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

Thanks

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.
  Ferdinand-Kurkoski-Nokleby-Aazhang, Kurkoski 2016, diPietro-Boutros 2016
- 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.
  Ferdinand-Kurkoski-Nokleby-Aazhang, Kurkoski 2016, diPietro-Boutros 2016
- 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.
  Ferdinand-Kurkoski-Nokleby-Aazhang, Kurkoski 2016, diPietro-Boutros 2016
- 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.
  Ferdinand-Kurkoski-Nokleby-Aazhang, Kurkoski 2016, diPietro-Boutros 2016
- A mixture of probabilistic and geometric shaping:
  Boutros-Jardel-Méasson 2017

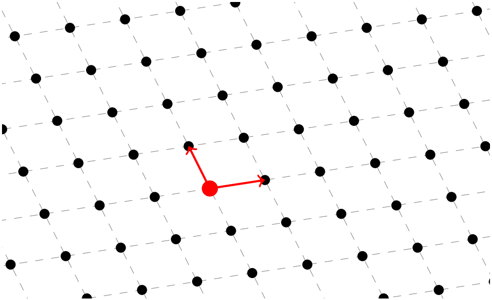
Outline of this talk

- 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

Lattices, Sphere Packings, and Codes (1)

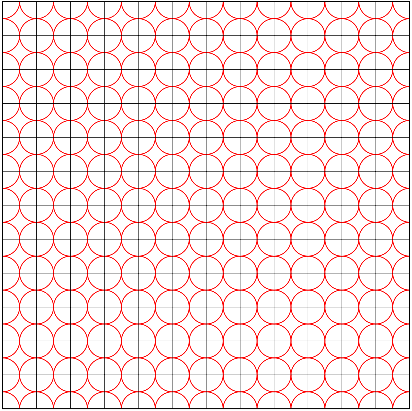
A lattice is a discrete additive subgroup of $\mathbb{R}^n$:

- 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. $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$.



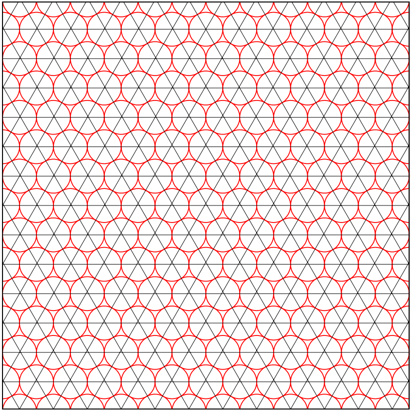
Lattices, Sphere Packings, and Codes (2)

Integer Cubic Lattice Packing



(a)

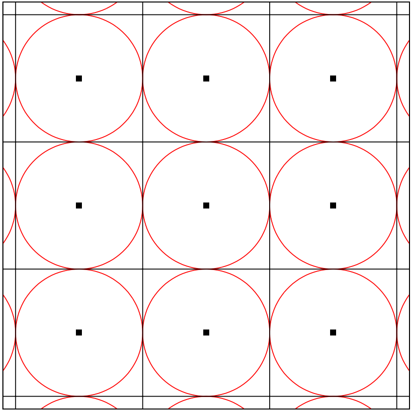
Hexagonal Lattice Packing



(b)

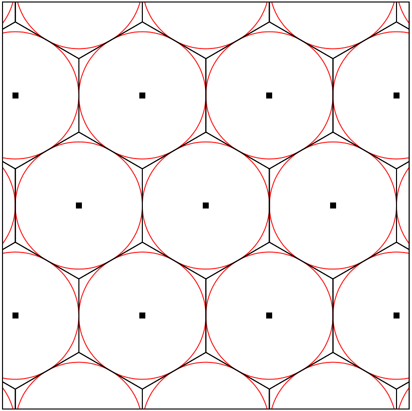
Lattices, Sphere Packings, and Codes (3)

Integer Cubic Lattice $\mathbb{Z}^2$



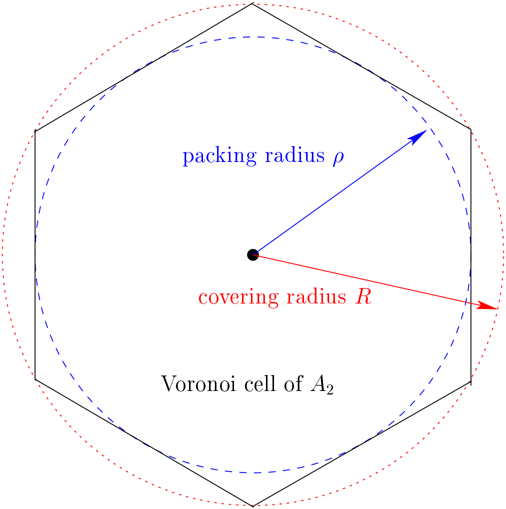
(a)

Hexagonal Lattice A_2



(b)

Lattices, Sphere Packings, and Codes (4)



Lattices, Sphere Packings, and Codes (5)

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.

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 ε if and only if $\mathrm{Vol}(\Lambda) > (\sqrt{2\pi e \sigma^2})^n$.

Volume-to-noise ratio of Λ (Forney 2000):

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

Corollary (Poltyrev Goodness)

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

$$\sigma^2 < \frac{\nu}{2\pi e} = \sigma^2_{\max}.$$

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 ε if and only if $\mathrm{Vol}(\Lambda) > (\sqrt{2\pi e \sigma^2})^n$.

Volume-to-noise ratio of Λ (Forney 2000):

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

Corollary (Poltyrev Goodness)

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

$$\sigma^2 < \frac{\nu}{2\pi e} = \sigma^2_{\max}.$$

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 ε if and only if $\mathrm{Vol}(\Lambda) > (\sqrt{2\pi e \sigma^2})^n$.

Volume-to-noise ratio of Λ (Forney 2000):

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

Corollary (Poltyrev Goodness)

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

$$\sigma^2 < \frac{\nu}{2\pi e} = \sigma^2_{\max}.$$

Poltyrev-Good Lattices from Codes on Graphs

- Low-Density Construction A (LDA) lattices
  di Pietro-Zémor-Boutros 2012-2016, Vatedka-Kashyap 2014

- Generalized Low Density (GLD) lattices
  Boutros-di Pietro-Basha-Huang 2014-2015

Finite Lattice Constellations (1)

- AWGN channel input is $\mathbf{x} = (x_1, \ldots, x_n)$. Power condition:

$$\mathbb{E}[x_i^2] \leq P, \qquad \text{for some } P > 0,$$

- Signal-to-noise ratio:

$$\mathrm{SNR} = \frac{P}{\sigma^2}$$

- Capacity of the channel is $\frac{1}{2}\log_2(1 + \mathrm{SNR})$ 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: Λ_f
- Shaping lattice or coarse lattice: $\Lambda \subseteq \Lambda_f$
- Quotient group

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

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

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

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

$$\mathcal{C} = \Lambda_f \cap \mathcal{V}(\Lambda).$$

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: Λ_f
- Shaping lattice or coarse lattice: $\Lambda \subseteq \Lambda_f$
- Quotient group

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

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

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

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

$$\mathcal{C} = \Lambda_f \cap \mathcal{V}(\Lambda).$$

Finite Lattice Constellations (3)

$\Longrightarrow$ Coding lattice Λ_f Shaping lattice Λ & $\Lambda \subseteq \Lambda_f$

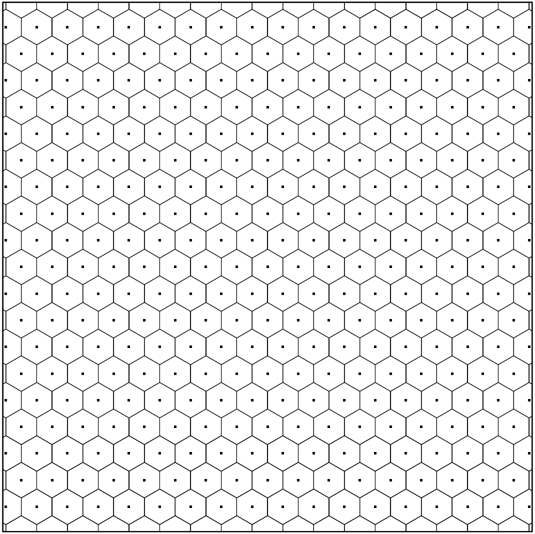
Our finite constellation

We work with a Voronoi constellation obtained from lattices Λ_f and Λ: it is the set of coset leaders of smaller norm of Λ_f/Λ. The coding lattice Λ_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:

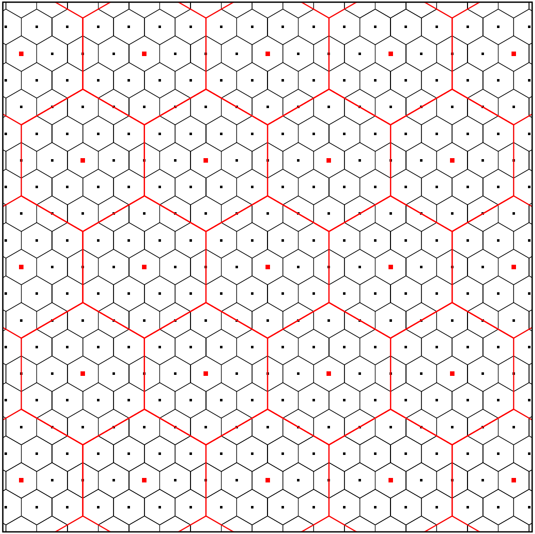
A Voronoi constellation of the hexagonal lattice A_2 in dimension 2.
$4^2 = 16$ points of the constellation $A_2/4A_2$.

Illustration: Voronoi Constellation $A_2/4A_2$ *(1)*



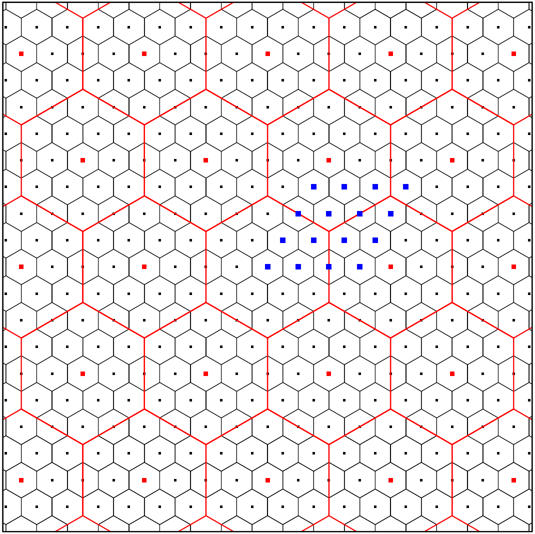
The hexagonal lattice A_2 and its Voronoi cells.

Illustration: Voronoi Constellation $A_2/4A_2$ (2)



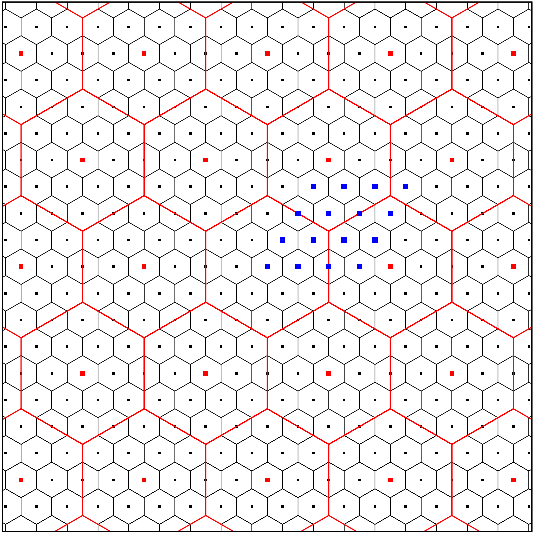
The lattice A_2, its sub-lattice $4A_2$, and their Voronoi cells.

Illustration: Voronoi Constellation $A_2/4A_2$ *(3)*



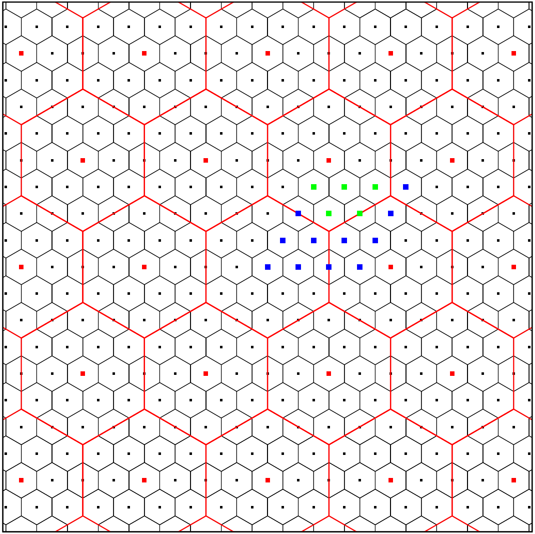
Select 16 points following the basis of A_2.

Illustration: Voronoi Constellation $A_2/4A_2$ *(3)*



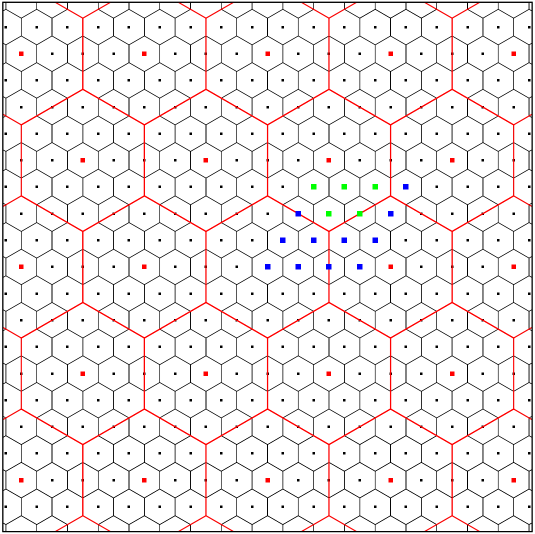
The constellation takes the shape of the fundamental parallelotope.

Illustration: Voronoi Constellation $A_2/4A_2$ *(4)*



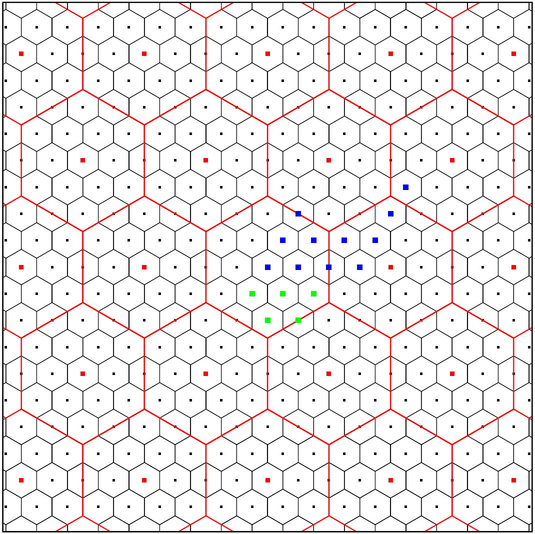
Consider the 5 points (in green) in the upper right red cell.

Illustration: Voronoi Constellation $A_2/4A_2$ (4)



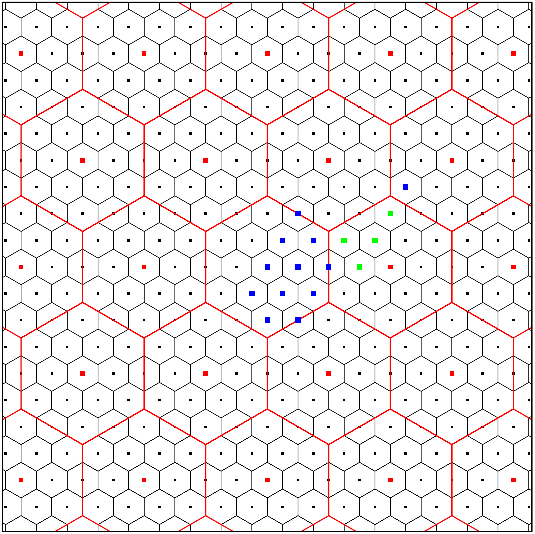
The nearest point in $4A_2$ to these 5 green points is the cell center.

Illustration: Voronoi Constellation $A_2/4A_2$ *(5)*



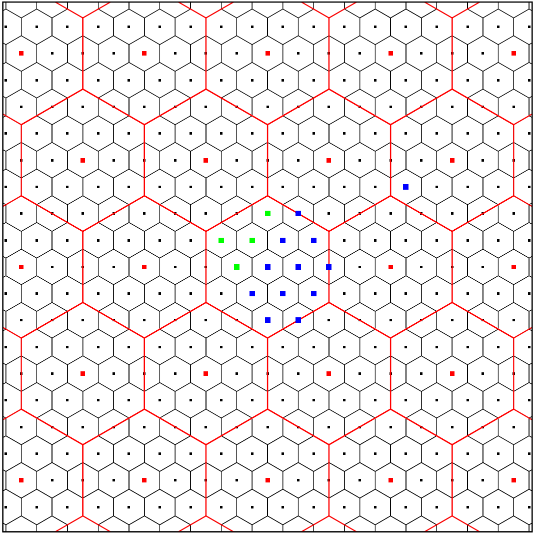
Subtract the cell center $(2, 4\sqrt{3}/2)$, i.e. translate down and left.

Illustration: Voronoi Constellation $A_2/4A_2$ *(6)*



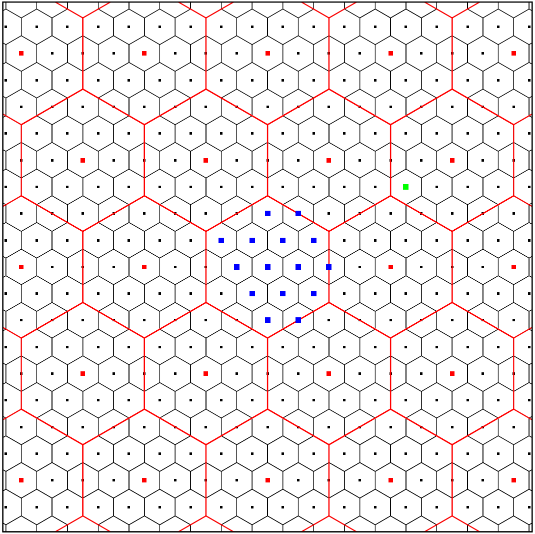
Consider the 4 points (in green) in the right red cell.

Illustration: Voronoi Constellation $A_2/4A_2$ (7)



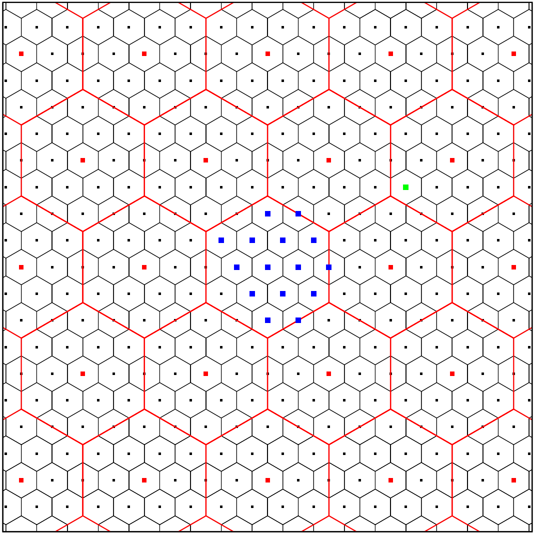
Translate to the left by subtracting the cell center $(4, 0)$.

Illustration: Voronoi Constellation $A_2/4A_2$ *(8)*



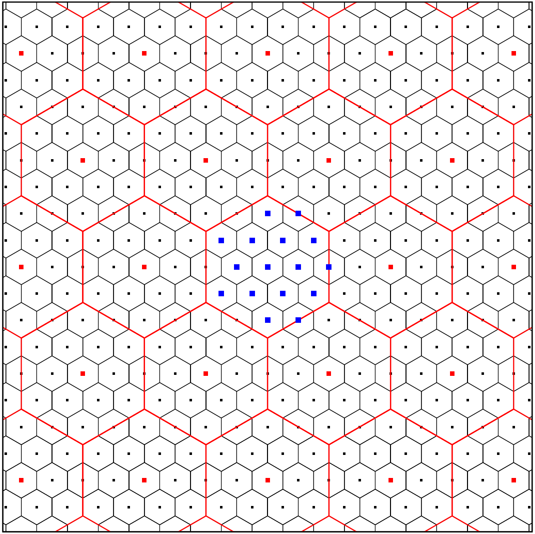
Consider the point (in green) in the upper (and twice to the right) red cell.

Illustration: Voronoi Constellation $A_2/4A_2$ (8)



Translate this green point by subtracting its red cell center $(6, 4\sqrt{3}/2)$.

Illustration: Voronoi Constellation $A_2/4A_2$ (9)



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 Λ_{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 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 Λ_{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

$$
\begin{pmatrix}
8 &&&&&&&&&&&&&&&&&&&&&&& \\
4 & 4 &&&&&&&&&&&&&&&&&&&&&& \\
4 & & 4 &&&&&&&&&&&&&&&&&&&&& \\
4 & & & 4 &&&&&&&&&&&&&&&&&&&& \\
4 & & & & 4 &&&&&&&&&&&&&&&&&&& \\
4 & & & & & 4 &&&&&&&&&&&&&&&&&& \\
4 & & & & & & 4 &&&&&&&&&&&&&&&&& \\
2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 &&&&&&&&&&&&&&&& \\
4 & & & & & & & & 4 &&&&&&&&&&&&&&& \\
4 & & & & & & & & & 4 &&&&&&&&&&&&&& \\
4 & & & & & & & & & & 4 &&&&&&&&&&&&& \\
2 & 2 & 2 & 2 & & & & & 2 & 2 & 2 & 2 &&&&&&&&&&&& \\
4 & & & & & & & & & & & & 4 &&&&&&&&&&& \\
2 & 2 & & & 2 & 2 & & & 2 & 2 & & & 2 & 2 &&&&&&&&&& \\
2 & & 2 & & 2 & & 2 & & 2 & & 2 & & 2 & & 2 &&&&&&&&& \\
2 & & & 2 & 2 & & & 2 & 2 & & & 2 & 2 & & & 2 &&&&&&&& \\
4 & & & & & & & & & & & & & & & & 4 &&&&&&& \\
2 & & 2 & & 2 & & & 2 & 2 & 2 & & & & & & & 2 & 2 &&&&&& \\
2 & & & 2 & 2 & 2 & & & 2 & & 2 & & & & & & 2 & & 2 &&&&& \\
2 & 2 & & & 2 & & 2 & & 2 & & & 2 & & & & & 2 & & & 2 &&&& \\
 & 2 & 2 & 2 & 2 & & & & 2 & & & & 2 & & & & 2 & & & & 2 &&& \\
 & & & & & & & & 2 & 2 & & & 2 & 2 & & & 2 & 2 & & & 2 & 2 && \\
 & & & & & & & & 2 & & 2 & & 2 & & 2 & & 2 & & 2 & & 2 & & 2 & \\
-3 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{pmatrix}
$$

Leech Constellations (2)

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

$$R_{\mathcal{C}} = \frac{\log_2 |\Lambda_f/\Lambda|}{n} = \frac{\log_2 \mathrm{Vol}(\Lambda)/\mathrm{Vol}(\Lambda_f)}{n} \text{ bits/dim}$$
$$= R \log_2 p + \log_2 \alpha + \frac{3}{2} \text{ bits/dim} .$$

How to Encode Voronoi Constellations (1)

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 Γ 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:

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

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 $C + p\mathcal{S} = \{\mathbf{c} + p\mathbf{s} \in \mathbb{Z}^n : \mathbf{c} \in C,\ \mathbf{s} \in \mathcal{S}\} \subseteq \Lambda_f$ is a complete set of coset leaders of Λ_f / Λ.

How to Encode Voronoi Constellations (2)

Sketch of the proof

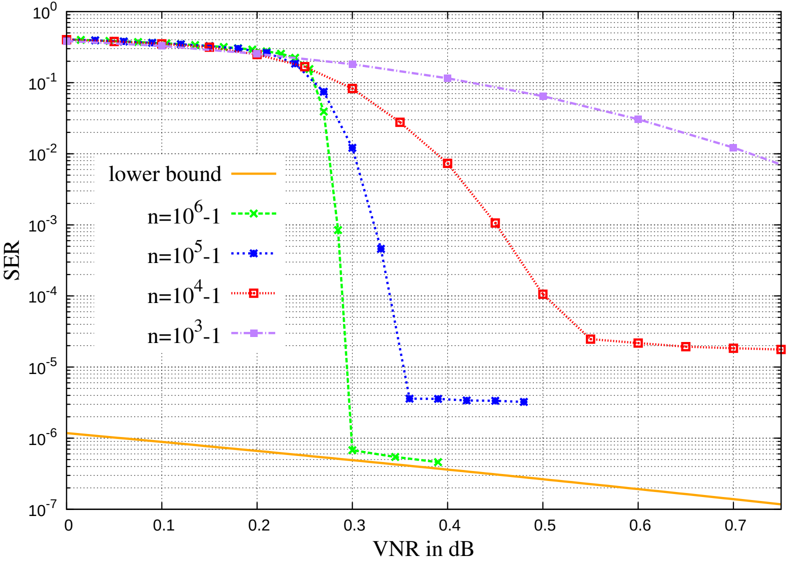
Counting points

$$|C + p\mathcal{S}| = |C||\mathcal{S}| = p^k \frac{\mathrm{Vol}(\Lambda)}{p^n} = |\Lambda_f/\Lambda|.$$

Distinct Cosets

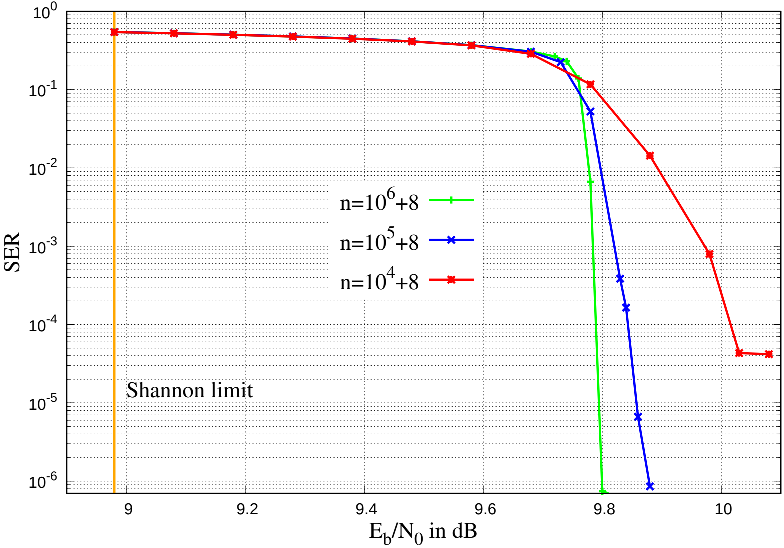
Take $\mathbf{x} = \mathbf{c} + p\mathbf{s}$ and $\mathbf{y} = \mathbf{d} + p\mathbf{v}$ in the same coset.
Then $\mathbf{x} - \mathbf{y} = \mathbf{c} - \mathbf{d} + p(\mathbf{s} - \mathbf{v}) \in \Lambda \subseteq p\mathbb{Z}^n$.
We get $\mathbf{c} = \mathbf{d}$. So $\mathbf{x} - \mathbf{y} = p(\mathbf{s} - \mathbf{v}) \in \Lambda = p\Gamma$.
It translates into $\mathbf{s} - \mathbf{v} \in \Gamma$, i.e. $\mathbf{s} - \mathbf{v} = \mathbf{z}T$.
From the definition of $\mathcal{S}$ and the triangularity of T, we find $\mathbf{s} = \mathbf{v}$ which proves that $\mathbf{x} = \mathbf{y}$.

Leech Constellations of LDA Lattices (1)



Infinite constellations of LDA lattices, $p = 13$ and $R = 1/3$

Leech Constellations of LDA Lattices (2)



Leech constellations of LDA lattices, $R_{\mathcal{C}} = 2.73$ bits/dim

Conclusions

- Complexity of mapping and demapping is linear in n.
- With a direct sum of Λ_{24}, the shaping gain is 1.03 dB.
- With a direct sum of Λ_{24}, the gap to Shannon capacity is 0.8 dB.
- Very fast universal Sphere Decoding of Λ_{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