Lattices from Codes or Codes from Lattices

Amin Sakzad
Dept of Electrical and Computer Systems Engineering
Monash University
amin.sakzad@monash.edu

Oct. 2013

Union Bound Estimate

An estimate upper bound for the probability of error for a maximum-likelihood decoder of an n-dimensional lattice Λ over an unconstrained AWGN channel with noise variance σ^2 with coding gain $\gamma(\Lambda)$ and volume-to-noise ratio $\alpha^2(\Lambda, \sigma^2)$:

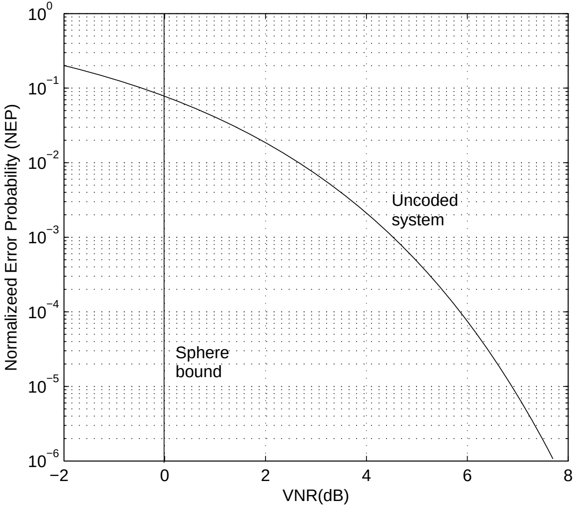
Union Bound Estimate

An estimate upper bound for the probability of error for a maximum-likelihood decoder of an n-dimensional lattice Λ over an unconstrained AWGN channel with noise variance σ^2 with coding gain $\gamma(\Lambda)$ and volume-to-noise ratio $\alpha^2(\Lambda, \sigma^2)$:

$$P_e(\Lambda, \sigma^2) \lesssim \frac{\tau(\Lambda)}{2} \text{erfc}\left(\sqrt{\frac{\pi e}{4}\gamma(\Lambda)\alpha^2(\Lambda, \sigma^2)}\right),$$

where

$$\text{erfc(t)} = \frac{2}{\sqrt{\pi}} \int_t^{\infty} \exp(-t^2) dt.$$


10^0
10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
10^{-6}
Normalizeed Error Probability (NEP)
−2
0
2
4
6
8
VNR(dB)
Uncoded system
Sphere bound

Lower Bound on Probability of Error

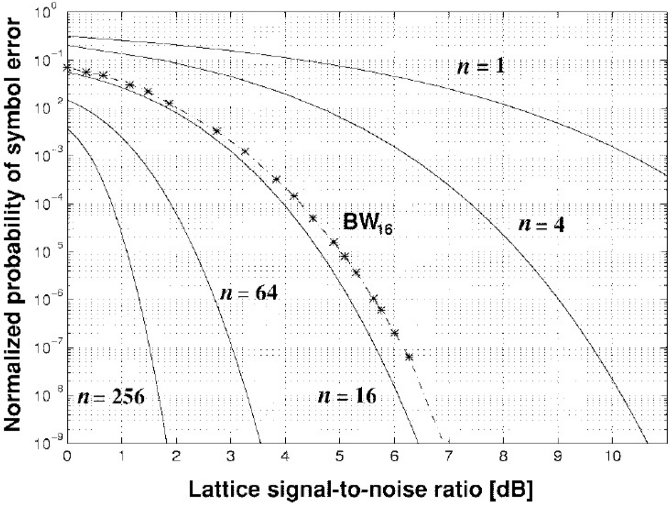
Theorem (Tarokh'99)

If points of an n-dimensional lattice are transmitted over unconstrained AWGN channel with noise variance σ^2, the probability of symbol error under maximum-likelihood decoding is lower-bounded as follows:

$$P_e(\Lambda, \sigma^2) \geq e^{-z}\left(1 + \frac{z}{1!} + \frac{z^2}{2!} + \cdots + \frac{z^{\frac{n}{2}-1}}{\left(\frac{n}{2}-1\right)}\right),$$

where

$$z = \alpha^2(\Lambda, \sigma^2)\Gamma\left(\frac{n}{2}+1\right)^{n/2}.$$


Normalized probability of symbol error
Lattice signal-to-noise ratio [dB]
n = 1
n = 4
n = 16
n = 64
n = 256
BW16
10^0
10^-1
10^-2
10^-3
10^-4
10^-5
10^-6
10^-7
10^-8
10^-9
0
1
2
3
4
5
6
7
8
9
10

Upper Bound on Coding Gain

Theorem (Tarokh'99)

Let $\zeta(k; P_e)$ *denote the unique solution of equation*

$$(1 - \mathit{erfc}(x))^{2k} = 1 - P_e,$$

and let $n = 2k$*, then:*

$$\gamma(\Lambda) \leq \frac{\zeta(k; P_e)^2}{\xi(k; P_e)} \cdot \frac{4(k!)^{\frac{1}{k}}}{\pi},$$

where $\xi(k; P_e)$ *is the unique solution of*

$$G_k(x) \triangleq e^{-x}\left(1 + \frac{x}{1!} + \cdots + \frac{x^{k-1}}{(k-1)!}\right) = P_e.$$

Backgrounds

- Linear code $\mathcal{C}[n, k, d_{\min}]$ and its generator matrix $\mathbf{G}$.

Backgrounds

- Linear code $\mathcal{C}[n, k, d_{\min}]$ and its generator matrix $\mathbf{G}$.
- Parity check matrix $\mathbf{H}$.

Backgrounds

- Linear code $\mathcal{C}[n, k, d_{\min}]$ and its generator matrix $\mathbf{G}$.
- Parity check matrix $\mathbf{H}$.
- Set $r = n - k$ and rate is $\mathfrak{r} = \frac{k}{n}$.

Backgrounds

- Linear code $\mathcal{C}[n, k, d_{\min}]$ and its generator matrix $\mathbf{G}$.
- Parity check matrix $\mathbf{H}$.
- Set $r = n - k$ and rate is $\mathfrak{r} = \frac{k}{n}$.
- Message-Passing algorithms for decoding.

Backgrounds

- Linear code $\mathcal{C}[n, k, d_{\min}]$ and its generator matrix $\mathbf{G}$.
- Parity check matrix $\mathbf{H}$.
- Set $r = n - k$ and rate is $\mathfrak{r} = \frac{k}{n}$.
- Message-Passing algorithms for decoding.
- Polynomial-time decoding algorithm if the corresponding "Tanner graph" has no cycle.

Backgrounds

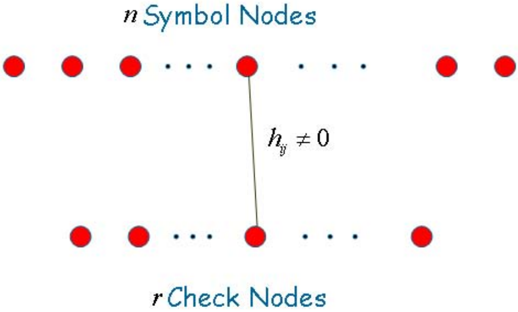
- Linear code $\mathcal{C}[n, k, d_{\min}]$ and its generator matrix $\mathbf{G}$.
- Parity check matrix $\mathbf{H}$.
- Set $r = n - k$ and rate is $\mathfrak{r} = \frac{k}{n}$.
- Message-Passing algorithms for decoding.
- Polynomial-time decoding algorithm if the corresponding "Tanner graph" has no cycle.
- Low-density Parity check (LDPC) code.

Tanner graph constructions for codes

Let $\mathbf{H} = (h_{ij})_{r \times n}$ be a parity check matrix for linear code $\mathcal{C}$ then we define Tanner graph of $\mathcal{C}$ as:

Tanner graph constructions for codes

Let $\mathbf{H} = (h_{ij})_{r \times n}$ be a parity check matrix for linear code $\mathcal{C}$ then we define Tanner graph of $\mathcal{C}$ as:



Cycle free Tanner graphs

Theorem (Etzion'99)

Let $\mathcal{C}[n, k, d_{\min}]$ *be a cycle free linear code of rate* $\mathfrak{r} \geq 0.5$*, then* $d_{\min} \leq 2$*. If* $\mathfrak{r} \geq 0.5$*, then*

$$d_{\min} \leq \left\lfloor \frac{n}{k+1} \right\rfloor + \left\lfloor \frac{n+1}{k+1} \right\rfloor < \frac{2}{\mathfrak{r}}.$$

Tanner graph for lattices

In the coordinate system $\mathcal{S} = \{\mathbf{W}_i\}_{i=1}^{n}$, a lattice Λ can be decomposed as

$$\Lambda = \mathbb{Z}^n \mathbf{C}(\Lambda) + \mathcal{L}\mathbf{P}(\Lambda) \qquad (1)$$

where $\mathcal{L} \subseteq \mathbb{Z}_{g_1} \times \mathbb{Z}_{g_2} \times \cdots \times \mathbb{Z}_{g_n}$ is the label code of Λ and

$$\mathbf{C}(\Lambda) = \text{diag}(\det(\Lambda_{\mathbf{W}_1}), \ldots, \det(\Lambda_{\mathbf{W}_n})),$$

$$\mathbf{P}(\Lambda) = \text{diag}(\det(P_{\mathbf{W}_1}(\Lambda)), \ldots, \det(P_{\mathbf{W}_n}(\Lambda))).$$

Tanner graph for lattices

In the coordinate system $\mathcal{S} = \{\mathbf{W}_i\}_{i=1}^{n}$, a lattice Λ can be decomposed as

$$\Lambda = \mathbb{Z}^n \mathbf{C}(\Lambda) + \mathcal{L}\mathbf{P}(\Lambda) \tag{1}$$

where $\mathcal{L} \subseteq \mathbb{Z}_{g_1} \times \mathbb{Z}_{g_2} \times \cdots \times \mathbb{Z}_{g_n}$ is the label code of Λ and

$$\mathbf{C}(\Lambda) = \text{diag}(\det(\Lambda_{\mathbf{W}_1}), \ldots, \det(\Lambda_{\mathbf{W}_n})),$$

$$\mathbf{P}(\Lambda) = \text{diag}(\det(P_{\mathbf{W}_1}(\Lambda)), \ldots, \det(P_{\mathbf{W}_n}(\Lambda))).$$

Tanner graph of a lattice Λ is the Tanner graph of its corresponding label code $\mathcal{L}$.

Cycle-free lattices

Theorem (Sakzad'11)

Let Λ be an n-dimensional cycle-free lattice whose label code has rate greater than 0.5. Then for a large even number n, the coding gain of Λ is $\gamma(\Lambda) \leq \frac{2n}{\pi}$.

Backgrounds

- Construction A: Let $\mathcal{C} \subseteq \mathbb{F}_2^n$ be a linear code. Define Λ as a lattice derived from $\mathcal{C}$ by:

$$\Lambda = 2\mathbb{Z}^n + \mathcal{C}.$$

Backgrounds

- Construction A: Let $\mathcal{C} \subseteq \mathbb{F}_2^n$ be a linear code. Define Λ as a lattice derived from $\mathcal{C}$ by:

$$\Lambda = 2\mathbb{Z}^n + \mathcal{C}.$$

- Construction D: Let $\mathcal{C}_0 \supseteq \mathcal{C}_1 \supseteq \cdots \supseteq \mathcal{C}_a$ be a family of $a+1$ linear codes where $\mathcal{C}_\ell[n, k_\ell, d_{\min}^\ell]$ for $1 \leq \ell \leq a$ and $\mathcal{C}_0[n, n, 1]$ trivial code $\mathbb{F}_2^n$. Define $\Lambda \subseteq \mathbb{R}^n$ as all vectors of the form

$$\mathbf{z} + \sum_{\ell=1}^{a} \sum_{j=1}^{k_\ell} \beta_j^{(\ell)} \frac{\mathbf{c}_j}{2^{\ell-1}},$$

where $\mathbf{z} \in 2\mathbb{Z}^n$ and $\beta_j^{(\ell)} = 0$ or 1.

Minimum distance and coding gain

Theorem (Barnes)

Let Λ be a lattice constructed based on Construction D. Then we have

$$d_{\min}(\Lambda) = \min_{1 \leq \ell \leq a} \left\{ 2, \frac{\sqrt{d_{\min}^{\ell}}}{2^{\ell-1}} \right\}$$

where $d_{\min}^{\ell}$ is the minimum distance of C_ℓ for $1 \leq \ell \leq a$. Its coding gain satisfies

$$\gamma(\Lambda) \geq 4^{\sum_{\ell=1}^{a} \frac{k_\ell}{n}}.$$

Kissing Number

Theorem (Sakzad'12)

Let Λ be a lattice constructed based on Construction D. Then for the kissing number of Λ we have:

$$\tau(\Lambda) \leq 2n + \sum_{\substack{1 \leq \ell \leq a \\ d^{\ell}_{\min} = 4^{\ell}}} 2^{d^{\ell}_{\min}} A_{d^{\ell}_{\min}}$$

where $A_{d^{\ell}_{\min}}$ denotes the number of codewords in $\mathcal{C}_{\ell}$ with minimum weight $d^{\ell}_{\min}$.

Construction D'

- Let $\mathcal{C}_0 \supseteq \mathcal{C}_1 \supseteq \cdots \supseteq \mathcal{C}_a$ be a set of nested linear block codes, where $\mathcal{C}_\ell \left[n, k_\ell, d_{\min}^{\ell}\right]$, for $1 \leq \ell \leq a$.

Construction D'

- Let $\mathcal{C}_0 \supseteq \mathcal{C}_1 \supseteq \cdots \supseteq \mathcal{C}_a$ be a set of nested linear block codes, where $\mathcal{C}_\ell \left[n, k_\ell, d_{\min}^{\ell}\right]$, for $1 \leq \ell \leq a$.
- Let $\{\mathbf{h}_1, \ldots, \mathbf{h}_n\}$ be a basis for $\mathbb{F}_2^n$, where the code $\mathcal{C}_\ell$ is formed by the $r_\ell = n - k_\ell$ parity check vectors $\mathbf{h_1}, \ldots, \mathbf{h}_{r_\ell}$.

Construction D'

- Let $\mathcal{C}_0 \supseteq \mathcal{C}_1 \supseteq \cdots \supseteq \mathcal{C}_a$ be a set of nested linear block codes, where $\mathcal{C}_\ell \left[n, k_\ell, d_{\min}^\ell\right]$, for $1 \leq \ell \leq a$.
- Let $\{\mathbf{h}_1, \ldots, \mathbf{h}_n\}$ be a basis for $\mathbb{F}_2^n$, where the code $\mathcal{C}_\ell$ is formed by the $r_\ell = n - k_\ell$ parity check vectors $\mathbf{h_1}, \ldots, \mathbf{h}_{r_\ell}$.
- Consider vectors $\mathbf{h}_i$, for $1 \leq i \leq n$, as real vectors with elements 0 or 1 in $\mathbb{R}^n$.

Construction D'

- Let $\mathcal{C}_0 \supseteq \mathcal{C}_1 \supseteq \cdots \supseteq \mathcal{C}_a$ be a set of nested linear block codes, where $\mathcal{C}_\ell \left[n, k_\ell, d_{\min}^\ell\right]$, for $1 \leq \ell \leq a$.
- Let $\{\mathbf{h}_1, \ldots, \mathbf{h}_n\}$ be a basis for $\mathbb{F}_2^n$, where the code $\mathcal{C}_\ell$ is formed by the $r_\ell = n - k_\ell$ parity check vectors $\mathbf{h_1}, \ldots, \mathbf{h}_{r_\ell}$.
- Consider vectors $\mathbf{h}_i$, for $1 \leq i \leq n$, as real vectors with elements 0 or 1 in $\mathbb{R}^n$.
- Let

$$\mathbf{H} = [\mathbf{h}_1, \ldots, \mathbf{h}_{r_0}, 2\mathbf{h}_{r_0+1}, \ldots, 2\mathbf{h}_{r_1}, \ldots, 2^a\mathbf{h}_{r_{a-1}+1}, \ldots, 2^a\mathbf{h}_{r_a}]$$

Construction D'

- Let $\mathcal{C}_0 \supseteq \mathcal{C}_1 \supseteq \cdots \supseteq \mathcal{C}_a$ be a set of nested linear block codes, where $\mathcal{C}_\ell \left[n, k_\ell, d^\ell_{\min}\right]$, for $1 \le \ell \le a$.
- Let $\{\mathbf{h}_1, \ldots, \mathbf{h}_n\}$ be a basis for $\mathbb{F}_2^n$, where the code $\mathcal{C}_\ell$ is formed by the $r_\ell = n - k_\ell$ parity check vectors $\mathbf{h_1}, \ldots, \mathbf{h}_{r_\ell}$.
- Consider vectors $\mathbf{h}_i$, for $1 \le i \le n$, as real vectors with elements 0 or 1 in $\mathbb{R}^n$.
- Let

$$\mathbf{H} = [\mathbf{h}_1, \ldots, \mathbf{h}_{r_0}, 2\mathbf{h}_{r_0+1}, \ldots, 2\mathbf{h}_{r_1}, \ldots, 2^a\mathbf{h}_{r_{a-1}+1}, \ldots, 2^a\mathbf{h}_{r_a}]$$

- $\mathbf{x} \in \Lambda \Leftrightarrow \mathbf{H}\mathbf{x}^T \equiv \mathbf{0} \pmod{2^{a+1}}$.

Construction D'

- Let $\mathcal{C}_0 \supseteq \mathcal{C}_1 \supseteq \cdots \supseteq \mathcal{C}_a$ be a set of nested linear block codes, where $\mathcal{C}_\ell\left[n, k_\ell, d^\ell_{\min}\right]$, for $1 \leq \ell \leq a$.
- Let $\{\mathbf{h}_1, \ldots, \mathbf{h}_n\}$ be a basis for $\mathbb{F}_2^n$, where the code $\mathcal{C}_\ell$ is formed by the $r_\ell = n - k_\ell$ parity check vectors $\mathbf{h_1}, \ldots, \mathbf{h}_{r_\ell}$.
- Consider vectors $\mathbf{h}_i$, for $1 \leq i \leq n$, as real vectors with elements 0 or 1 in $\mathbb{R}^n$.
- Let

$$\mathbf{H} = [\mathbf{h}_1, \ldots, \mathbf{h}_{r_0}, 2\mathbf{h}_{r_0+1}, \ldots, 2\mathbf{h}_{r_1}, \ldots, 2^a\mathbf{h}_{r_{a-1}+1}, \ldots, 2^a\mathbf{h}_{r_a}]$$

- $\mathbf{x} \in \Lambda \Leftrightarrow \mathbf{H}\mathbf{x}^T \equiv \mathbf{0} \pmod{2^{a+1}}$.
- The number $a+1$ is called the *level* of the construction.

Properties

It can be shown that the volume of an $(a+1)$-level lattice Λ constructed using Construction D' is

$$\det(\Lambda) = 2^{\left(\sum_{\ell=0}^{a} r_\ell\right)}.$$

Properties

It can be shown that the volume of an $(a+1)$-level lattice Λ constructed using Construction D' is

$$\det(\Lambda) = 2^{\left(\sum_{\ell=0}^{a} r_\ell\right)}.$$

Also the minimum distance of Λ satisfies the following bounds

$$\min_{0 \leq \ell \leq a} \left\{ 4^{\ell} d_{\min}^{a-\ell} \right\} \leq d_{\min}^2(\Lambda) \leq 4^{a+1}.$$

LDA lattices [Botrous'13]

- A lattice Λ constructed based on Construction A is called an LDA lattice if the underlying code $\mathcal{C}$ be a "non-binary" low density parity check code.

LDA lattices [Botrous'13]

- A lattice Λ constructed based on Construction A is called an LDA lattice if the underlying code $\mathcal{C}$ be a "non-binary" low density parity check code.
- If the code is "binary", this will be an LDPC lattice with only one level.

LDPC lattices [Sadeghi'06]

- A lattice Λ constructed based on Construction D' is called an low density parity check lattice (LDPC lattice) if the matrix $\mathbf{H}$ is a sparse matrix.

LDPC lattices [Sadeghi'06]

- A lattice Λ constructed based on Construction D' is called an low density parity check lattice (LDPC lattice) if the matrix $\mathbf{H}$ is a sparse matrix.
- It is trivial that if the underlying nested codes $\mathcal{C}_\ell$ are LDPC codes then the corresponding lattice is an LDPC lattice and vice versa.

LDPC lattices [Sadeghi'06]

- A lattice Λ constructed based on Construction D' is called an low density parity check lattice (LDPC lattice) if the matrix $\mathbf{H}$ is a sparse matrix.
- It is trivial that if the underlying nested codes $\mathcal{C}_\ell$ are LDPC codes then the corresponding lattice is an LDPC lattice and vice versa.
- An Extended Edge-Progressive Graph algorithm is introduced to construct LDPC lattices with high girth efficiently.

LDPC lattices [Sadeghi'06]

- A lattice Λ constructed based on Construction D' is called an low density parity check lattice (LDPC lattice) if the matrix $\mathbf{H}$ is a sparse matrix.
- It is trivial that if the underlying nested codes $\mathcal{C}_\ell$ are LDPC codes then the corresponding lattice is an LDPC lattice and vice versa.
- An Extended Edge-Progressive Graph algorithm is introduced to construct LDPC lattices with high girth efficiently.
- A generalized Min-Sum algorithm has been proposed to decode these lattices based on their Tanner graph representation. 'Vectors' are messages.

LDLC lattices [Sommer'08]

- An n-dimensional low density lattice code (LDLC) is generated with a nonsingular lattice generator matrix $\mathbf{G}$ satisfying $\det(\mathbf{G}) = 1$, for which the parity check matrix $\mathbf{H} = \mathbf{G}^{-1}$ is sparse.

LDLC lattices [Sommer'08]

- An n-dimensional low density lattice code (LDLC) is generated with a nonsingular lattice generator matrix $\mathbf{G}$ satisfying $\det(\mathbf{G}) = 1$, for which the parity check matrix $\mathbf{H} = \mathbf{G}^{-1}$ is sparse.
- An n-dimensional regular LDLC with degree d is called Latin square LDLC if every row and column of the parity check matrix $\mathbf{H}$ has the same d nonzero values, except for a possible change of order and random signs.

LDLC lattices [Sommer'08]

- An n-dimensional low density lattice code (LDLC) is generated with a nonsingular lattice generator matrix $\mathbf{G}$ satisfying $\det(\mathbf{G}) = 1$, for which the parity check matrix $\mathbf{H} = \mathbf{G}^{-1}$ is sparse.
- An n-dimensional regular LDLC with degree d is called Latin square LDLC if every row and column of the parity check matrix $\mathbf{H}$ has the same d nonzero values, except for a possible change of order and random signs.
- A generalized Sum-Product algorithm is provided to decode these lattices based on their Tanner graph representation. 'Probability Density Functions' are messages.

Turbo Lattices [Sakzad'10]

- Using Construction D along with a set of nested turbo codes, we define turbo lattices.

Turbo Lattices [Sakzad'10]

- Using Construction D along with a set of nested turbo codes, we define turbo lattices.
- Nested interleavers and turbo codes were first constructed to be used in these lattices.

Turbo Lattices [Sakzad'10]

- Using Construction D along with a set of nested turbo codes, we define turbo lattices.
- Nested interleavers and turbo codes were first constructed to be used in these lattices.
- An Iterative turbo decoding algorithm is established for decoding purposes.

Numerical experiments

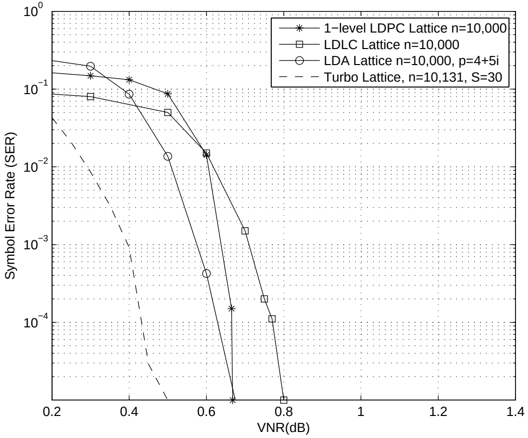


Figure: Comparison graph for various well-known lattices.

Definition

Let $\mathcal{D}$ be a convex, measurable, nonempty subset of $\mathbb{R}^n$. Then lattice code $\mathcal{C}(\Lambda, \mathcal{D})$ is defined by

$$\Lambda \cap \mathcal{D},$$

and $\mathcal{D}$ is called the support(shaping) region of the code.

Definition

Let $\mathcal{D}$ be a convex, measurable, nonempty subset of $\mathbb{R}^n$. Then lattice code $\mathcal{C}(\Lambda, \mathcal{D})$ is defined by

$$\Lambda \cap \mathcal{D},$$

and $\mathcal{D}$ is called the support(shaping) region of the code.

Definition

Let $\mathcal{C}(\Lambda, \mathcal{D}) = \{\mathbf{c}_1, \ldots, \mathbf{c}_M\}$, then the average power ρ is

$$\rho = \frac{1}{n} \sum_{i=1}^{M} \frac{\|\mathbf{c}_i\|^2}{M}.$$

Two fundamental operations

- Bit labeling: A map that sends bits to signal points. Huge look-up table.
- Shaping Constellation: How much do we gain by using a specific shaping? Sphere/Cubic/Voronoi?

Shaping Gain

Definition

The quantity

$$\gamma_s(\mathcal{D}) = \frac{1}{12G(\mathcal{D})}$$

is known as the shaping gain of the support region $\mathcal{D}$.

Shaping Gain

Definition

The quantity

$$\gamma_s(\mathcal{D}) = \frac{1}{12G(\mathcal{D})}$$

is known as the shaping gain of the support region $\mathcal{D}$*.*

It is well known that the highest possible shaping gain is obtained when $\mathcal{D}$ is a sphere, in which case:

$$\gamma_s(\mathcal{D}) = \frac{\pi(n+2)}{12\Gamma(\frac{n}{2}+1)^{\frac{2}{n}}}.$$

Different Techniques

- Cubic Shaping,
- Voronoi Shaping.

Lower Bound on Probability of Error

Theorem (Tarokh'99)

If an n-dimensional lattice code $\mathcal{C}(\Lambda, \mathcal{D}) = \{\mathbf{c}_1, \ldots, \mathbf{c}_M\}$ with $n = 2k$ is used to transmit information over an AWGN channel, then

$$P_e(\Lambda, \sigma^2) \geq G_k(z),$$

where

$$z = \frac{6\Gamma(\frac{n}{2}+1)^{\frac{2}{n}}}{\pi}\gamma_s(\mathcal{D})\mathit{SNR}_{norm}$$

and

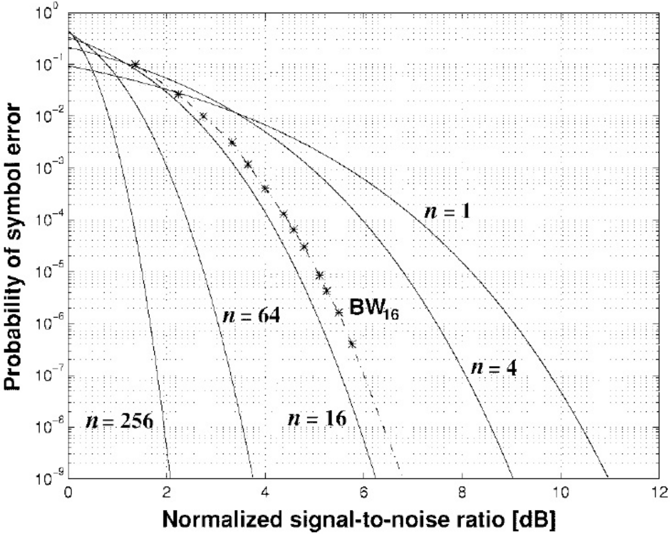
$$\mathit{SNR}_{norm} = \frac{\rho}{\left(2^{2\mathfrak{r}}-1\right)\sigma^2}.$$

Upper Bound on Coding Gain

Theorem

Let $\mathcal{C}(\Lambda, \mathcal{D})$ be a high rate n-dimensional lattice code with a spherical support region $\mathcal{D}$, and let $n = 2k$. Then the coding gain of $\mathcal{C}(\Lambda, \mathcal{D})$ is upper bounded by:

$$\gamma(\mathcal{C}) \leq \frac{\zeta(k; P_e)^2}{\xi(k; P_e)} . \frac{4\Gamma(k+1)^{\frac{1}{k}}}{\pi} .$$


Probability of symbol error
Normalized signal-to-noise ratio [dB]
n = 1
n = 4
n = 16
n = 64
n = 256
BW16
10^0
10^-1
10^-2
10^-3
10^-4
10^-5
10^-6
10^-7
10^-8
10^-9
0
2
4
6
8
10
12

Thanks for your attention! Wed. 23rd Oct., same time, Building 72, Room 132.