Lattice coding over AWGN channel
- Introduction -

Vincent Herbert

TELECOM Bretagne - Département SC

Monday, February 4, 2013 - 10h

Course Material

John Horton Conway and Neil James Alexander Sloane.
Sphere-Packings, Lattices, and Groups.
Springer-Verlag New York, Inc., 1987.

David Forney.
Lattice and Trellis Codes - Lectures 24 and 25
http://ocw.mit.edu, 2005.

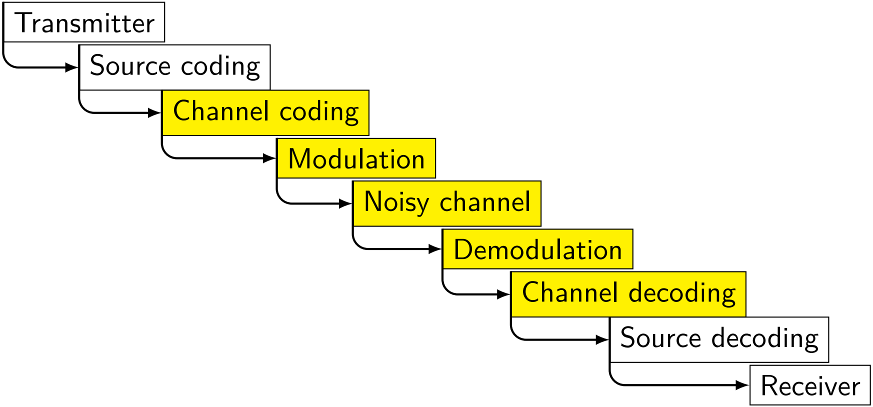
Sphere Packing, Lattices

These objects are studied in different areas.

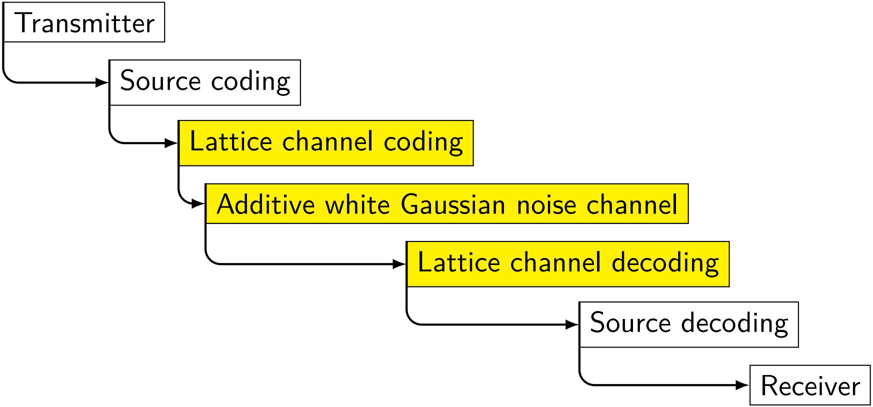
- mathematics
- analog-to-digital conversion
- data compression
- design of error-correcting codes
- digital signature
- data encryption
- cristallography
- ...

They have both a theoretical and practical interest.

Communication Channel



Today Example : Lattice Communication Channel



Nyquist-Shannon sampling theorem (1949)

Theorem

Let f be a signal (i.e. a function of time) contain no frequencies higher than cutoff frequency, W hertz. It is completely determined by giving its ordinates at a series of points spaced $\frac{1}{2W}$ second apart.

Guess f has almost all of its energy in $[0, T]$.

Sample f each $\frac{1}{2W}$ second during T seconds.

Set $F = (f(0), f(\frac{1}{2W}), f(\frac{2}{2W}), \ldots, f(\frac{n-1}{2W}))$ where $n = 2TW$.

We obtain f from F with the cardinal series :

$$f(t) = \sum_{i=0}^{\infty} f(\frac{i}{2W}) \frac{sin(2\pi W(t - i/2W))}{2\pi W(t - i/2W)}.$$

Signal energy and average power

Let $\mathcal{E}_f$ be the energy in $f(t)$.

$$\mathcal{E}_f := \int_{-\infty}^{\infty} |f(t)|^2 \,\mathrm{d}t$$

Proposition

$$\mathcal{E}_f = \frac{1}{2W} \sum_{i=0}^{n-1} f^2(\frac{i}{2W})$$

Let $\mathcal{P}$ be the average power in $f(t)$.

$$\mathcal{P} := \frac{1}{T}\mathcal{E}_f$$

Norm and signal energy

Let $\|.\|$ be the Euclidean norm or length.

$$\boxed{\|F\|^2 := F \cdot F}$$

Let us remind $n = 2TW$.

Proposition

$\|F\|^2 = 2W\mathcal{E}_f = n\mathcal{P}$

The squared length is proportionnal to the energy in $f(t)$.

F is on the n-sphere of radius $\sqrt{n\mathcal{P}}$ centered at the origin.

Additive white Gaussian noise channel

The AWGN channel transmits continuous signals.

Let $Y = (Y_i)_{1 \leqslant i \leqslant n}$ be a family of *i.i.d* random variables.
Guess $Y_i \hookrightarrow \mathcal{N}(0, \sigma^2)$ for all $1 \leqslant i \leqslant n$.
σ^2 is the average power of the noise.

Information signal $f(t)$

↓

Transmitted signal $F = (f(0),\ f(\frac{1}{2W})\ , f(\frac{2}{2W}),\ \ldots,\ f(\frac{n-1}{2W}))$

↓

Received signal $F + Y$

For the AWGN channel, the code $\mathcal{C}$ is a set of points in $\mathbb{R}^n$.

Denote M the cardinality of $\mathcal{C}$.

The rate of the code is :

$$\boxed{R = \frac{1}{T} \log_2(M) \text{ bits/s}}$$

Each codeword represents a signal of bandwidth W and duration T.

Notice the rate is sometimes defined as :

$$R = \frac{1}{n} \log_2(M) \text{ bits/dimension}$$

Reducing noise effects over AWGN channel

We want a code with big minimum distance to correct numerous errors.

But, keep in mind, we have a power constraint on the signal.

Indeed, the squared length is proportionnal to the energy in the signal.

Thus, it could be too costly.

Noisy-channel coding theorem ensures the existence of a solution.

But, it does not exhibit a way to construct it.

Noisy-channel coding theorem

Let P_e be the error probability, that is, the probability of a decoding error.

The signal-to-noise ratio SNR is equal to $\dfrac{\mathcal{P}}{\sigma^2}$.

Theorem

For any rate $R < C = W \log_2(1 + \text{SNR})$ *bits/s with* T *and thus* $n = 2WT$ *sufficiently large, there exists a code of rate* R*, average power* $\mathcal{P}$*, for which* P_e *is arbitrarily small.*
Conversely, such codes do not exist for rates $R \geqslant C$*.*

C is called the channel capacity or the Shannon limit.

The spectral efficiency η is equal to $\dfrac{R}{W}$. It is measured in *bit/s/Hz*.

In practice, we often use : $\text{SNR}_{dB} = 10 \log_{10} \text{SNR}$.

Error probability

Let $\mathcal{C} = \{c_1, \ldots, c_M\}$. Let $V(x)$ be the Voronoi cell of any $x \in \mathcal{C}$.

Let x be the sent codeword and y the received word.

y is correctly decoded if and only if $y \in V(x)$.

$$P(y \in V(x)) = \frac{1}{(\sigma\sqrt{2\pi})^n} \int_{V(x)} e^{-\frac{1}{2}\left(\frac{x}{\sigma}\right)^2} \mathrm{d}x$$

Assume each codeword has the same probability to be sent (uniformity).

$$P_e = 1 - \frac{1}{M} \sum_{i=1}^{M} P(y \in V(c_i))$$

Gaussian channel coding problem

Error-correcting code version

Find a n-dimensional code $\{c_1, \ldots, c_M\}$ *such that*

$$\|c_i\|^2 \leqslant n\mathcal{P} \text{ for } i = 1, \ldots, M$$

for which P_e *is minimized.*

Real lattice

A lattice $\Lambda \subseteq \mathbb{R}^n$ is a discrete additive subgroup of the Euclidean space $\mathbb{R}^n$.

- (additive subgroup) $\Lambda \subseteq \mathbb{R}^n$ is closed under substraction
- (discrete) There is an $\epsilon > 0$ such that any two distinct lattice points $x \neq y \in \Lambda$ are at distance at least ϵ. There is no accumulation point.

It is also a free $\mathbb{Z}$-module (free abelian group).

A free module is a module which possess a basis.

The cardinal of a basis is the rank of the module. It is often understood as the dimension.

The cardinal of a lattice is infinite.

Counterexample : $\mathbb{Q}^n$ and $\mathbb{Z} + x\mathbb{Z}$ with $x \in \mathbb{R}\backslash\mathbb{Q}$ are not lattices.
0 is an accumulation point.

Lattice parameters

Let $B = (b_1, b_2, \ldots, b_k)$ be a basis of a lattice Λ with dimension k in $\mathbb{R}^n$.

Let $b_{i,j}$ be the $j-$th coordinate the $n-$coordinates vector b_i.

$$G := \begin{pmatrix} b_{1,1} & b_{1,2} & b_{1,3} & \ldots & b_{1,n} \\ b_{2,1} & b_{2,2} & b_{2,3} & \ldots & b_{2,n} \\ \vdots & \vdots & \vdots & & \vdots \\ b_{k,1} & b_{k,2} & b_{k,3} & \ldots & b_{k,n} \end{pmatrix}$$

G is a generator matrix of Λ.

$$\Lambda = \mathbb{Z}^k G$$

The $k-$order matrix $A := GG^t$ is called the Gram matrix.

The $(i, j)^{th}$ entry of A is equal to $b_i \cdot b_j$.

Lattice parameters (contd)

The fundamental region Π of Λ is :

$$\left\{ \lambda_1 b_1 + \ldots + \lambda_k b_k : 0 \leqslant \lambda_i < 1,\ \forall i \in [\![1, k]\!] \right\}$$

We can choose different bases of Λ and thus different fundamental regions.

But, the volume of fundamental regions is invariant.

It is named the (fundamental) volume of Λ.

$$\boxed{\mathrm{Vol}(\Pi) = \sqrt{|\mathrm{Det}(Gram)|}}$$

If Λ has full-rank, that is $k = n$, then $\mathrm{Vol}(\Pi) = |\mathrm{Det}(B)|$.

Gaussian channel coding problem (contd)

Assume the code forms a lattice.

Then, all the Voronoi cells are congruent to a polytope V.

V has the same volume than Π.

$$P_e = 1 - \frac{1}{(\sigma\sqrt{2\pi})^n} \int_V e^{-\frac{1}{2}(\frac{x}{\sigma})^2} \mathrm{d}x$$

Lattice version

Find a n-dimensional lattice of volume 1 for which P_e is minimized.

Toy example : In 1D, there is only one lattice of volume 1.

This is an integer lattice $\mathbb{Z}$. Not to be confused with an integral lattice.

But, for real-life examples, we upper bound P_e with simpler expressions.

Main lattice problems

- Geometrical problems
  - Packing : densest packing of equal non-overlapping spheres
  - Covering : thinnest covering of equal overlapping spheres
  - Quantizing : closest point of a set from a received point
- Communication problem
  - Channel Coding : power-constrained code with minimum P_e

Sphere packings, lattices and codes

A sphere packing is described by the set of centers and their radius.

When the set of centers form a lattice, it is a lattice packing.

Lattice packings will be often understood as lattices.

Coded modulation systems can be obtained from a lattice.

We focus on some of them : lattice constellations or lattice codes.

Sphere packings and particularly lattices can be constructed from codes.

There often exist different constructions for a same lattice.

Lattice parameters (contd)

Let V_n be the volume of the $n-$dimensional unit sphere.

The radius of the spheres in a lattice is the packing radius ρ.

The density of Λ is the proportion of the space occupied by the spheres :

$$\boxed{\Delta := \frac{V_n \rho^n}{\mathrm{Vol}(\Pi)}}$$

The larger the volume, the sparser the lattice.

The center density of Λ is :

$$\delta := \frac{\Delta}{V_n}$$

In 2D, the hexagonal lattice A_2 is the densest packing.

In 3D, the face-centered cubic lattice A_3 is the densest lattice.

But, it is not known if it is the densest packing.

Construction A (Leech, 1964)

Let $\mathcal{C}$ be a binary code with minimum Hamming distance d and $x \in \mathbb{R}^n$.

x belongs to the set of centers $\Leftrightarrow$ x is congruent to a word of $\mathcal{C}$ modulo 2

If $\mathcal{C}$ is linear, the sphere packing forms a lattice.

If two distinct centers are congruent, their distance is at least 2.

Else, their Hamming distance is $\geqslant d$, then their distance is $\geqslant \sqrt{d}$.

$$\rho \geqslant \frac{1}{2}\min(2, \sqrt{d})$$

This construction gives the densest sphere packings up to dimension 15.

Let us mention the E_8 lattice, for instance.

The minimum Hamming distance is always 1.

Construction A with $\mathbb{Z}[i]$-lattices

A $\mathbb{Z}[i]$-lattice $\Lambda \subseteq \mathbb{C}^n$ is a free discrete $\mathbb{Z}[i]$-module of $\mathbb{C}^n$.

We consider the lattice is generated by a basis $\{b_1, \ldots, b_n\}$ of $\mathbb{C}^n$ as :

$$\Lambda = \left\{ \sum_{i=1}^{n} a_i b_i : \forall a_i \in \mathbb{Z}[i] \right\}$$

Let $\mathcal{C}$ be a binary linear code and $x \in \mathbb{C}^n$.

x belongs to the lattice $\Leftrightarrow$ x is congruent to a word of $\mathcal{C}$ modulo $1 + i$

The minimum Hamming distance is always 1.

Construction A over different rings and alphabets

To sum up.

For real lattices : $\Lambda = \mathcal{C} + 2\mathbb{Z}^n$.

For $\mathbb{Z}[i]$-lattice : $\Lambda = \mathcal{C} + (1+i)\mathbb{Z}[i]^n$.

The real construction can be extended for linear codes over rings $\mathbb{Z}/q\mathbb{Z}$.

In this way, we obtain the lattice $\Lambda = \mathcal{C} + q\mathbb{Z}^n$.

Notice $(1+i)$ is a Gaussian prime whereas 2 is not since $2 = (1+i)(1-i)$ and 2 does not divide any factor on the right.

So $(1+i)$ is a prime in $\mathbb{Z}[i]$, it has norm $|1+i| = 2$ and thus we have :

$$\mathbb{Z}[i]/(1+i)\mathbb{Z}[i] \cong \mathbb{F}_2$$

We can also use Eisenstein integers, $\mathbb{Z}[\omega]$-lattices, $\omega = e^{i2\pi/3}$.

Other constructions

Let us mention some variants of construction A. We only give keywords.

- A_f, linear codes, real lattices, symmetric bilinear form
- A_ϕ, $\mathbb{Z}[e^{i\pi/4}]$-lattices, code over $\mathbb{F}_9$, hermitian bilinear form

Construction B (Leech, 1964)

Let $\mathcal{C}$ be an even binary code with minimum Hamming distance d and $x = (x_1, \cdots, x_n) \in \mathbb{R}^n$.

$$x \text{ belongs to the set of centers}$$
$$\Updownarrow$$
$$\left\{ \begin{array}{l} x \text{ is congruent to a word of } \mathcal{C} \text{ modulo } 2 \\ \sum_{i=1}^{n} x_i \equiv 0 \bmod 4 \end{array} \right\}$$

If $\mathcal{C}$ is linear, the sphere packing forms a lattice.

The minimum Hamming distance is always 1.

Construction C (Leech, 1964)

Most of the time, it gives non-lattice packings.

Construction D is a modified version which produces lattices .

Construction D in two words

The construction D generalizes the construction A with linear codes .

It rests upon a nested family of binary linear codes.

It always produces lattices.

Examples : Take $n = 2^m$.

- Consider $n-$length Reed-Muller codes $\mathcal{R}(2r, m)$.

  For $0 \leqslant s \leqslant t \leqslant m$, $\mathcal{R}(s, m) \subseteq \mathcal{R}(t, m)$.

  It is a way to get the $n-$dimensional Barnes-Wall lattice BW_n.

- Consider $n-$length extended BCH codes of designed distance δ.

  For $1 \leqslant \delta_1 \leqslant \delta_2 \leqslant n$, $\mathrm{BCH}(\delta_2) \subseteq \mathrm{BCH}(\delta_1)$.

  We obtain the $n-$dimensional B_n lattices.

Construction D (Barnes & Sloane, 1983)

Let $\mathcal{C}_i$ be a $[n, k_i, d_i]$ binary linear code for $i \in [\![0, a]\!]$. Let $\mathbb{F}_2^n = \mathcal{C}_0 \supset \mathcal{C}_1 \supset \ldots \supset \mathcal{C}_a$. Let $(c_1, \ldots, c_n)$ be a row basis of $\mathbb{F}_2^n$ such that :

- $c_1, \ldots c_{k_i}$ spans $\mathcal{C}_i$ for $i \in [\![0, a]\!]$.
- we can build an upper triangular matrix by permuting c_i for $i \in [\![0, n]\!]$

Let us define :

- $\bar{\sigma}_i : \mathbb{F}_2 \to \mathbb{R}, \; x \mapsto \frac{x}{2^{i-1}}$
- $\sigma_i : \mathbb{F}_2^n \to \mathbb{R}^n, \; x \mapsto (\bar{\sigma}_i(x_1), \bar{\sigma}_i(x_2), \cdots, \bar{\sigma}_i(x_n))$

A lattice in $\mathbb{R}^n$ is defined by the vectors x such that :

$$x = \sum_{i=1}^{a} \sum_{j=1}^{k_i} b_{i,j} \sigma_i(c_j) + y$$

where $b_{i,j} \in \{0, 1\}$ and $y \in 2\mathbb{Z}^n$.

The minimum Hamming distance is always 1.

Construction D' (Barnes & Sloane, 1983)

Let $\mathcal{C}_i$ be a $[n, n - r_i, d_i]$ binary linear code for $i \in [\![0, a]\!]$. Let $\mathcal{C}_0 \supset \mathcal{C}_1 \supset \ldots \supset \mathcal{C}_a$. Let $(h_1, \ldots, h_n)$ be a row basis of $\mathbb{F}_2^n$ such that :

- $h_1, \ldots h_{r_i}$ give parity check equations defining $\mathcal{C}_i$ for $i \in [\![0, a]\!]$.
- we can build an upper triangular matrix by permuting h_i for $i \in [\![0, n]\!]$

Let us define :

- $r_{-1} = 0$

A lattice in $\mathbb{Z}^n$ is defined by the vectors x such that :

$$h_j \cdot x \equiv 0 \bmod 2^{i+1}$$

where $i \in [\![0, a]\!]$ and $r_{a-i-1} + 1 \leqslant j \leqslant r_{a-i}$.

Craig's lattice

$$A_n^{(m)} = \Delta^{m-1} A_n$$

where $\Delta = \begin{pmatrix} 1 & -1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -1 \\ 1 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$ is a matrix of order n.

→ densest known packings for $148 \leqslant n \leqslant 3000$ are Craig's lattices when $n+1$ is prime and m is the nearest integer to $1/2 \ \dfrac{n}{\ln(n+1)}$.

Construction E in two words (Bos, Conway & Sloane, 1982)

It generalizes construction D amongst others.

It inputs :

- a lattice Λ in $\mathbb{R}^N$
- a nested family of n-length additive codes $(\mathcal{C}_i)_{0 \leqslant i \leqslant a}$ over an elementary abelian group ($\cong \mathbb{F}_p^b$ for p prime and b integer).

It is a recursive construction in two meanings :

- It outputs a nested family of lattices $(\Lambda_i)_{0 \leqslant i \leqslant a}$ in $\mathbb{R}^{nN}$ with $\Lambda_0 = \Lambda^n$. For some function f, $\Lambda_i = f(\Lambda_{i-1})$ and $\Lambda_{i-1} \subset \Lambda_i$ for $i \in [\![1, a]\!]$.
- It can be applied to the densest lattice Λ_a.

A lattice obtained by applying construction E to Λ is named $\eta(\Lambda)$.

This construction give the densest known lattices in high dimension.

Construction E through example

$$\Lambda = \mathbb{Z}^2,\ \mathcal{C}_0 = \mathbb{F}_2^2,\ \mathcal{C}_1 = \{00, 11\}$$

$$\Downarrow$$

$$D_4$$

$$\Downarrow$$

$$\Lambda_4 = D_4,\ \Lambda_8 = E_8,\ \Lambda_{12},\ \Lambda_{16},\ \Lambda_{20} \text{ with } n = 1, \ldots, 5.$$

$(u, u+v)$ construction

The $(u, u+v)$ construction is an algebraic construction.

Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be a $[n, k_1, d_1]$ (resp. $[n, k_2, d_2]$) linear codes.

It gives a $[2n, k_1 + k_2, \min(2d_1, d_2)]$ code :

$$\left\{ (u, u+v) : u \in \mathcal{C}_1, v \in \mathcal{C}_2 \right\}$$

Denote $\mathbb{1}$, the all-ones vector.

$$\mathcal{R}(1,1) = \mathbb{F}_2^2$$

$$\mathcal{R}(1,m) = \left\{ (u,u), (u, u+\mathbb{1}) : u \in \mathcal{R}(1, m-1) \right\}$$

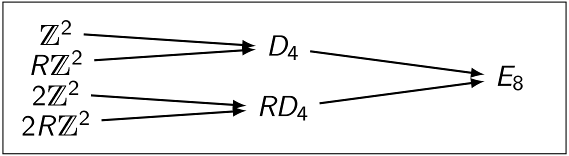
$(u, u+v)$ construction (contd)

Let Λ_1 and Λ_2 be two lattices in $\mathbb{R}^n$.

The $(u, u+v)$ construction gives a lattice in $\mathbb{R}^{2n}$:

$$\left\{ (u, u+v) : u \in \Lambda_1, v \in \Lambda_2 \right\}$$

Set $R := \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $\mathrm{BW}_2 := \mathbb{Z}^2$.



$$R^j \, \mathrm{BW}_{2^{m+1}} = \left\{ (u, u+v) : u \in R^j \, \mathrm{BW}_{2^m}, v \in R^{j+1} \, \mathrm{BW}_{2^m} \right\}$$

Current status

Most of the densest sphere packings are lattice packings.

Some non-lattice packings are denser than the densest known lattice packing.

We ignore if there exists a non-lattice packing denser than the densest lattice packing.

Density and error probability

In practice, lattice codes which minimizes P_e correspond to densest lattice.

Nevertheless, sphere packing problem and channel coding problem differ.

Both asks to maximize the packing radius ρ.

But, channel coding problem involves another parameter.

It requires to minimize the average number of code points at distance 2ρ.

Notice, the minimum distance $d = 2\rho$.

The minimum squared distance d^2 is also important parameter of a lattice.

Since $0 \in \Lambda$, d^2 is equal to the minimum squared length.

Coding gain

The coding gain of a code $\mathcal{C}_1$ over a code $\mathcal{C}_2$ of minimum distance d_1 (resp. d_2) and average energy $\mathcal{E}_1$ (resp. $\mathcal{E}_2$) is equal to

$$\gamma(\mathcal{C}_1, \mathcal{C}_2) := \frac{d_1^2 \mathcal{E}_2}{d_2^2 \mathcal{E}_1}$$

The (nominal) coding gain of a lattice Λ over the integral lattice $\mathbb{Z}^n$ is :

$$\gamma_c(\Lambda) := 4\delta^{\frac{2}{n}} = \frac{d^2}{\mathrm{Vol}(\Pi)^{\frac{2}{n}}}$$

The Hermite's constant is :

$$\gamma_n := 4\delta_n^{\frac{2}{n}}$$

where δ_n is the center density of the densest lattice in $\mathbb{R}^n$.

Practical channel codes

- permutation codes
- group codes
- spherical codes
- trellis modulation (convolutional code + geometrical channel code)
- lattice codes
- ...

Lattice codes can achieve the capacity $\frac{1}{2}\log_2(1+\mathrm{SNR})$ bits/dimension.

R. Urbanke & B. Rimoldi,
Lattice codes can achieve capacity on the AWGN channel,
IEEE Transactions on Information Theory, Vol. 44, Nr. 1, pp. 273-278, 1998

Lattice constellation

Let Λ be a lattice in $\mathbb{R}^n$, $\lambda \in \mathbb{R}^n$ and $\mathcal{R}$ be a compact region of $\mathbb{R}^n$.

$\Lambda + \lambda$ is a coset or translated of Λ.

A lattice constellation $C(\Lambda, \mathcal{R})$ is the finite set :

$$\boxed{C(\Lambda, \mathcal{R}) = (\Lambda + \lambda) \cap \mathcal{R}}$$

Notice, if $\lambda \in \Lambda$, then $\Lambda + \lambda = \Lambda$. (geometrical uniformity)

Region parameters

The volume of $\mathcal{R}$ is :

$$\text{Vol}(\mathcal{R}) = \int_{\mathcal{R}} \mathrm{d}x$$

The average energy per dimension of a uniform pdf over $\mathcal{R}$ is :

$$\mathcal{E}(\mathcal{R}) = \int_{\mathcal{R}} \frac{\|x\|^2}{n} \frac{\mathrm{d}x}{\text{Vol}(\mathcal{R})}$$

The normalized second moment of a uniform pdf over $\mathcal{R}$ is :

$$\mathcal{G}(\mathcal{R}) = \frac{\mathcal{E}(\mathcal{R})}{\text{Vol}(\mathcal{R})^{\frac{2}{n}}}$$

$\mathcal{G}(\mathcal{R})$ is invariant to scaling, orthogonal transformations, Cartesian products.

Take $n = 1$, $m \in \mathbb{Z}$, $\mathcal{R} = [-1, 1]$.

$$\mathrm{Vol}(\mathcal{R}) = 2$$

$$\mathcal{E}(\mathcal{R}) = \int_{-1}^{1} \frac{\|x\|^2}{2} \mathrm{d}x = \frac{1}{3}$$

$$\boxed{\mathcal{G}(\mathcal{R}^m) = \frac{1}{12}}$$

Total coding gain

The coding gain measures the increase in density over $\mathbb{Z}^n$:

$$\gamma_c(\Lambda) := 4\delta^{\frac{2}{n}} = \frac{d^2}{\mathrm{Vol}(\Pi)^{\frac{2}{n}}}$$

The shaping gain of the region is defined as :

$$\gamma_s(\mathcal{R}) := \frac{1/12}{\mathcal{G}_(\mathcal{R})}$$

It measures the decrease in average energy of $\mathcal{R}$ over a cube centered in 0.

The total coding gain is

$$\gamma_{tot} = \gamma_c(\Lambda)\gamma_s(\mathcal{R})$$

"[Euclidean-space coding] is to [Hamming-space coding]
as classical music is to rock and roll."
N. J. A. Sloane, Shannon Lecture

Changelog

1. lattice constellations denoted $C(\Lambda, \mathcal{R})$ instead of $\mathcal{C}$.
2. an integer lattice is $\subset \mathbb{Z}^n$
3. generator matrix $k \times n$ instead of $n \times k$
4. Constructions A,B,C,D,E