Leech Constellations of Construction-A Lattices

Joseph J. Boutros
Talk at Nokia Bell Labs, Stuttgart

Texas A&M University at Qatar
In collaboration with Nicola di Pietro.

March 7, 2017
Many Thanks to Dr Laurent Schmalen and his group for this invitation.
Shaping in Coded Modulations (Gaussian Channel)

- Shaping is necessary to achieve capacity.
  - Probabilistic shaping:
    Assign Gaussian-like prior distribution to constellation points.
    Kschischang-Pasupathy 1993, Böcherer-Steiner-Schulte 2015
  - Geometric shaping in lattices:
    Design a spherical-like constellation for covering goodness.
  - A mixture of probabilistic and geometric shaping:
    Boutros-Jardel-Méasson 2017
Shaping is necessary to achieve capacity.

- **Probabilistic shaping:**
  Assign Gaussian-like prior distribution to constellation points.
  - Kschischang-Pasupathy 1993, Böcherer-Steiner-Schulte 2015

- **Geometric shaping in lattices:**
  Design a spherical-like constellation for covering goodness.

- **A mixture of probabilistic and geometric shaping:**
  - Boutros-Jardel-Méasson 2017
Shaping is necessary to achieve capacity.

**Probabilistic shaping:**
Assign Gaussian-like prior distribution to constellation points.
Kschischang-Pasupathy 1993, Böcherer-Steiner-Schulte 2015

**Geometric shaping in lattices:**
Design a spherical-like constellation for covering goodness.

A mixture of probabilistic and geometric shaping:
Boutros-Jardel-Méasson 2017
Shaping in Coded Modulations (Gaussian Channel)

- Shaping is necessary to achieve capacity.

- **Probabilistic shaping:**
  Assign Gaussian-like prior distribution to constellation points.
  Kschischang-Pasupathy 1993, Böcherer-Steiner-Schulte 2015

- **Geometric shaping in lattices:**
  Design a spherical-like constellation for covering goodness.

- **A mixture of probabilistic and geometric shaping:**
  Boutros-Jardel-Méasson 2017
Outline of this talk

- Brief general introduction on lattices
- Infinite Constellations - Poltyrev Goodness
- Finite Constellations - Voronoi shaping
- Leech shaping of Construction-A lattices
- Numerical Results - Performance on a Gaussian channel
A lattice is a discrete additive subgroup of $\mathbb{R}^n$:

- There are $n$ basis vectors.
- The lattice is given by all their integer linear combinations.
- Lattices are the real Euclidean counterpart of error-correcting codes.
  - Codes are vector spaces over a finite field.
  - Lattices are modules over a real or a complex ring, e.g. $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$. 

![Diagram of a lattice]
Lattices, Sphere Packings, and Codes (2)

Integer Cubic Lattice Packing

Hexagonal Lattice Packing

(a) (b)
Integer Cubic Lattice $\mathbb{Z}^2$

Hexagonal Lattice $A_2$
Lattices, Sphere Packings, and Codes (4)

packing radius $\rho$

covering radius $R$

Voronoi cell of $A_2$
Building lattices out of codes: Construction A by Leech and Sloane 1971.

Lattices as coset codes (Forney 1988):
- The lattice $p\mathbb{Z}^n$ has $p^n$ cosets in $\mathbb{Z}^n$.
- A subset of size $p^k$ cosets is selected among the $p^n$ cosets via a code $C$.
- A coset code in Forney's terminology with the formula ($p$ is prime)

$$\Lambda = C[n, k]_p + p\mathbb{Z}^n.$$ 

The ring can be $\mathbb{Z}$ (relative integers), $\mathbb{Z}[i]$ (Gaussian integers), $\mathbb{Z}[\omega]$ (Eisenstein integers), etc. $C[n, k]_p$ should be correctly embedded in the ring.

Construction A can be thought of as
- drawing $p^k$ points representing the codewords of $C$ inside the cube $[0, p - 1]^n$
- then paving the whole space $\mathbb{R}^n$ by translating the cube by multiples of $p$ in all directions.
**Theorem (Poltyrev 1994)**

Over the unconstrained AWGN channel and for every $\varepsilon > 0$, there exists a lattice $\Lambda \subseteq \mathbb{R}^n$ (in dimension $n$ big enough) that can be decoded with error probability less than $\varepsilon$ if and only if $\text{Vol}(\Lambda) > (\sqrt{2\pi e\sigma^2})^n$.

Volume-to-noise ratio of $\Lambda$ (Forney 2000):

$$
VNR = \frac{\text{Vol}(\Lambda)^{\frac{2}{n}}}{2\pi e\sigma^2}.
$$

**Corollary (Poltyrev Goodness)**

In the set of all lattices $\Lambda$ with fixed normalized volume $\text{Vol}(\Lambda)^{\frac{2}{n}} = \nu$, there exists a lattice that can be decoded with vanishing error probability over the unconstrained AWGN channel only if the noise variance satisfies

$$
\sigma^2 < \frac{\nu}{2\pi e} = \sigma_{\text{max}}^2.
$$
Infinite Lattice Constellations

**Theorem (Poltyrev 1994)**

Over the unconstrained AWGN channel and for every $\varepsilon > 0$, there exists a lattice $\Lambda \subseteq \mathbb{R}^n$ (in dimension $n$ big enough) that can be decoded with error probability less than $\varepsilon$ if and only if $\text{Vol}(\Lambda) > (\sqrt{2\pi e\sigma^2})^n$.

Volume-to-noise ratio of $\Lambda$ (Forney 2000):

$$VNR = \frac{\text{Vol}(\Lambda)^{\frac{2}{n}}}{2\pi e\sigma^2}.$$ 

**Corollary (Poltyrev Goodness)**

In the set of all lattices $\Lambda$ with fixed normalized volume $\text{Vol}(\Lambda)^{\frac{2}{n}} = \nu$, there exists a lattice that can be decoded with vanishing error probability over the unconstrained AWGN channel only if the noise variance satisfies

$$\sigma^2 < \frac{\nu}{2\pi e} = \sigma_{\text{max}}^2.$$
Infinite Lattice Constellations

**Theorem (Poltyrev 1994)**

Over the unconstrained AWGN channel and for every \( \varepsilon > 0 \), there exists a lattice \( \Lambda \subseteq \mathbb{R}^n \) (in dimension \( n \) big enough) that can be decoded with error probability less than \( \varepsilon \) if and only if \( \text{Vol}(\Lambda) > (\sqrt{2\pi e}\sigma^2)^n \).

Volume-to-noise ratio of \( \Lambda \) (Forney 2000):

\[
\text{VNR} = \frac{\text{Vol}(\Lambda)^{\frac{2}{n}}}{2\pi e\sigma^2}.
\]

**Corollary (Poltyrev Goodness)**

In the set of all lattices \( \Lambda \) with fixed normalized volume \( \text{Vol}(\Lambda)^{\frac{2}{n}} = \nu \), there exists a lattice that can be decoded with vanishing error probability over the unconstrained AWGN channel only if the noise variance satisfies

\[
\sigma^2 < \frac{\nu}{2\pi e} = \sigma_{\text{max}}^2.
\]
Poltyrev-Good Lattices from Codes on Graphs

- Low-Density Construction A (LDA) lattices

- Generalized Low Density (GLD) lattices
Finite Lattice Constellations (1)

- AWGN channel input is \( x = (x_1, \ldots, x_n) \). Power condition:
  \[
  \mathbb{E}[x_i^2] \leq P, \quad \text{for some } P > 0,
  \]

- Signal-to-noise ratio:
  \[
  \text{SNR} = \frac{P}{\sigma^2}
  \]

- Capacity of the channel is \( \frac{1}{2} \log_2 (1 + \text{SNR}) \) bits per dimension.
Finite Lattice Constellations (2)

- An efficient way to build finite set of lattice points: Voronoi constellations (*Conway and Sloane 1983*)
- Coding lattice or fine lattice: $\Lambda_f$
- Shaping lattice or coarse lattice: $\Lambda \subseteq \Lambda_f$
- Quotient group

$$\Lambda_f/\Lambda = \{x + \Lambda : x \in \Lambda_f\}, \text{ equivalently } \Lambda_f = \Lambda_f/\Lambda + \Lambda.$$  

- Coset $x + \Lambda$, coset leader $x$.
- Order of the quotient group (number of cosets)

$$|\Lambda_f/\Lambda| = \frac{\text{Vol}(\Lambda)}{\text{Vol}(\Lambda_f)}.$$  

- The Voronoi constellation $C$ given by the coset leaders of $\Lambda$ in $\Lambda_f$ with smallest Euclidean norm (*Conway and Sloane 1983, Forney 1989*):

$$C = \Lambda_f \cap V(\Lambda).$$
**Finite Lattice Constellations (2)**

- An efficient way to build finite set of lattice points: Voronoi constellations (*Conway and Sloane 1983*)
- Coding lattice or fine lattice: $\Lambda_f$
- Shaping lattice or coarse lattice: $\Lambda \subseteq \Lambda_f$
- Quotient group

$$\Lambda_f / \Lambda = \{x + \Lambda : x \in \Lambda_f\}, \quad \text{equivalently} \quad \Lambda_f = \Lambda_f / \Lambda + \Lambda.$$

- Coset $x + \Lambda$, coset leader $x$.
- Order of the quotient group (number of cosets)

$$|\Lambda_f / \Lambda| = \frac{\text{Vol}(\Lambda)}{\text{Vol}(\Lambda_f)}.$$

- The Voronoi constellation $\mathcal{C}$ given by the coset leaders of $\Lambda$ in $\Lambda_f$ with smallest Euclidean norm (*Conway and Sloane 1983, Forney 1989*):

$$\mathcal{C} = \Lambda_f \cap \mathcal{V}(\Lambda).$$
Finite Lattice Constellations (3)

\[ \Rightarrow \quad \text{Coding lattice } \Lambda_f \]

\[ \text{Shaping lattice } \Lambda \quad \& \quad \Lambda \subseteq \Lambda_f \]

Our finite constellation
We work with a Voronoi constellation obtained from lattices \( \Lambda_f \) and \( \Lambda \): it is the set of coset leaders of smaller norm of \( \Lambda_f/\Lambda \). The coding lattice \( \Lambda_f \) can be selected in the LDA ensemble as shown in the numerical results at the end of this talk.

Illustration made in the following slides:

A Voronoi constellation of the hexagonal lattice \( A_2 \) in dimension 2.
\[ 4^2 = 16 \text{ points of the constellation } A_2/4A_2. \]
Illustration: Voronoi Constellation $A_2/4A_2 \ (1)$

The hexagonal lattice $A_2$ and its Voronoi cells.
Illustration: Voronoi Constellation $A_2/4A_2$ (2)

The lattice $A_2$, its sub-lattice $4A_2$, and their Voronoi cells.
Illustration: Voronoi Constellation $A_2/4A_2$ (3)

Select 16 points following the basis of $A_2$. 
Illustration: Voronoi Constellation $A_2/4A_2$ (3)

The constellation takes the shape of the fundamental parallelootope.
Consider the 5 points (in green) in the upper right red cell.
Illustration: Voronoi Constellation $A_2/4A_2$ (4)

The nearest point in $4A_2$ to these 5 green points is the cell center.
Illustration: Voronoi Constellation $A_2/4A_2$ (5)

Subtract the cell center $(2, 4\sqrt{3}/2)$, i.e. translate down and left.
Consider the 4 points (in green) in the right red cell.
Illustration: Voronoi Constellation $A_2/4A_2$ (7)

Translate to the left by subtracting the cell center $(4,0)$. 
Consider the point (in green) in the upper (and twice to the right) red cell.
Illustration: Voronoi Constellation $A_2/4A_2$ (8)

Translate this green point by subtracting its red cell center $(6, 4\sqrt{3}/2)$. 
Now you get the Voronoi constellation $A_2/4A_2$ with 16 points.
**Leech Constellations (1)**

- The Leech lattice $\Lambda_{24} \subset \mathbb{Z}^{24}$, an even unimodular lattice (see the SPLAG).

- Its Voronoi region has 196560 facets.

- Densest sphere packing in dimension 24 (Cohn et al., March 2016).

- Shaping again of $\Lambda_{24}$ is 1.03 dB. Gap of 0.5 dB from maximal shaping gain ($n \to \infty$).

- Let $n = 24\ell$. The shaping lattice is, for $\alpha \in \mathbb{N} \setminus \{0\}$,

  $$\Lambda = p \times \alpha \times \Lambda_{24}^{\oplus \ell}.$$  

- The fine lattice is $\Lambda_f = C[n, k]_p + p\mathbb{Z}^n$. 

Joseph Jean Boutros
Nokia Bell Labs at Stuttgart
March 7, 2017 15 / 23
Leech Constellations (1)

- The Leech lattice $\Lambda_{24} \subset \mathbb{Z}^{24}$, an even unimodular lattice (see the SPLAG).
- Its Voronoi region has 196560 facets.
- Densest sphere packing in dimension 24 (Cohn et al., March 2016).
- Shaping again of $\Lambda_{24}$ is 1.03 dB. Gap of 0.5 dB from maximal shaping gain ($n \to \infty$).
- Let $n = 24\ell$. The shaping lattice is, for $\alpha \in \mathbb{N} \setminus \{0\}$,
  \[ \Lambda = p \times \alpha \times \Lambda_{24}^{\oplus \ell}. \]
- The fine lattice is $\Lambda_f = C[n, k]_p + p\mathbb{Z}^n$. 
Leech Generator Matrix in Triangular Form
Leech Constellations (2)

Given the coding rate $R = k/n$ in the fine lattice and the volume $\text{Vol}(\Lambda_{24}) = 2^{36}$, the information rate of the Leech constellation $C$ is

$$R_C = \frac{\log_2 |\Lambda_f/\Lambda|}{n} = \frac{\log_2 \text{Vol}(\Lambda)/\text{Vol}(\Lambda_f)}{n} \text{ bits/dim}$$

$$= R \log_2 p + \log_2 \alpha + \frac{3}{2} \text{ bits/dim}.$$
**Lemma** (di Pietro and Boutros, Nov. 2016)
Let $\Gamma \subseteq \mathbb{Z}^n$ be any integer lattice and let $\Lambda = p\Gamma \subseteq p\mathbb{Z}^n$. Let us call $T$ a lower triangular generator matrix of $\Gamma$ with $t_{i,i} > 0$ for every $i$:

$$T = \begin{pmatrix}
t_{1,1} & 0 & \cdots & 0 \\
t_{2,1} & t_{2,2} & \ddots & \vdots \\
\vdots & \ddots & \ddots & 0 \\
t_{n,1} & \cdots & t_{n,n-1} & t_{n,n}
\end{pmatrix} \in \mathbb{Z}^{n \times n}.$$ 

Consider the set:

$$S = \{0, 1, \ldots, t_{1,1} - 1\} \times \{0, 1, \ldots, t_{2,2} - 1\} \times \cdots \times \{0, 1, \ldots, t_{n,n} - 1\} \subseteq \mathbb{Z}^n.$$

Let $C$ be the code that underlies the construction of $\Lambda_f = C + p\mathbb{Z}^n$; we embed it in $\mathbb{Z}^n$ via the coordinate-wise morphism $\mathbb{F}_p \hookrightarrow \{0, 1, \ldots, p-1\} \subseteq \mathbb{Z}$, hence $C \subseteq \{0, 1, \ldots, p-1\}^n$. Then $C + pS = \{c + ps \in \mathbb{Z}^n : c \in C, \ s \in S\} \subseteq \Lambda_f$ is a complete set of coset leaders of $\Lambda_f/\Lambda$. 

---

**Joseph Jean Boutros**  
**Nokia Bell Labs at Stuttgart**  
**March 7, 2017 18 / 23**
Sketch of the proof

Counting points

\[ |C + pS| = |C||S| = p^k \frac{\text{Vol}(\Lambda)}{p^n} = |\Lambda_f/\Lambda|. \]

Distinct Cosets
Take \( x = c + ps \) and \( y = d + pv \) in the same coset.
Then \( x - y = c - d + p(s - v) \in \Lambda \subseteq p\mathbb{Z}^n. \)
We get \( c = d. \) So \( x - y = p(s - v) \in \Lambda = p\Gamma. \)
It translates into \( s - v \in \Gamma, \) i.e. \( s - v = zT. \)
From the definition of \( S \) and the triangularity of \( T, \) we find \( s = v \) which proves that \( x = y. \)
Infinite constellations of LDA lattices, $p = 13$ and $R = 1/3$
Leech Constellations of LDA Lattices (2)

Leech constellations of LDA lattices, $R_C = 2.73$ bits/dim
Conclusions

- Complexity of mapping and demapping is linear in $n$.
- With a direct sum of $\Lambda_{24}$, the shaping gain is 1.03 dB.
- With a direct sum of $\Lambda_{24}$, the gap to Shannon capacity is 0.8 dB.
- Very fast universal Sphere Decoding of $\Lambda_{24}$ (Viterbo-Boutros 1999).
  Needed to quantize points of the information set defined by the encoding Lemma.
- Other specific decoders for the Leech lattice (Vardy-Be’ery 1993).
- Any dense integer lattice can be used for shaping. Density is presumed to bring a high kissing number of low-dimensional lattices (conjecture) which implies a Voronoi region with a small second-order moment.
Main Reference Paper for this Talk

Nicola di Pietro and Joseph J. Boutros,

Leech Constellations of Construction-A Lattices
arXiv:1611.04417v2

January 2017