MONASH University

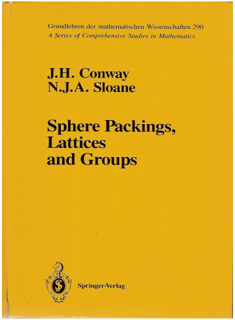
Lattice Index Coding

Part II - Mathematical Preliminaries

Emanuele Viterbo

European School of Information Theory
4 April 2016, Gothenburg

Based on..



IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 7, NO. 6, AUGUST 1989 941

Multidimensional Constellations—Part II: Voronoi Constellations

G. DAVID FORNEY, JR., FELLOW, IEEE

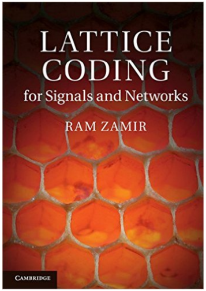
***Abstract*—Voronoi constellations, introduced in [1], are implementable *N* dimensional constellations based on partitions of *N* dimensional lattices that can achieve good shape gains and that are inherently suited for use with coded modulation. We give two methods for specifying Voronoi constellations based on arbitrary partitions Λ/Λ_s, one of which is conjectured to be optimum, and the other of which has desirable symmetries and naturally supports opportunistic secondary channels. When Λ and Λ_s are 2D-symmetric, the constituent 2D constellation is itself a Voronoi constellation; the shaping constellation expansion ratio and peak-to-average power ratio are determined in general and for various shaping lattices Λ_s. Methods for labeling Voronoi constellations are given; their complexity is dominated by that of "decoding" Λ_s. It is shown that coding and shaping are separable and dual. Bounds on the shape gain of Voronoi constellations are given that depend on the depth $\mu(\Lambda_s)$ and normalized informativity $\kappa(\Lambda_s)$ of the shaping lattice Λ_s. These bounds suggest the use of lattices Λ_s with depth 2 and normalized informativity less than 1. Examples are given that show that lattices of this type can achieve near-optimal shape gains with reduced constellation expansion and implementation complexity.**

I. Introduction

VORONOI constellations were introduced in [1] where they were called "Voronoi codes." Let Λ be an N dimensional lattice, and let Λ_s be an N dimensional subment of ℝ (Part I). The normalized second moment $G(\Lambda_s)$ is known for the Voronoi regions of a number of the most interesting lattices ([3], [4], [5], [6]). Table I gives the shape gains $\gamma_s(\Lambda_s) = 1/[12G(\Lambda_s)]$ for the Voronoi regions of some of these lattices, compared to the shape gain $\gamma_{\otimes}(N)$ (in dB) for an N sphere of the same dimension, and also to a bound $\gamma_{CS}(N)$ conjectured in [7].

We see that the shape gain for these lattices remains within about 0.1 dB of the N sphere limit for dimensions up to 24, i.e., for shape gains up to the order of 1.0 dB. Therefore, Voronoi constellations are potentially attractive, because they can achieve considerably better shape gains than are achieved by the generalized cross constellations of Part I, and in higher dimensions may possibly approach the ultimate limit on shape gain of $\pi e/6 = 1.423$ (1.53 dB).

Voronoi constellations also satisfy the fundamental requirement for use with a coset code based on a lattice partition Λ/Λ' [8], provided that Λ_s is a sublattice of Λ'. For then $\Lambda/\Lambda'/\Lambda_s$ is a lattice partition chain, and the $|\Lambda/\Lambda_s|$ cosets of Λ_s in any translate $\Lambda + \boldsymbol{a}$ of Λ partition into $|\Lambda/\Lambda'|$ subsets, each containing the $|\Lambda'/\Lambda_s|$ cosets



References

- J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups.* New York, NY, USA: Springer-Verlag, 1999.
- G. D. Forney, "Multidimensional constellations. II. Voronoi constellations," *IEEE Journal on Selected Areas in Communications*, vol. 7, no. 6, pp. 941–958, Aug 1989.
- R. Zamir, *Lattice Coding for Signals and Networks.* Cambridge, UK: Cambridge University Press, 2014.
- B. Nazer and M. Gastpar, "Compute-and-Forward: Harnessing Interference Through Structured Codes," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6463-6486, Oct. 2011.
- C. Feng, D. Silva and F. R. Kschischang, "An Algebraic Approach to Physical-Layer Network Coding," *IEEE Transactions on Information Theory*, vol. 59, no. 11, pp. 7576-7596, Nov. 2013.
- Y.-C. Huang and K. R. Narayanan, "Construction π_A and π_D Lattices: Construction, Goodness, and Decoding Algorithms," arXiv:1506.08269, Jun. 2015.

Abelian Groups

Definition

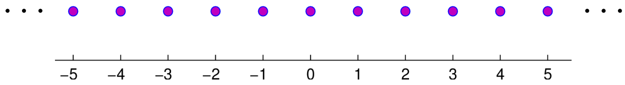
An Abelian group $\mathcal{G}$ is a set endowed with an 'addition' operation

$$(a, b) \to a + b$$

such that

1. $\mathcal{G}$ is *closed* under the addition operation
2. there exists an *identity element* $0 \in \mathcal{G}$: $a + 0 = a$ for all $a \in \mathcal{G}$
3. for every a, there is a $-a \in \mathcal{G}$ such that $a + (-a) = 0$
4. *Associative:* $a + (b + c) = (a + b) + c$ for all $a, b, c \in \mathcal{G}$
5. *Commutative:* $a + b = b + a$ for all $a, b \in \mathcal{G}$

Example The set of all integers $\mathcal{G} = \mathbb{Z}$, with usual definition of addition



Finite Abelian Groups

Example The finite binary group $\{0, 1\}$ with addition mod 2 (or XOR $\oplus$)

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

Example The finite ternary group $\{0, 1, 2\}$ with addition mod 3

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

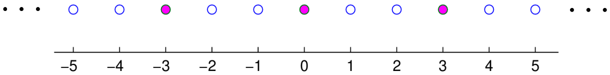
Subgroups of Abelian Groups

Definition

Let $(\mathcal{G}, +)$ be group. Then $\mathcal{H}$ is a subgroup of $\mathcal{G}$ if

1. $\mathcal{H} \subset \mathcal{G}$, and is non-empty
2. $(\mathcal{H}, +)$ is a group, i.e.,
   - $\mathcal{H}$ is closed under addition and negation.

Example Multiples of 3, i.e., $\mathcal{H} = 3\mathbb{Z}$ form a subgroup of $\mathcal{G} = \mathbb{Z}$



- For any integer M, $M\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

Cosets of a Subgroup in a Group

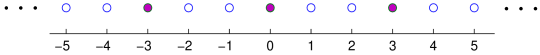
Definition

A coset is any set of the form $a + \mathcal{H} = \{a + h \,|\, h \in \mathcal{H}\}$, where $a \in \mathcal{G}$.

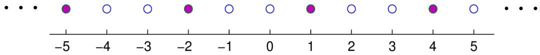
- Cosets are 'translates' of $\mathcal{H}$ in $\mathcal{G}$.
- **Notation**: $\mathcal{G}/\mathcal{H}$ = set of all cosets of $\mathcal{H}$ in $\mathcal{G}$.

Example $\mathcal{G}/\mathcal{H} = \mathbb{Z}/3\mathbb{Z} = \{0 + 3\mathbb{Z},\, 1 + 3\mathbb{Z},\, 2 + 3\mathbb{Z}\}$

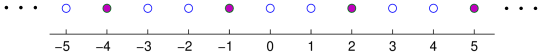
$$0 + 3\mathbb{Z} = 3 + 3\mathbb{Z} = \cdots$$



$$1 + 3\mathbb{Z} = 4 + 3\mathbb{Z} = \cdots$$



$$-1 + 3\mathbb{Z} = 2 + 3\mathbb{Z} = \cdots$$



Quotient Group

Definition

Quotient group is the group formed by the cosets $\mathcal{G}/\mathcal{H}$ under the rules

$$(a+\mathcal{H})+(b+\mathcal{H})=(a+b)+\mathcal{H}, \quad -(a+\mathcal{H})=(-a)+\mathcal{H}$$

Example

$$(1+3\mathbb{Z})+(1+3\mathbb{Z})=2+3\mathbb{Z}, \qquad -(1+3\mathbb{Z})=-1+3\mathbb{Z}=2+3\mathbb{Z}$$

Coset Leaders

- Coset leader: a representative element of a coset $(a+\mathcal{H})$.

Example

$$\begin{aligned}(0+3\mathbb{Z}) &\to \quad 0\\ (1+3\mathbb{Z}) &\to \quad 1\\ (2+3\mathbb{Z}) &\to \quad 2\end{aligned}$$

$$\Rightarrow \mathbb{Z}/3\mathbb{Z}=\{0,1,2\}$$

Addition in $\mathbb{Z}/3\mathbb{Z}$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

M-ary Pulse Amplitude Modulation

In general, for a fixed positive integer M,

- $\mathcal{G} = \mathbb{Z}$, subgroup $\mathcal{H} = M\mathbb{Z}$
- Quotient group $\mathcal{G}/\mathcal{H} = \mathbb{Z}/M\mathbb{Z} = \{0, 1, \ldots, M-1\} = M$-PAM

Addition and negation performed 'modulo M'

- $a \bmod M$ is the remainder when a is divided by M.
  - $14 \bmod 4 = 2$ since $14 = 3 \times 4 + 2$

- If $a, b \in \{0, 1, \ldots, M-1\} = \mathbb{Z}/M\mathbb{Z}$, then

Addition: $(a + b) \bmod M$

Negation: $(-a) \bmod M = M - a$

M-PAM has the additive structure of a group.
Are there multidimensional codes with group structure?

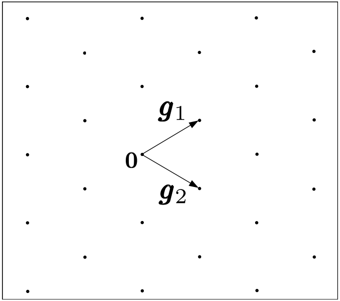
Lattices

- A Lattice is a discrete group of points in $\mathbb{R}^n$

$$\Lambda = \{\boldsymbol{G}\boldsymbol{u} \,|\, \boldsymbol{u} \in \mathbb{Z}^n\}$$

- $\boldsymbol{G} = [\boldsymbol{g}_1 \ \cdots \ \boldsymbol{g}_n]$ is an $n \times n$ full-rank matrix (in this tutorial).
- Lattice points are integer-linear combinations of *basis vectors*

$$\{u_1\boldsymbol{g}_1 + \cdots + u_n\boldsymbol{g}_n | u_1, \ldots, u_n \in \mathbb{Z}\}$$



- Λ is an abelian group under usual addition of vectors.

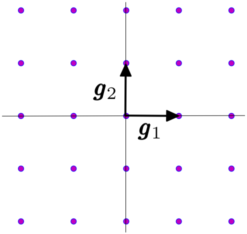
  - $d_{\min}(\Lambda)$ = min Euclidean distance between any two lattice points $= \min_{\boldsymbol{\lambda} \in \Lambda \setminus \{\mathbf{0}\}} \|\boldsymbol{\lambda}\|$

Lattices – Examples

$\mathbb{Z}^2$

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

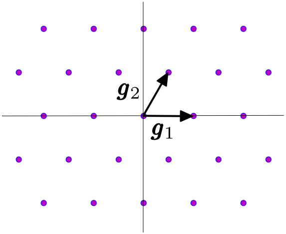
$$\mathrm{d}_{\min} = 1$$



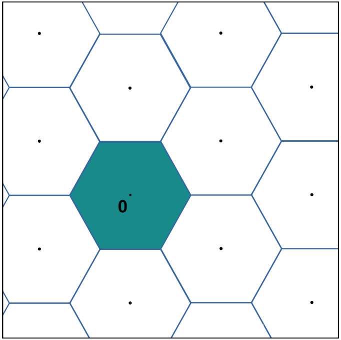
A_2

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

$$\mathrm{d}_{\min} = 1$$

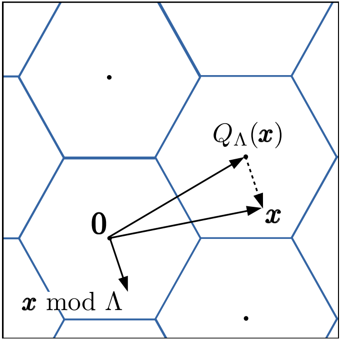


Voronoi Region



- Quantizer $Q_\Lambda : \mathbb{R}^n \to \Lambda$ gives the lattice point $Q_\Lambda(\boldsymbol{x})$ closest to $\boldsymbol{x}$
- The Voronoi region $\mathcal{V}_\Lambda = Q_\Lambda^{-1}(\mathbf{0})$
- $\mathrm{Vol}(\Lambda) \triangleq \mathrm{Vol}(\mathcal{V}_\Lambda) = |\det(\boldsymbol{G})|$
- Shifted Voronoi regions tile $\mathbb{R}^n$

Modulo Lattice Operation



$$\boldsymbol{x} \bmod \Lambda = \boldsymbol{x} - Q_\Lambda(\boldsymbol{x})$$

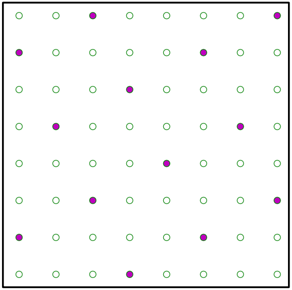
Modulo operation lends algebraic structure to the Voronoi region $\mathcal{V}_\Lambda$

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

Nested Lattices and Lattice Codes

<u>Nested Lattices</u>

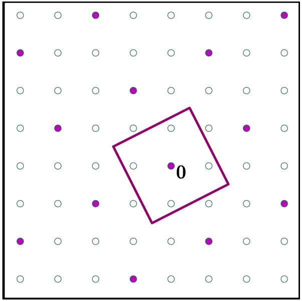
$\mathrm{Vol}(\Lambda)$



- $\Lambda_{\mathsf{s}} \subset \Lambda$ are lattices
- Λ_{s} is a subgroup of Λ
- $\Lambda/\Lambda_{\mathsf{s}}$ is a quotient group

<u>Lattice Codes</u>

$\mathrm{Vol}(\Lambda_{\mathsf{s}}) = 5\mathrm{Vol}(\Lambda)$



- Coset leaders are $\Lambda \cap \mathcal{V}_{\Lambda_{\mathsf{s}}}$
- $\Lambda/\Lambda_{\mathsf{s}} = \Lambda \cap \mathcal{V}_{\Lambda_{\mathsf{s}}}$ is a group

  Addition: $(\boldsymbol{x} + \boldsymbol{y}) \bmod \Lambda_{\mathsf{s}}$

Lattice Codes

Coding lattice (Fine lattice) Λ

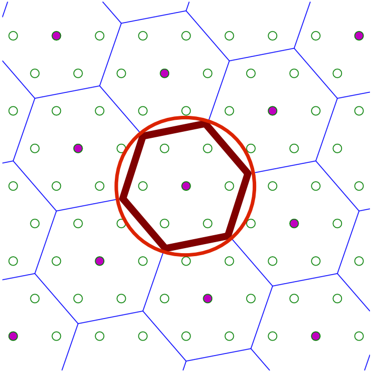
- Provides noise resilience
- Want large $\mathrm{d_{min}}(\Lambda)$ & small $\mathrm{Vol}(\Lambda)$

Shaping lattice (Coarse lattice) Λ_{s}

- Carves a finite code from Λ
- Constrains peak power
- Want small power & large $\mathrm{Vol}(\Lambda_{\mathsf{s}})$

Lattice Code $\Lambda/\Lambda_{\mathsf{s}}$

- Finite group under addition $\bmod \Lambda_{\mathsf{s}}$
- $|\Lambda/\Lambda_{\mathsf{s}}| = {}^{\mathrm{Vol}(\Lambda_{\mathsf{s}})}/_{\mathrm{Vol}(\Lambda)}$
- Rate $R = \frac{1}{n}\log_2 \frac{\mathrm{Vol}(\Lambda_{\mathsf{s}})}{\mathrm{Vol}(\Lambda)}$



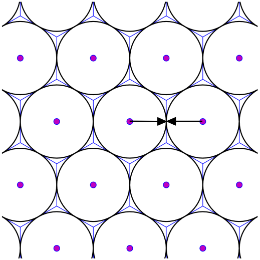
Lattice codes are good for many things: achieve capacity in AWGN and dirty paper channel, DMT in MIMO channel, relay networks (compute & forward), wiretap channels, interference channels, quantization, cryptography, etc. etc. etc.

The Sphere Packing Problem

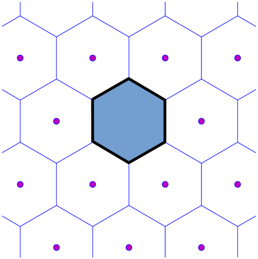
How densely can we pack identical non-intersecting spheres of radius r_{pack} in n-dimensional space

Packing radius

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



$\mathrm{Vol}(\Lambda)$



Center density $\delta(\Lambda) = \dfrac{(r_{\text{pack}}(\Lambda))^n}{\mathrm{Vol}(\Lambda)}$ is the number of spheres per unit volume when the lattice is scaled to pack spheres of unit radius

Coding lattice Λ: pack many points in a given region with large min distance

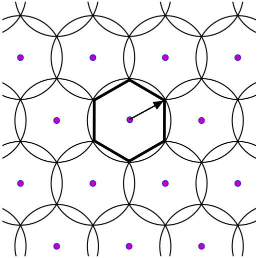
min distance $= \mathrm{d}_{\min}(\Lambda) = 2r_{\text{pack}}(\Lambda)$ No. of codewords $\propto \frac{1}{\mathrm{Vol}(\Lambda)}$

The Sphere Covering Problem

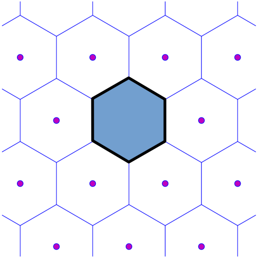
How sparsely can we arrange identical overlapping spheres of radius r_{cov} with every point in n-dimensional space covered by at least one sphere

Covering radius

$$r_{\text{cov}}(\Lambda_{\mathsf{s}}) = \sup_{\boldsymbol{x} \in \mathcal{V}(\Lambda_{\mathsf{s}})} \|\boldsymbol{x}\|$$



$\mathrm{Vol}(\Lambda_{\mathsf{s}})$



Covering thickness $\theta(\Lambda_{\mathsf{s}}) = \dfrac{(r_{\text{cov}}(\Lambda_{\mathsf{s}}))^n}{\mathrm{Vol}(\Lambda_{\mathsf{s}})}$ is the number of spheres per unit volume when the lattice is scaled to use spheres of unit radius

Shaping lattice Λ_{s}: pack many codewords in Voronoi region using min power

$$\text{power} = \frac{\mathrm{r}_{\text{cov}}(\Lambda_{\mathsf{s}})^2}{n} \qquad \text{No. of codewords} \propto \mathrm{Vol}(\Lambda_{\mathsf{s}})$$

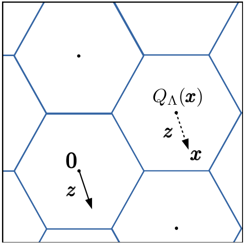
The Quantization Problem

Quantization codebook must use as few codewords as possible while minimizing the mean square error distortion

No. of codewords $\propto \dfrac{1}{\mathrm{Vol}(\Lambda)}$ Distortion $= \dfrac{\mathbb{E}\,\|\boldsymbol{x} - Q_\Lambda(\boldsymbol{x})\|^2}{n}$

- The quantization error $\boldsymbol{z} = \boldsymbol{x} - Q_\Lambda(\boldsymbol{x}) = \boldsymbol{x} \bmod \Lambda \in \mathcal{V}(\Lambda)$
- For high resolution quantization

Distortion (per dimension) $\sigma^2(\Lambda) = \dfrac{1}{\mathrm{Vol}(\Lambda)} \cdot \dfrac{1}{n} \displaystyle\int_{\boldsymbol{z} \in \mathcal{V}(\Lambda)} \|\boldsymbol{z}\|^2 \mathrm{d}\boldsymbol{z}$



Choose Λ with small normalized second moment $G(\Lambda) = \dfrac{\sigma^2(\Lambda)}{\mathrm{Vol}(\Lambda)^{2/n}}$

Coding for the Unconstrained AWGN Channel

Infinite Codebook: Λ Channel $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{z}$, Gaussian noise power: σ^2

Decoder: $\boldsymbol{y} \to Q_\Lambda(\boldsymbol{y})$ Error probability $P_e(\Lambda, \sigma^2) = \mathsf{P}\Big(\boldsymbol{z} \notin \mathcal{V}(\Lambda)\Big)$

The volume-to-noise ratio $\mu(\Lambda, \sigma^2) = \dfrac{\mathrm{Vol}(\Lambda)^{2/n}}{\sigma^2}$ defines the effective SNR of the system

The problem of coding for unconstrained AWGN channel

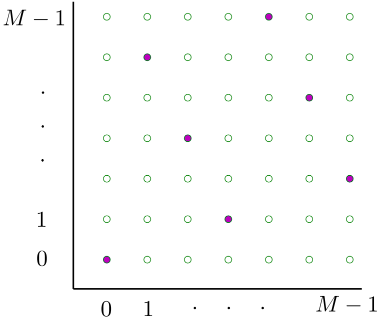
Given σ^2 and ϵ find a lattice Λ with $P_e(\Lambda, \sigma^2) = \epsilon$ and as small a VNR $\mu(\Lambda, \sigma^2)$ as possible

Lattices from Codes: Construction A

Linear Codes over $\mathbb{Z}_M$

A code $\mathcal{C} \subset \mathbb{Z}_M^n$ is linear if it is closed under addition $\mod M$

$$\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C} \Rightarrow (\boldsymbol{x} + \boldsymbol{y}) \mod M \in \mathcal{C}$$

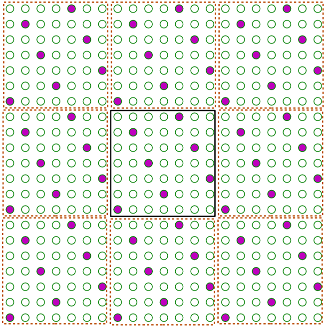


- Addition is defined component-wise modulo M
- Additive inverse exists: $-\boldsymbol{x} = (M-1)\boldsymbol{x} \mod M \in \mathcal{C}$
- Additive identity exists: $\mathbf{0} \in \mathcal{C}$
- $\mathcal{C}$ is a group.
- Embed $\mathcal{C}$ into $\mathbb{R}^n$ using natural map

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

Lattices from Codes: Construction A

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



- Mod-M lattice: $M\mathbb{Z}^n \subset \Lambda \subset \mathbb{Z}^n$
- Usually, $M =$ prime, which makes $\mathbb{Z}_M$ a *field*
- If $\Lambda_\mathsf{s} = M\mathbb{Z}^n$ is used as shaping lattice, then $\Lambda/\Lambda_\mathsf{s} \cong \mathcal{C}$

Mod-2 lattices: $M = 2$ and, say, $|\mathcal{C}| = 2^k$, $w_\mathrm{H} = \min$ Hamming distance

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

Several other constructions of lattices: Constructions B, D, constructions from algebraic number fields, etc.

Rings and Fields

Definition

A set $\mathbb{D}$ endowed with operations '$+$' and '$\cdot$' is a ring if

1. $(\mathbb{D}, +)$ is a group $\Rightarrow$ addition well defined.
2. $(\mathbb{D}, \cdot)$ is a monoid
   - $a(bc) = (ab)c$ for all $a, b, c \in \mathbb{D}$
   - there exists a multiplicative identity $1 \in \mathbb{D}$: $1 \cdot a = a \cdot 1 = a$
3. $a(b + c) = ab + ac \Rightarrow$ addition and multiplication interact nicely

Definition

A ring $(\mathbb{D}, +, \cdot)$ is a field if $(\mathbb{D} \setminus \{0\}, \cdot)$ is a group

Examples

- $\mathbb{Z}$ – the set of integers with usual addition and multiplication
- $\mathbb{R}, \mathbb{C}, \mathbb{Q}$ – real, complex and rational numbers
  - Further, can divide by any non-zero element $\Rightarrow$ fields.

Euclidean Domain

Definition

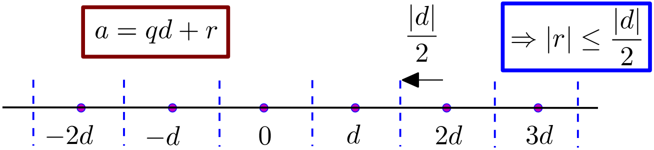
A Euclidean domain $\mathbb{D}$ is a ring such that

1. **No zero divisors**
   product of non-zero elements is non-zero
2. **Division with small remainder**
   there is a function $N : \mathbb{D} \to \{0, 1, 2, \ldots\}$ such that
   - for any $a, d \in \mathbb{D}$, there exists q, r such that

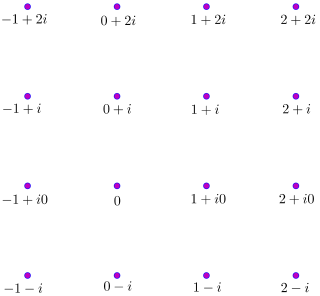
$$a = qd + r \text{ and } N(r) < N(d)$$

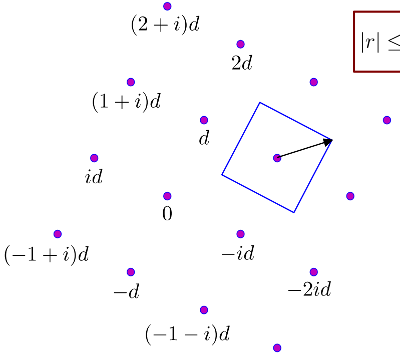
Example

$\mathbb{D} = \mathbb{Z}$ is a Euclidean domain: $N(a) = |a|$ is the absolute value



Gaussian Integers $\mathbb{Z}[i]$





$$\boxed{|r| \le \frac{|d|}{\sqrt{2}}}$$

$$i = \sqrt{-1}$$

$$\mathbb{Z}[i] = \{m + in \mid m, n \in \mathbb{Z}\}$$

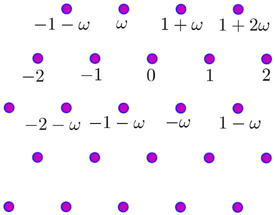
$$N(m+in) = |m+in|^2 = m^2+n^2$$

<u>Division with small remainder</u>

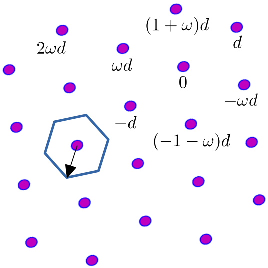
For $a, d \in \mathbb{Z}[i]$

$a = qd + r$, with $N(r) \le \dfrac{N(d)}{2}$

Eisenstein Integers $\mathbb{Z}[\omega]$



$$|r| \le \frac{|d|}{\sqrt{3}}$$



$$\omega = \exp\left(\frac{i2\pi}{3}\right)$$

$$\mathbb{Z}[\omega] = \{m + n\omega \,|\, m, n \in \mathbb{Z}\}$$

$$N(m+n\omega) = |m+n\omega|^2 = m^2 - mn + n^2$$

Division with small remainder

$a = qd + r,$ with

$$N(r) \le \frac{N(d)}{3}$$

Hurwitz Quaternionic Integers $\mathbb{H}$

Hyper-complex numbers with 4 components

$$\mathbb{H} = \left\{ a + ib + jc + kd \,\middle|\, a, b, c, d \in \mathbb{Z} \text{ or } a, b, c, d \in \mathbb{Z} + \frac{1}{2} \right\}$$

Geometry

- $(a + ib + jc + kd) \to (a, b, c, d)$ generates the lattice $D_4^* \subset \mathbb{R}^4$
- $\mathrm{d}_{\min}(D_4^*) = 1$ and $\mathrm{Vol}(D_4)^* = {}^1\!/_2$

Algebra

- *Non-commutative* multiplication: $i^2 = j^2 = k^2 = ijk = -1$
- Norm $N(a + ib + jc + kd) = a^2 + b^2 + c^2 + d^2 \in \mathbb{Z}$
- Division with small remainder

$$a = qd + r \text{ with } N(r) \leq \frac{N(d)}{2}$$

Gaussian and Eisenstein Lattices

A complex lattice is a discrete group of points in $\mathbb{C}^n$

- Gaussian lattice $\Lambda = \{\boldsymbol{G}\boldsymbol{u} \,|\, \boldsymbol{u} \in \mathbb{Z}[i]^n\}$, $\boldsymbol{G} \in \mathbb{C}^{n\times n}$ full-rank
- Eisenstein lattice $\Lambda = \{\boldsymbol{G}\boldsymbol{u} \,|\, \boldsymbol{u} \in \mathbb{Z}[\omega]^n\}$, $\boldsymbol{G} \in \mathbb{C}^{n\times n}$ full-rank

The real version is obtained by natural embedding

$$\begin{aligned} \mathbb{C}^n &\to \quad \mathbb{R}^{2n} \\ \boldsymbol{\lambda} &\to (\mathrm{Re}(\boldsymbol{\lambda}), \mathrm{Im}(\boldsymbol{\lambda})) \end{aligned}$$

Let $\Lambda \subset \mathbb{C}^n$ be a $\mathbb{D}$–lattice where $\mathbb{D} = \mathbb{Z}[i]$ or $\mathbb{Z}[\omega]$

- $M\Lambda$ is a sub-lattice of Λ for any $M \in \mathbb{D}$
- $\Lambda/M\Lambda$ is a lattice code

Ideals

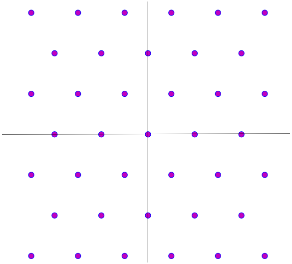
Definition

An ideal $\mathcal{I}$ of a ring $\mathbb{D}$ is a subset $\mathcal{I} \subset \mathbb{D}$ such that

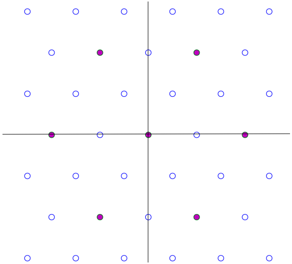
1. $(\mathcal{I}, +)$ is a group $\Rightarrow$ a subgroup of $(\mathbb{D}, +)$
2. $a\mathcal{I} \subset \mathcal{I}$ for any $a \in \mathbb{D}$

Property Every ideal of an Euclidean domain $\mathbb{D}$ is of the form $\mathcal{I} = M\mathbb{D}$ for some $M \in \mathbb{D}$

$\mathbb{D} = \mathbb{Z}[\omega]$

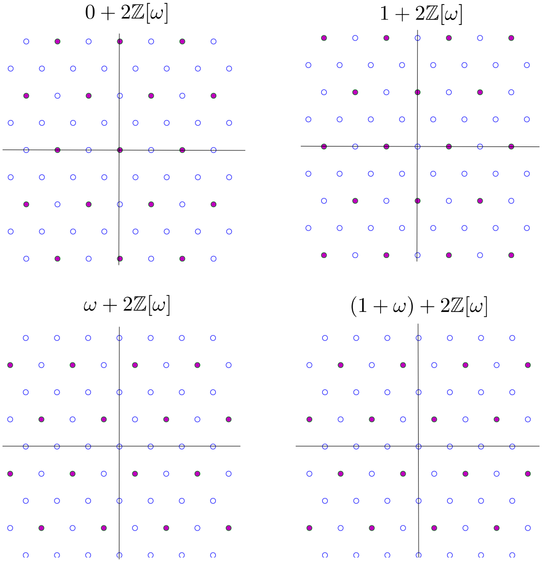


$\mathcal{I} = 2\mathbb{Z}[\omega]$



Cosets of Ideals

Coset of $M\mathbb{D}$ in $\mathbb{D}$: $a + M\mathbb{D}$, where $a \in \mathbb{D}$



Quotient Ring $\mathbb{D}/M\mathbb{D}$

- $\mathbb{D}/M\mathbb{D} =$ set of all cosets of $M\mathbb{D}$ in $\mathbb{D}$.

$$\mathbb{Z}[\omega]/2\mathbb{Z}[\omega] = \{0 + 2\mathbb{Z}[\omega], 1 + 2\mathbb{Z}[\omega], \omega + 2\mathbb{Z}[\omega], 1 + \omega + 2\mathbb{Z}[\omega]\}$$

- Can add, subtract and multiply cosets

$$(a + M\mathbb{D}) + (b + M\mathbb{D}) = (a + b) + M\mathbb{D}$$

$$(a + M\mathbb{D}) \cdot (b + M\mathbb{D}) = ab + M\mathbb{D}$$

$\boxed{\mathbb{D}/M\mathbb{D} \textbf{ forms a ring with this definition}}$

$\mathbb{D}/M\mathbb{D}$ is a field if M is *prime* in $\mathbb{D}$.

Example

- $(1 + 2\mathbb{Z}[\omega]) + (1 + 2\mathbb{Z}[\omega]) = 2 + 2\mathbb{Z}[\omega] = 0 + 2\mathbb{Z}[\omega]$
- $(\omega + 2\mathbb{Z}[\omega]) \cdot (\omega + 2\mathbb{Z}[\omega]) = \omega^2 + 2\mathbb{Z}[\omega] = (1 + \omega) + 2\mathbb{Z}[\omega]$
- $-(\omega + 2\mathbb{Z}[\omega]) = -\omega + 2\mathbb{Z}[\omega] = \omega + 2\mathbb{Z}[\omega]$

Coset Leaders of $\mathbb{D}/M\mathbb{D}$

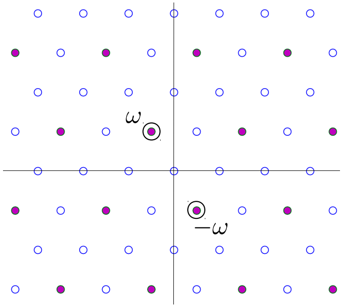
Coset leader

- is a representative element of a coset.
- usually, it is an element with the smallest norm in a coset.
- Identify $\mathbb{D}/M\mathbb{D}$ as the set of coset leaders.

Example $\mathbb{Z}[\omega]/2\mathbb{Z}[\omega]$

- $0 + 2\mathbb{Z}[\omega] \to 0$
- $1 + 2\mathbb{Z}[\omega] \to 1$
- $\omega + 2\mathbb{Z}[\omega] \to \omega$
- $1 + \omega + 2\mathbb{Z}[\omega] \to 1 + \omega$

$$\boxed{\mathbb{Z}/2\mathbb{Z}[\omega] = \{0,\ 1,\ \omega,\ 1+\omega\}}$$



Finite Constellations with Ring Structure

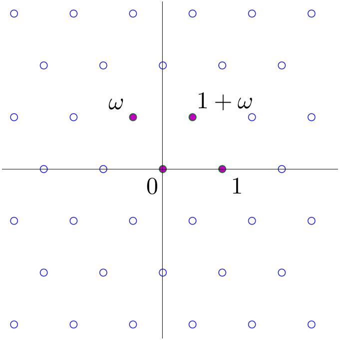
- For any $a \in \mathbb{D}$, $a \bmod M\mathbb{D} \triangleq$ coset leader of $(a + M\mathbb{D})$
- Identify $\mathbb{D}/M\mathbb{D} \triangleq$ set of all coset leaders
- $\mathbb{D}/M\mathbb{D}$ is a ring under modulo arithmetic

Addition: $(a + b) \bmod M\mathbb{D}$

Multiplication: $(ab) \bmod M\mathbb{D}$

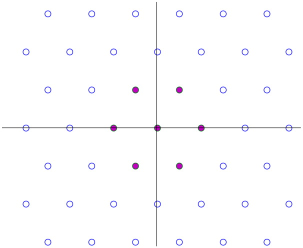
Multiplication in $\mathbb{Z}[\omega]/2\mathbb{Z}[\omega] \cong \mathbb{F}_4$

$\times$	0	1	ω	$1+\omega$
0	0	0	0	0
1	0	1	ω	$1+\omega$
ω	0	ω	$1+\omega$	1
$1+\omega$	0	$1+\omega$	1	ω

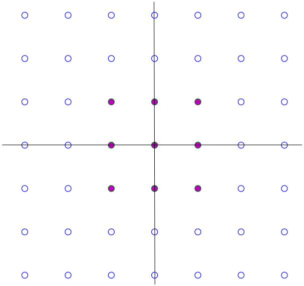


Finite Constellations with Ring Structure

$\mathbb{Z}[\omega]/(1+3\omega)\mathbb{Z}[\omega] \cong \mathbb{F}_7$



$\mathbb{Z}[i]/3\mathbb{Z}[i] \cong \mathbb{F}_3 \times \mathbb{F}_3$



$$|\mathbb{D}/M\mathbb{D}| = \begin{cases} |M|^2 & \text{if } \mathbb{D} = \mathbb{Z}[i] \text{ or } \mathbb{Z}[\omega] \\ |M| & \text{if } \mathbb{D} = \mathbb{Z} \end{cases}$$

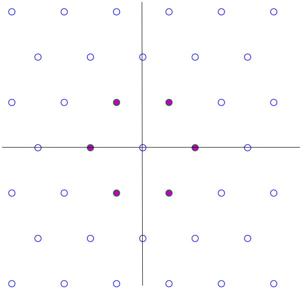
Units of $\mathbb{D}$

- Units are elements with multiplicative inverse

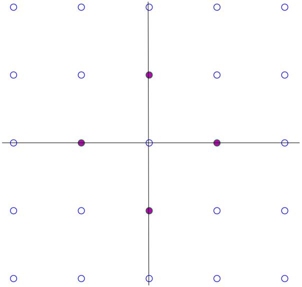
$$a \in \mathbb{D} \text{ is a unit iff } ab = 1 \text{ for some } b \in \mathbb{D}$$

- Units of $\mathbb{Z} = \{+1, -1\}$
- Units of $\mathbb{Z}[\omega]$ and $\mathbb{Z}[i]$:

$\mathbb{Z}[\omega]$



$\mathbb{Z}[i]$



In both cases, $a \in \mathbb{D}$ is a unit iff $|a| = 1$

Greatest Common Divisor (GCD)

Given $a, b \in \mathbb{D}$

- Generate the ideal $\mathcal{I} = a\mathbb{D} + b\mathbb{D} = \{am + bn \,|\, m, n \in \mathbb{D}\}$
- This ideal can be generated by a single element d, i.e., $\mathcal{I} = d\mathbb{D}$

$$\boxed{d \triangleq \gcd(a, b)}$$

Properties

- $d|a$ and $d|b$, i.e., $a = md$ and $b = nd$ for some $m, n \in \mathbb{D}$
- Any divisor of a and b divides d

Definition

$a, b \in \mathbb{D}$ are relatively prime if $\gcd(a, b) = 1$

Relatively prime $\Leftrightarrow a\mathbb{D} + b\mathbb{D} = \mathbb{D}$

Primes in $\mathbb{D}$

Definition

An element $\phi \in \mathbb{D}$ is prime if ϕ is not a product of two non-units.

Properties

- If ϕ_1 and ϕ_2 are prime then

$$\text{either } \phi_1 = \text{unit} \times \phi_2 \text{ or } \gcd(\phi_1, \phi_2) = 1$$

- Any $M \in \mathbb{D}$ can be factorized into primes

$$M = \text{unit} \times \phi_1^{k_1}\,\phi_2^{k_2} \cdots \phi_n^{k_n} \text{ with } \gcd(\phi_i, \phi_j) = 1$$

- Say $M = \text{unit} \times \phi_1^{k_1}\,\phi_2^{k_2} \cdots \phi_n^{k_n}$ and $N = \text{unit} \times \rho_1^{k_1}\,\rho_2^{k_2} \cdots \rho_m^{k_m}$

$$\gcd(M, N) = 1 \text{ iff } \gcd(\phi_i, \rho_j) = 1 \text{ for all } i, j$$

Primes in $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$

Tables of first few primes that are relatively prime

Primes in $\mathbb{Z}[i]$

Norm $\lvert\phi\rvert^2$	Prime ϕ
2	$1+i$
5	$1+2i, 1-2i$
9	3
13	$2+3i, 2-3i$
17	$1+4i, 1-4i$
29	$2+5i, 2-5i$
37	$1+6i, 1-6i$
41	$4+5i, 4-5i$
49	7
53	$2+7i, 2-7i$

Primes in $\mathbb{Z}[\omega]$

Norm $\lvert\phi\rvert^2$	Prime ϕ
3	$1-\omega$
4	2
7	$1+3\omega, 1+3\overline{\omega}$
13	$1+4\omega, 1+4\overline{\omega}$
19	$2+5\omega, 2+5\overline{\omega}$
25	5
31	$1+6\omega, 1+6\overline{\omega}$
37	$3+7\omega, 3+7\overline{\omega}$
43	$1+7\omega, 1+7\overline{\omega}$
61	$4+9\omega, 4+9\overline{\omega}$

Chinese Remainder Theorem (over $\mathbb{Z}$)

Given relatively prime $M_1, \ldots, M_K \in \mathbb{Z}$, let $M = \prod_{k=1}^{K} M_k$.

Theorem

For any set of K elements $w_k \in \mathbb{Z}/M_k\mathbb{Z}$, $k = 1, \ldots, K$, there exists a unique $x \in \mathbb{Z}/M\mathbb{Z}$ with

$$x \bmod M_1 = w_1, \quad x \bmod M_2 = w_2, \quad \ldots, \quad x \bmod M_K = w_K$$

The one-to-one correspondence is given by

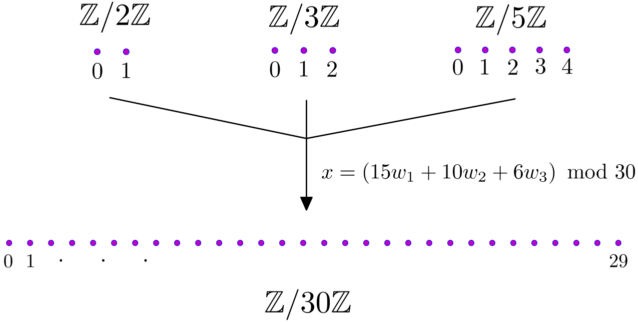
$$\begin{aligned} \mathbb{Z}/M_1\mathbb{Z} \times \cdots \times \mathbb{Z}/M_K\mathbb{Z} \to & \qquad \mathbb{Z}/M\mathbb{Z} \\ (w_1, \cdots, w_K) \quad & \to w_1 \frac{M}{M_1} + \cdots + w_K \frac{M}{M_K} \bmod M\mathbb{Z} \end{aligned}$$

This is an isomorphism between two rings

$\mathbb{Z}/M_1\mathbb{Z} \times \cdots \times \mathbb{Z}/M_K\mathbb{Z}$: component-wise addition and multiplication performed modulo M_k at the k^{th} comp.

$\mathbb{Z}/M\mathbb{Z}$: arithmetic performed modulo M

$(M_1, M_2, M_3) = (2, 3, 5)$ and $M = 30$



Chinese Remainder Theorem (over $\mathbb{D}$)

- Let $M_1, \ldots, M_K \in \mathbb{D}$ be relatively prime

$$\gcd(M_i, M_j) = 1 \text{ for all } i \neq j$$

- Let $M = M_1 \, M_2 \cdots M_K$, then ${}^{M}\!/\!{}_{M_i} = \prod_{j \neq i} M_j$

Theorem

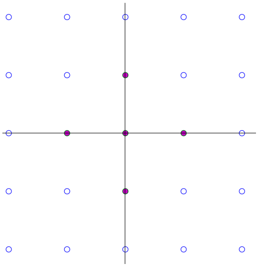
The following map is a one-to-one correspondence between $\mathbb{D}/M_1\mathbb{D} \times \mathbb{D}/M_2\mathbb{D} \times \cdots \times \mathbb{D}/M_K\mathbb{D} \to \mathbb{D}/M\mathbb{D}$

$$\mathcal{M}(w_1, \ldots, w_K) \to w_1 \frac{M}{M_1} + \cdots + w_K \frac{M}{M_K} \bmod M\mathbb{D}$$

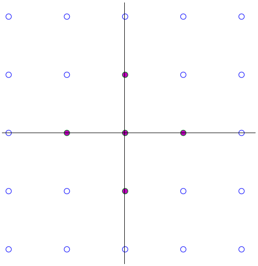
Remarks

- The constellation $\mathbb{D}/M\mathbb{D}$ encodes K messages taking values from the quotient rings $\mathbb{D}/M_k\mathbb{D}$, $k = 1, \ldots, K$
- If M_k is prime in $\mathbb{D}$, then $\mathbb{D}/M_k\mathbb{D}$ is a finite field.

$w_1 \in \mathbb{Z}[i]/(1+2i)\mathbb{Z}[i] \cong \mathbb{F}_5$

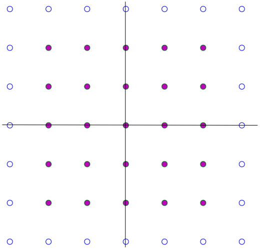


$w_2 \in \mathbb{Z}[i]/(1-2i)\mathbb{Z}[i] \cong \mathbb{F}_5$



$$x = w_1(1-2i) \; + \; w_2(1+2i) \bmod 5\mathbb{Z}[i]$$

$$\boxed{\begin{array}{c} 5 = (1+2i)(1-2i) \\ \gcd(1+2i, 1-2i) = 1 \end{array}}$$



$x \in \mathbb{Z}[i]/5\mathbb{Z}[i]$

$\boxed{\text{25-QAM}}$

Lattices from Codes: Construction π_A

$\boxed{\text{Construct a lattice using } K \text{ linear codes, one each over } \mathbb{D}/\phi_k\mathbb{D}}$

- Choose K relatively-prime primes $\phi_1, \ldots, \phi_K \in \mathbb{D}$, $M = \prod_{k=1}^{K} \phi_k$
  - Each $\mathbb{D}/\phi_k\mathbb{D}$ is a finite field
- Construct K linear codes, $\mathcal{C}_k \subset (\mathbb{D}/\phi_k\mathbb{D})^n$, $k = 1, \ldots, K$
- Generate a code $\mathcal{C} \subset (\mathbb{D}/M\mathbb{D})^n$ using Chinese remainder theorem

$$\mathcal{M}(\mathcal{C}_1, \ldots, \mathcal{C}_K) = \mathcal{C}$$
$$(\boldsymbol{c}_1, \ldots, \boldsymbol{c}_K) \to \frac{M}{\phi_1}\boldsymbol{c}_1 + \cdots + \frac{M}{\phi_K}\boldsymbol{c}_K \bmod M\mathbb{D}^n$$

- Tile shifted copies of $\mathcal{C}$ to obtain a lattice: $\Lambda = \mathcal{C} + M\mathbb{D}^n$

Lattice codes obtained from Construction π_A lattices can be used in compute-and-forward and to attain AWGN channel capacity under **low-complexity multistage decoding**.