{C} + p\,\boldsymbol{u})$$



Example (continued)

$$\boldsymbol{G} = \begin{bmatrix} 3 & -1 \\ 1 & 2 \end{bmatrix}$$

$p = 2$: Using codes over $\mathbb{F}_2 = \{0, 1\}$, $\mathcal{C} \subset \mathbb{F}_2^N$

$p = 2$ and, say, $|\mathcal{C}| = 2^k$, $d_{\mathrm{H}} = \min$ Hamming distance

$$\mathrm{Vol}(\Lambda) = 2^{(N-k)} \text{ and } d_{\min}(\Lambda) = \min\{2, \sqrt{d_{\mathrm{H}}}\}$$

Examples of Construction A Lattices from Binary Codes

1. **The D_4 lattice**

   Let $\mathcal{C} = \{(0,0,0,0),(1,1,1,1)\}$ be repetition code of length $N = 4$. Dimension $k = 1$ and min Hamming distance $d_{\mathrm{H}} = 4$.

   $$V(\Lambda) = 8 \text{ and } d_{\min} = 2 \quad \Rightarrow \quad \gamma(\Lambda) = \sqrt{2}$$

   $$\boldsymbol{G} = \begin{bmatrix} 2 & 0 & 0 & 1 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

2. **The E_8 lattice**

   Use $\mathcal{C} = [N = 8, k = 4, d_{\mathrm{H}} = 4]$ extended Hamming code.

   $$V(\Lambda) = 16 \text{ and } d_{\min} = 2 \quad \Rightarrow \quad \gamma(\Lambda) = 2$$

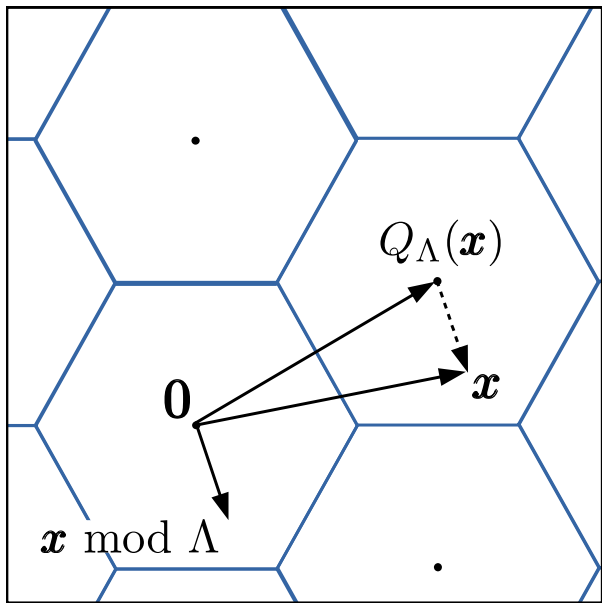
D_4 and E_8 are the densest lattices in their dimensions.

Theorem

For N large, there exists a Construction A lattice with $\gamma \gtrsim \dfrac{N}{2\pi e}$

1. Lattices
2. Sphere Packing Problem and Coding for Gaussian Channel
3. Construction A: From Error Correcting Codes to Lattices
4. Nested Lattice Codes/Voronoi Constellations

Modulo Lattice Operation



$$\boldsymbol{x} \bmod \Lambda = \boldsymbol{x} - Q_\Lambda(\boldsymbol{x})$$
$$\mathbb{R}^N \to \mathcal{V}(\Lambda)$$

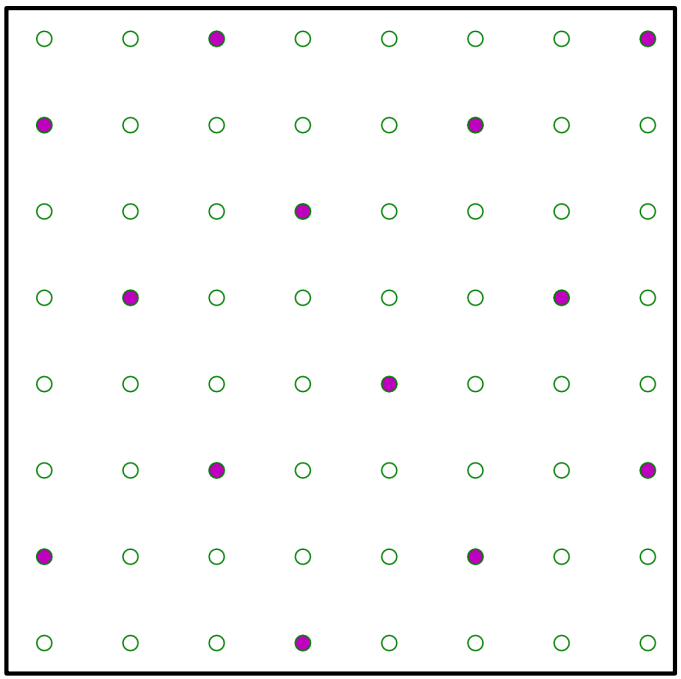
Modulo operation lends algebraic structure to the Voronoi region $\mathcal{V}_\Lambda$

$$\begin{aligned} \mathcal{V}(\Lambda) \times \mathcal{V}(\Lambda) \to \quad & \mathcal{V}(\Lambda) \\ (\boldsymbol{x}, \boldsymbol{y}) \quad \to & (\boldsymbol{x} + \boldsymbol{y}) \bmod \Lambda \end{aligned}$$

- The origin $\mathbf{0} \in \mathcal{V}(\Lambda)$, and for every $\boldsymbol{x} \in \mathcal{V}$, there exists a unique $\boldsymbol{y} = -\boldsymbol{x} \bmod \mathcal{V}$ such that $(\boldsymbol{x} + \boldsymbol{y}) \bmod \Lambda = \mathbf{0}$
- $\mathcal{V}(\Lambda)$ is a group under addition modulo Λ.

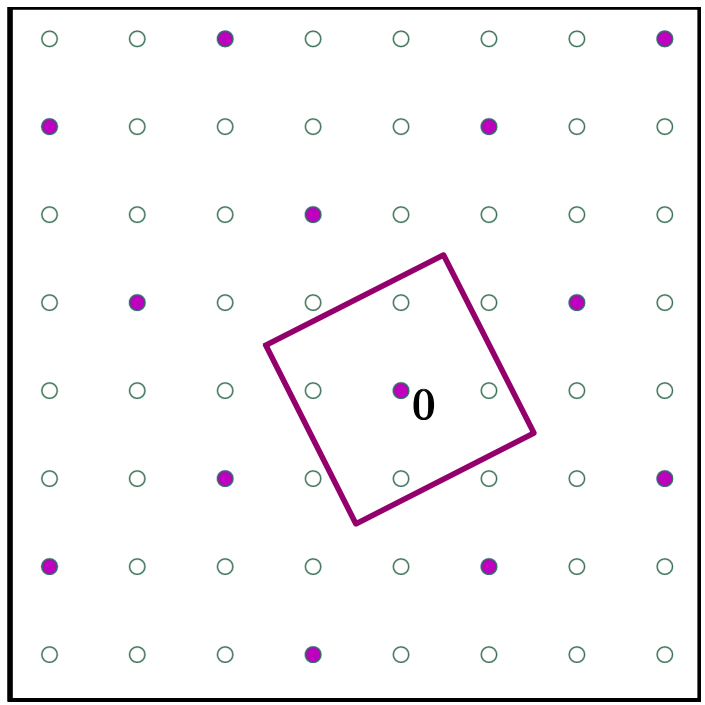
Nested Lattices and Lattice Codes/Voronoi Constellations

Nested Lattices



- $\Lambda_s \subset \Lambda$ are lattices
- Λ_s is a subgroup of Λ

Lattice Codes or Voronoi Constellations



- $\Lambda/\Lambda_s = \Lambda \cap \mathcal{V}_{\Lambda_s}$ is a group

  Addition: $\boldsymbol{x} \oplus \boldsymbol{y} = (\boldsymbol{x} + \boldsymbol{y}) \bmod \Lambda_s$

Lattice Codes

Lattice Code Λ/Λ_s

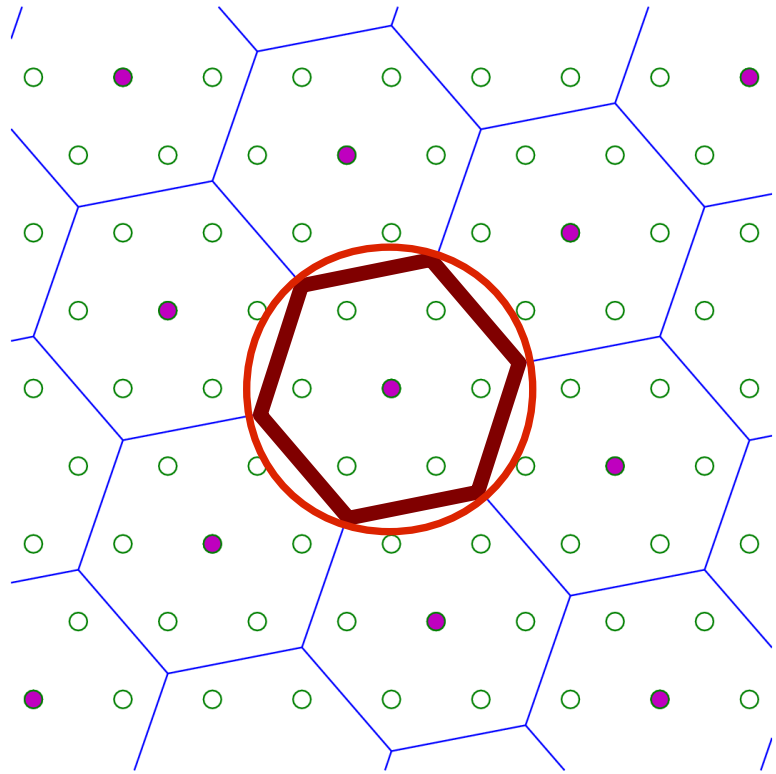
- Finite group under addition $\mathrm{mod}\ \Lambda_s$
- $|\Lambda/\Lambda_s| = V(\Lambda_s)/V(\Lambda)$
- $\eta = \frac{2}{N}\log_2 \frac{V(\Lambda_s)}{V(\Lambda)}$

Coding lattice (Fine lattice) Λ

- Provides noise resilience
- Want large $\mathrm{d}_{\min}(\Lambda)$ & small $V(\Lambda)$

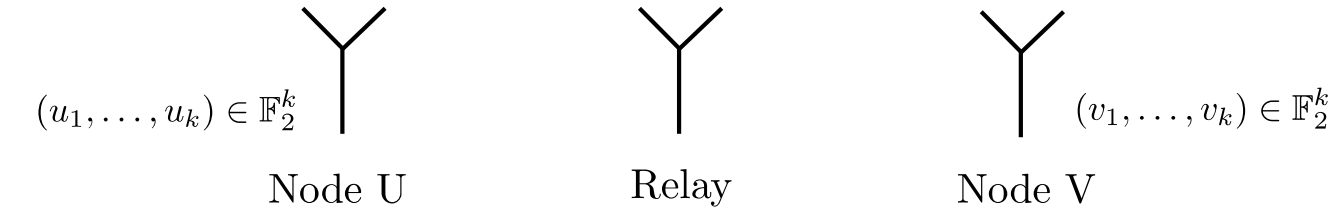
Shaping lattice (Coarse lattice) Λ_s

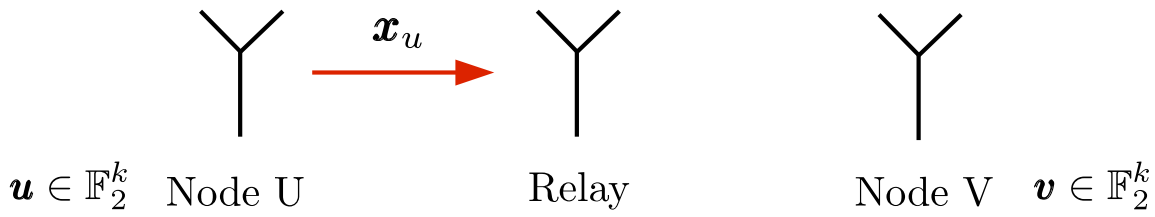
- Carves a finite code from Λ
- Determines transmit power
- Want small power & large $V(\Lambda_s)$

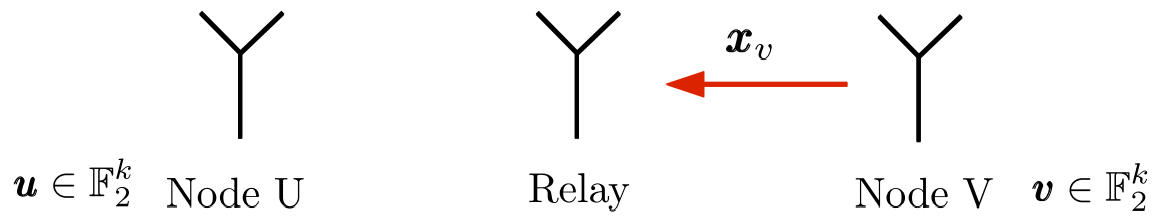


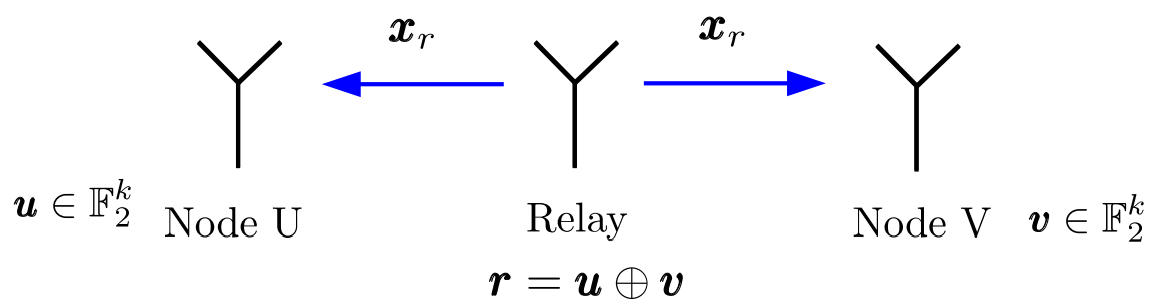
Lattice codes are good for many things: achieve capacity in Gaussian channel and dirty paper channel, Diversity-Multiplexing Trade-off in multiple-antenna channels, relay networks (compute & forward), wiretap channels, interference channels, quantization, cryptography, etc. etc. etc.

Example Application: Bidirectional Relay Channel



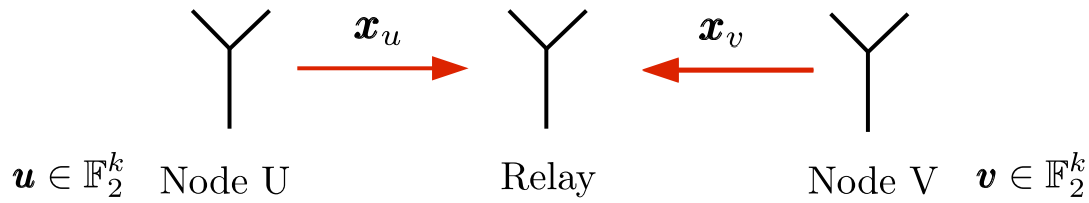






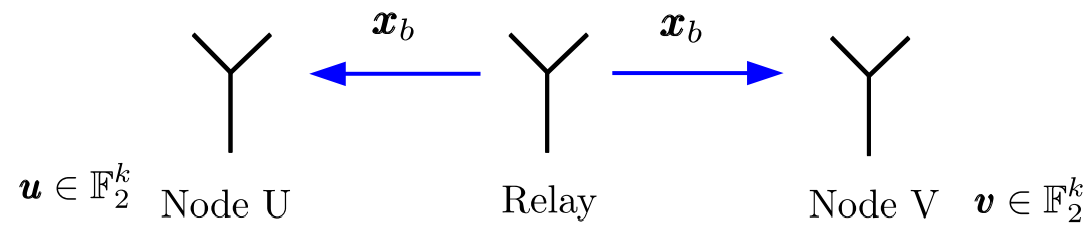
Joint PHY/Network-layer Lattice Coding Scheme

Use a lattice code $\mathscr{C} = \Lambda/\Lambda_s$ at all nodes



Relay decodes $x_u + x_v \in \Lambda$

Relay broadcasts $x_b = (x_u + x_v) \mod \Lambda_s$



Node U: $(x_b - x_u) \mod \Lambda_c = x_v$

Node V: $(x_b - x_v) \mod \Lambda_c = x_u$

Wilson, Narayanan, Pfister and Sprintson, *IEEE Trans. Inf. Theory*, Nov. 2010.

Conclusion

- Lattices have rich algebraic and geometric properties.
- They have strong connection to coding/modulation for Gaussian channel, and to error correcting codes over finite fields.
- Structured codes can be obtained using nested lattice pairs. This structure can be useful in communication engineering, for instance for exploiting interference in wireless channels.
- Lattices have several other applications: cryptography, information-theoretic security, codes for fading and multiple antenna channels, vector quantization etc.

Thank You!!