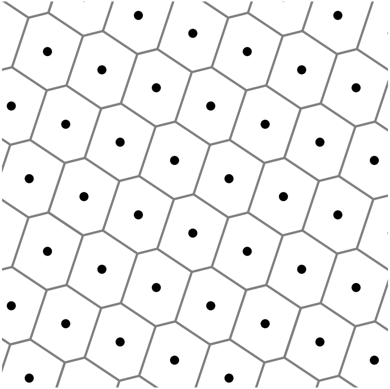
A Simple Proof for the Existence of "Good" Pairs of Nested Lattices

Or Ordentlich
Joint work with Uri Erez

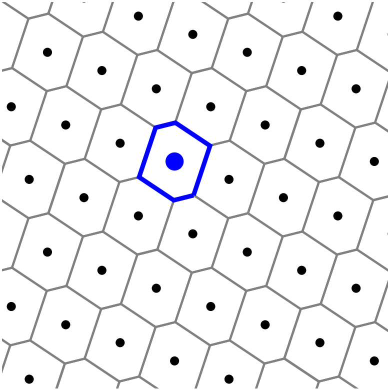
November 15th, IEEEI 2012
Eilat, Israel

What are lattices?



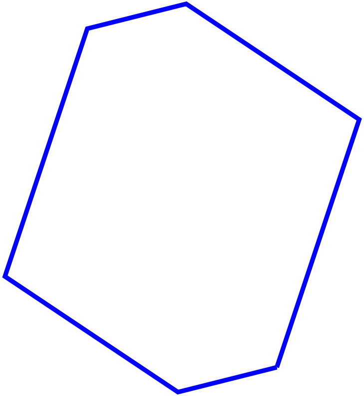
- A lattice Λ is a discrete subgroup of $\mathbb{R}^n$ closed under addition and reflection.

Lattice definitions



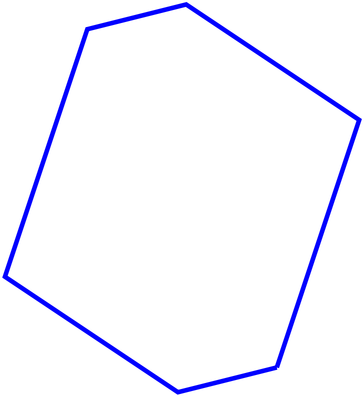
- The Voronoi region $\mathcal{V}$ of a lattice point is the set of all points in $\mathbb{R}^n$ which are closest to it.

Lattice definitions



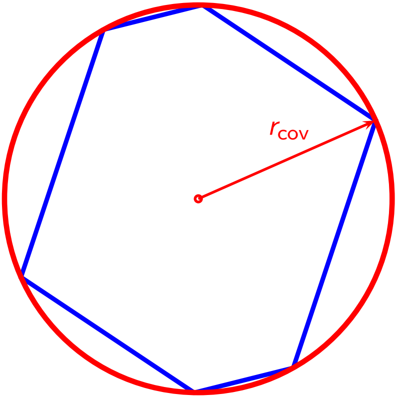
- The Voronoi region $\mathcal{V}$ of a lattice point is the set of all points in $\mathbb{R}^n$ which are closest to it.

Lattice definitions



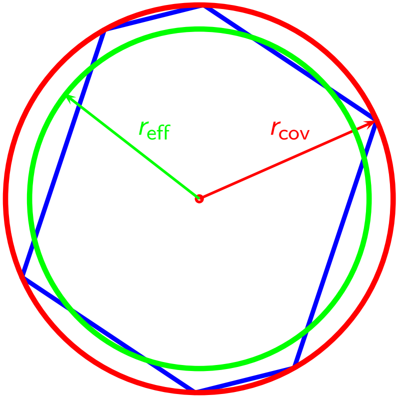
- A sequence of lattices is good for AWGN coding if the probability that an AWGN (with appropriate variance) is not contained in $\mathcal{V}$ vanishes with the dimension.

Lattice definitions



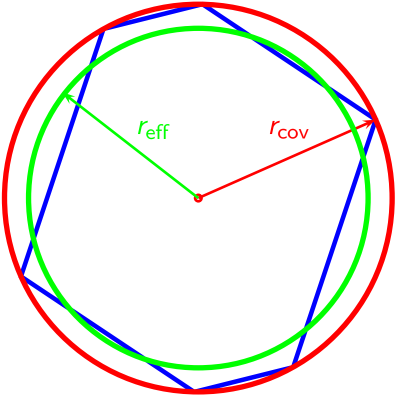
- The covering radius is the radius of the smallest ball that contains the Voronoi region $\mathcal{V}$.

Lattice definitions



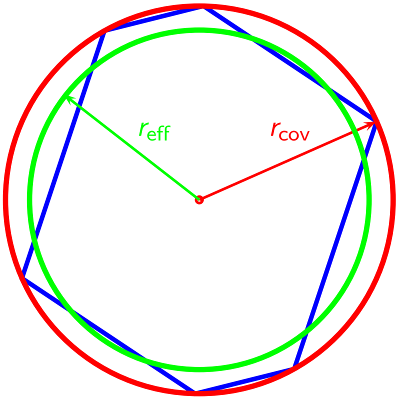
- The effective radius is the radius of a ball with the same volume as the Voronoi region $\mathcal{V}$.

Lattice definitions



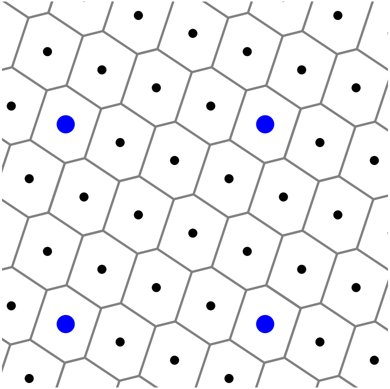
- A sequence of lattices is good for covering ("Rogers-good") if $\frac{r_{\text{eff}}}{r_{\text{cov}}} \to 1$ as the lattice dimension grows.

Lattice definitions



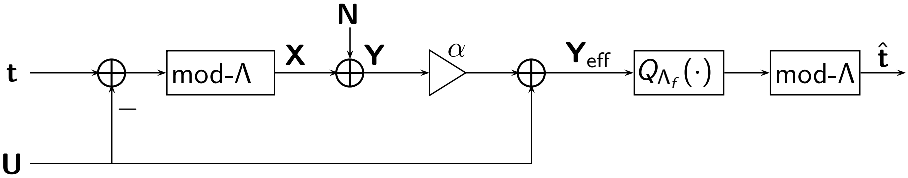
- A sequence of lattices is good for MSE quantization if for a random dither $\mathbf{U}$ uniformly distributed over $\mathcal{V}$ we have $\mathbb{E}\|\mathbf{U}\|^2 \to r_{\text{eff}}^2$ as the lattice dimension grows.

Lattice definitions



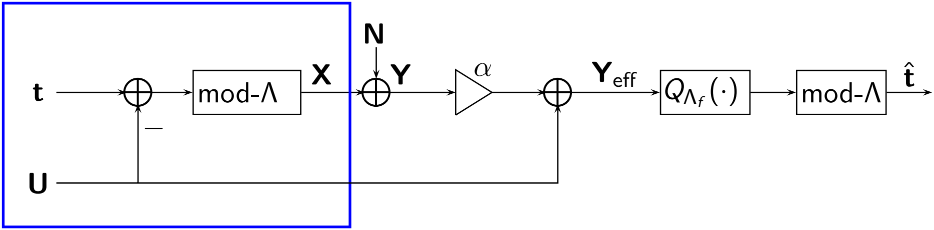
- A lattice Λ_c is nested in Λ if $\Lambda_c \subset \Lambda$.

The mod-Λ transmission scheme [Erez-Zamir IT04]



- The scheme uses a pair of nested lattice $\Lambda \subset \Lambda_f$ and a dither $\mathbf{U}$.

The mod-Λ transmission scheme [Erez-Zamir IT04]



Tx:

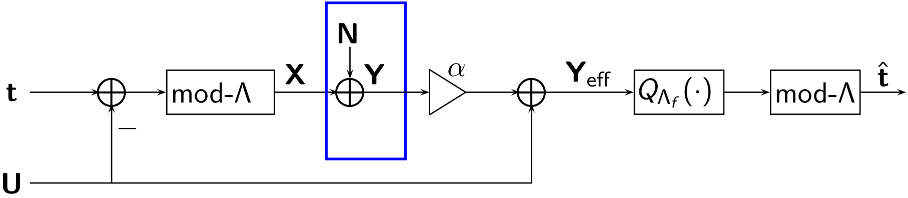
- The transmitted signal is

$$\mathbf{X} = [\mathbf{t} - \mathbf{U}] \bmod \Lambda$$

- $\mathbf{X}$ is uniformly distributed over the Voronoi region of Λ.
- The average transmission power is the second moment of Λ.

Λ needs to be good for MSE quantization

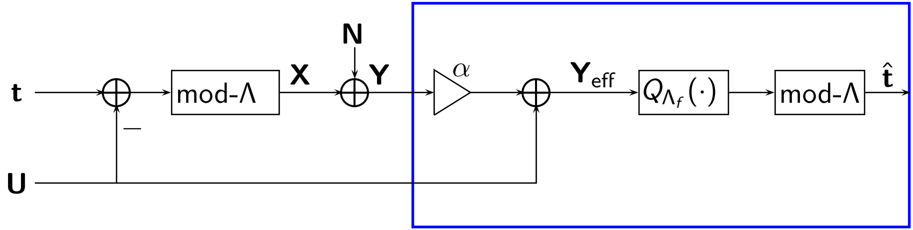
The mod-Λ transmission scheme [Erez-Zamir IT04]



AWGN Channel:

$$\mathbf{Y} = \mathbf{X} + \mathbf{N}$$

The mod-Λ transmission scheme [Erez-Zamir IT04]



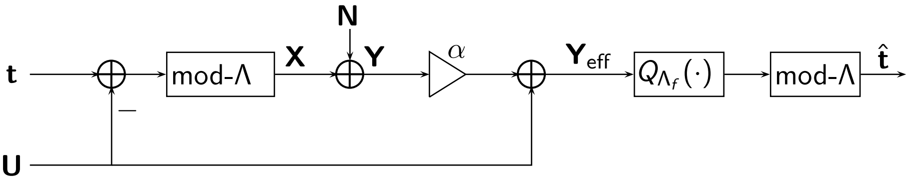
Rx:

$$
\begin{aligned}
\mathbf{Y}_{\text{eff}} &= \alpha\mathbf{Y} + \mathbf{U} \\
&= \mathbf{X} + \mathbf{U} + (\alpha - 1)\mathbf{X} + \alpha\mathbf{N} \\
&= \mathbf{t} - \mathbf{U} + \boldsymbol{\lambda} + \mathbf{U} + (\alpha - 1)\mathbf{X} + \alpha\mathbf{N} \\
&= \mathbf{t} + \boldsymbol{\lambda} + \mathbf{Z}_{\text{eff}},
\end{aligned}
$$

where $\boldsymbol{\lambda} \in \Lambda$ and $\mathbf{Z}_{\text{eff}} = (\alpha - 1)\mathbf{X} + \alpha\mathbf{N}$.

Decoding is correct if $\mathbf{Z}_{\text{eff}} \in \mathcal{V}_f$

The mod-Λ transmission scheme [Erez-Zamir IT04]

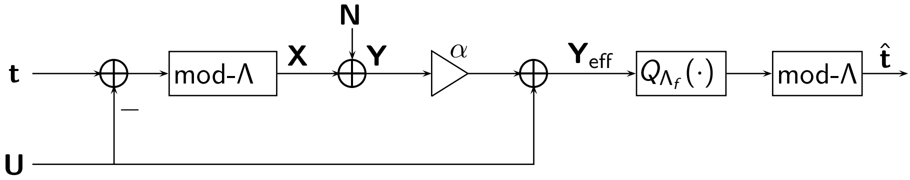


To approach capacity with nearest neighbor decoding we need:

- The coarse lattice Λ to be good for MSE quantization.
- The fine lattice Λ_f to be good for coding (with NN decoding) in the presence of effective noise $\mathbf{Z}_{\text{eff}} = (\alpha - 1)\mathbf{X} + \alpha\mathbf{N}$.

Note that $\mathbf{Z}_{\text{eff}}$ depends on the coarse lattice.

The mod-Λ transmission scheme [Erez-Zamir IT04]



To be more formal, we want:

- $\frac{1}{n}\mathbb{E}\|\mathbf{U}\|^2 \to \frac{1}{2\pi e}\mathrm{Vol}(\Lambda)^{2/n}$ (or alternatively $G(\Lambda) \to \frac{1}{2\pi e}$).
- If $V(\Lambda_f)^{\frac{2}{n}} > 2\pi e \frac{1}{n}\mathbb{E}\|\mathbf{Z}_{\text{eff}}\|^2$,

$$\Pr\left(\left[Q_{\Lambda_f}(\mathbf{t}+\mathbf{Z}_{\text{eff}})\right] \bmod \Lambda \neq \mathbf{t} \bmod \Lambda\right) \to 0.$$

If the two conditions are satisfied the scheme achieves any rate below

$$R = \frac{1}{n}\log\left(\frac{\mathrm{Vol}(\Lambda)}{\mathrm{Vol}(\Lambda_f)}\right) = \frac{1}{2}\log\left(\frac{\mathrm{SNR}}{1/n\mathbb{E}\|\mathbf{Z}_{\text{eff}}\|^2}\right)$$

How to construct “good” pairs of nested lattices?

	Binary linear code	Lattice
Single		
Nested		

How to construct "good" pairs of nested lattices?

	Binary linear code	Lattice
Single	Draw $G \in \mathbb{Z}_2^{K \times N}$ with entries i.i.d. and uniform over $\mathbb{Z}_2$	
Nested		

How to construct "good" pairs of nested lattices?

	Binary linear code	Lattice
Single	Draw $G \in \mathbb{Z}_2^{K \times N}$ with entries i.i.d. and uniform over $\mathbb{Z}_2$	Draw $G \in \mathbb{Z}_p^{K \times N}$ with entries i.i.d. and uniform over $\mathbb{Z}_p$. Construct a linear code $\mathcal{C}$ with this generating matrix. Set $$\Lambda = p^{-1}\mathcal{C} + \mathbb{Z}^n$$
Nested		

How to construct "good" pairs of nested lattices?

	Binary linear code	Lattice
Single	Draw $G \in \mathbb{Z}_2^{K \times N}$ with entries i.i.d. and uniform over $\mathbb{Z}_2$	Draw $G \in \mathbb{Z}_p^{K \times N}$ with entries i.i.d. and uniform over $\mathbb{Z}_p$. Construct a linear code $\mathcal{C}$ with this generating matrix. Set $$\Lambda = p^{-1}\mathcal{C} + \mathbb{Z}^n$$
Nested	Draw $G_f = \begin{bmatrix} \mathbf{G} \\ --- \\ \mathbf{G}' \end{bmatrix}$ with entries i.i.d. and uniform over $\mathbb{Z}_2$. G generates the coarse code and G_f the fine code	

How to construct "good" pairs of nested lattices?

	Binary linear code	Lattice
Single	Draw $G \in \mathbb{Z}_2^{K\times N}$ with entries i.i.d. and uniform over $\mathbb{Z}_2$	Draw $G \in \mathbb{Z}_p^{K\times N}$ with entries i.i.d. and uniform over $\mathbb{Z}_p$. Construct a linear code $\mathcal{C}$ with this generating matrix. Set $$\Lambda = p^{-1}\mathcal{C} + \mathbb{Z}^n$$
Nested	Draw $G_f = \begin{bmatrix} \mathbf{G} \\ --- \\ \mathbf{G}' \end{bmatrix}$ with entries i.i.d. and uniform over $\mathbb{Z}_2$. G generates the coarse code and G_f the fine code	?

How to construct "good" pairs of nested lattices?

Previous works

- Find a lattice Λ which is good for covering, and has a generating matrix F.
- Draw $G \in \mathbb{Z}_p^{K \times N}$ with entries i.i.d. and uniform over $\mathbb{Z}_p$. Construct a linear code $\mathcal{C}$ with this generating matrix.
- Set $\Lambda_f = F \cdot \left(p^{-1}\mathcal{C} + \mathbb{Z}^n\right) = p^{-1}F\mathcal{C} + F\mathbb{Z}^n$.

This work

- Draw $G_f = \begin{bmatrix} \mathbf{G} \\ - - - \\ \mathbf{G}' \end{bmatrix} \in \mathbb{Z}_p$ with entries i.i.d. and uniform over $\mathbb{Z}_p$.
- Construct a linear code $\mathcal{C}$ from the generating matrix G, and a linear code $\mathcal{C}_f$ from the generating matrix G_f.
- Set $\Lambda = p^{-1}\mathcal{C} + \mathbb{Z}^n, \quad \Lambda_f = p^{-1}\mathcal{C}_f + \mathbb{Z}^n$.

Differences from previous work

Current approach vs. previous work

- A simpler ensemble to analyze.
- A basic proof that makes no use of previous results from geometry of numbers.
- The coarse lattice only has to be good for MSE quantization (not necessarily for covering).

Differences from previous work

Current approach vs. previous work

- A simpler ensemble to analyze.
- A basic proof that makes no use of previous results from geometry of numbers.
- The coarse lattice only has to be good for MSE quantization (not necessarily for covering).

Historical note:

- When Erez and Zamir's work was published it was known that good covering lattices exist, but it was not known that Construction A lattices are usually good for covering.
  $\Longrightarrow$ The two-step construction was needed.
- Erez and Zamir studied the error exponents the mod-Λ scheme achieves. For that purpose it is important that the coarse lattice will be good for covering. For capacity, goodness for quantization suffices.

Proof outline

- We show that w.h.p. the coarse lattice Λ is good for MSE quantization.
- We show that w.h.p. the fine lattice Λ_f is good for coding in the presence of noise that rarely leaves a ball.

$\Longrightarrow$ Most members of the ensemble are "good" pairs of nested lattices.

- We show that for a coarse lattice Λ which is good for MSE quantization the effective noise

$$\mathbf{Z}_{\text{eff}} = (\alpha - 1)\mathbf{X} + \alpha\mathbf{N}$$

rarely leaves a ball.

Proof outline - Goodness for MSE quantization

- Our ensemble induces a distribution on the lattice points that is "almost" i.i.d. and "uniform" on $\mathbb{R}^n$ with point density $1/(V_n r_{\text{eff}}^n)$.
- For any $\mathbf{x} \in \mathbb{R}^n$: $\left|\Lambda \cap \mathcal{B}(\mathbf{x}, \sqrt{nD})\right| \sim \left(\frac{\sqrt{nD}}{r_{\text{eff}}}\right)^n$.

  $\Longrightarrow$ For $\sqrt{nD} > r_{\text{eff}}$ almost surely $\left|\Lambda \cap \mathcal{B}(\mathbf{x}, \sqrt{nD})\right| > 1$.

  $\Longrightarrow$ If $\sqrt{nD} > r_{\text{eff}}$, almost surely a point $\mathbf{x} \in \mathbb{R}^n$ is covered by a lattice point with distance $< \sqrt{nD}$.
- Since Λ is nested within the cubic lattice, the covering radius is bounded.

  $\Longrightarrow$ For $\sqrt{nD} > r_{\text{eff}}$ the average MSE distortion Λ achieves is smaller than nD.
- Setting r_{eff} slightly smaller than $\sqrt{nD}$, a dither $\mathbf{U}$ uniformly distributed over $\mathcal{V}$ satisfies

$$\frac{1}{n}\mathbb{E}\|\mathbf{U}\|^2 \leq D \approx \frac{r_{\text{eff}}^2}{n} = \frac{1}{nV_n^{2/n}} V(\Lambda)^{2/n} \approx \frac{V(\Lambda)^{2/n}}{2\pi e}$$

Proof outline - effective noise rarely leaves a ball

Lemma:

Let $\mathbf{U}$ be a dither from a lattice Λ which is good for MSE quantization and has effective radius r_{eff}. Then, for any $\epsilon > 0$ and n large enough

$$\Pr\left(\mathbf{U} \notin \mathcal{B}(\mathbf{0}, (1+\epsilon)r_{\text{eff}})\right) < \epsilon$$

- The pdf of a random vector uniform over a ball is upper bounded by that of an AWGN. [Erez-Zamir 04]
- Combining with our lemma, w.p. $1-\epsilon$ we have that $\mathbf{U}$ is approximately Gaussian .

With probability $1-\epsilon$ the effective noise $\mathbf{Z}_{\text{eff}} = (1-\alpha)\mathbf{U} + \alpha\mathbf{N}$ is Gaussian.
$\Longrightarrow$ It suffices that the fine lattice will be good for AWGN channels.

Showing that Construction A lattices are good for AWGN channels is straightforward.

Corollaries and extensions

Chains of nested lattices

A similar construction results in a chain of nested lattice codes which are all good for MSE quantization and AWGN coding.

Cubic shaping lattice

If the coarse lattice is cubic (no shaping) and the fine lattice is good for AWGN coding, the mod-Λ scheme can achieve any rate satisfying

$$R < \frac{1}{2}\log(1 + \mathsf{SNR}) - \frac{1}{2}\log\left(\frac{2\pi e}{12}\right).$$

Additive non-Gaussian noise

For any additive i.i.d. noise channel the mod-Λ scheme can achieve any rate satisfying $R < \frac{1}{2}\log(1 + \mathsf{SNR})$ with nearest-neighbor decoding (followed by mod-Λ).

This is reminiscent of Lapidoth 96.