When Cryptography Meets Modern Channel Coding

Joseph J. Boutros
Texas A&M University at Qatar

Lattices: Geometry, Algorithms and Hardness
The Simons Institute for the Theory of Computing, UC Berkeley.

February 21, 2020

Channel coding versus cryptography

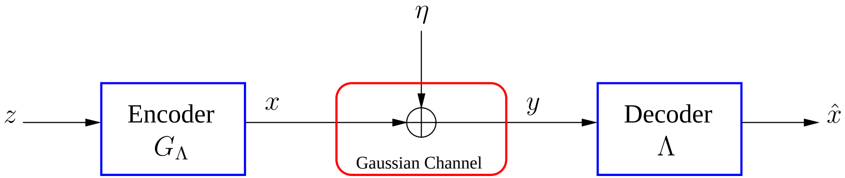
Criterion or Parameter	Channel Coding (Information Theory)	Cryptography (Computer Science)
Space type	$\mathbb{C}^n$, $\mathbb{R}^n$, $\mathbb{Z}^n$	$\mathbb{Z}_q^n$ (Crypto.), $\mathbb{R}^n$ (CS)
Random lattices	Channel models, coding and for analysis	Encryption and for analysis
Probability of Error	For Bob only 10^{-2}, 10^{-6}, 10^{-9}, 10^{-15} No 0 error rate!	For Bob and for Eve 0 for Bob (2^{-256}, 10^{-128}) Anything for Eve is fine!
Dimension	Up to 1 million, $n \to \infty$ for analysis	Up to 8000, $n \to \infty$ for analysis
Proofs	Shannon capacity	Proof of security
Signal-to-noise ratio	Energy or power, finite lattice constellations	Threshold on noise level in hom. encryption
Linearity	Geometrically uniform	Homomorphic encryption
Multiple access	CDMA, OFDMA, SDMA	Ciphers being added!
Complexity	Limited computational power for Alice and Bob.	Infinite for Eve, limited for Alice and Bob.

Channel coding versus cryptography

Criterion or Parameter	Channel Coding (Information Theory)	Cryptography (Computer Science)
Space type	$\mathbb{C}^n$, $\mathbb{R}^n$, $\mathbb{Z}^n$	$\mathbb{Z}_q^n$ (Crypto.), $\mathbb{R}^n$ (CS)
Random lattices	Channel models, coding and for analysis	Encryption and for analysis
Probability of Error	For Bob only 10^{-2}, 10^{-6}, 10^{-9}, 10^{-15} No 0 error rate!	For Bob and for Eve 0 for Bob (2^{-256}, 10^{-128}) Anything for Eve is fine!
Dimension	Up to 1 million, $n \to \infty$ for analysis	Up to 8000, $n \to \infty$ for analysis
Proofs	Shannon capacity	Proof of security
Signal-to-noise ratio	Energy or power, finite lattice constellations	Threshold on noise level in hom. encryption
Linearity	Geometrically uniform	Homomorphic encryption
Multiple access	CDMA, OFDMA, SDMA	Ciphers being added!
Complexity	Limited computational power for Alice and Bob.	Infinite for Eve, limited for Alice and Bob.

Transmitting information via lattice encoding/decoding

Simplified model for information transmission:
A lattice Λ of rank n in $\mathbb{R}^n$ undergoing an additive white Gaussian noise (AWGN).



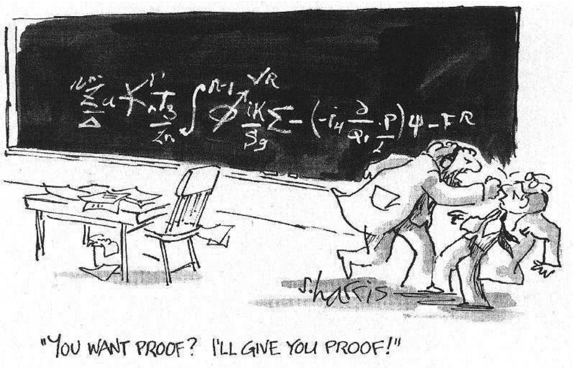
$z \in \mathbb{Z}^n$: information vector.
$x = zG_\Lambda \in \Lambda$: lattice point, infinite constellation..
$y = x + \eta \in \mathbb{R}^n$: channel output, $\eta_i \sim \mathcal{N}(0, \sigma^2)$.
AWGN: the $\{\eta_i\}$ are i.i.d.

Probability of error: $\mathcal{P}_e = \mathcal{P}\{x \neq \hat{x}\}$ (WER), $\quad \mathcal{P}_{es} = \mathcal{P}\{x_i \neq \hat{x}_i\}$ (SER).

Challenge in coding/communication theory

Take into account the volume of the Voronoi/Dirichlet cell, $vol(\Lambda) = |\det(G_\Lambda)|$.

- What is the maximal σ^2 such that $\lim_{n\to\infty} \mathcal{P}_e = 0$?
- Can we build a family of lattices Λ_n achieving $\sigma^2_{\max}$?
- Can we build a decoder for Λ_n for $n \gg 1$?



Leech & Sloane's Construction A (1)

Building lattices out of error-correcting codes: 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

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

The ring can be $\mathbb{Z}$ (relative integers), $\mathbb{Z}[i]$ (Gaussian integers), $\mathbb{Z}[\omega]$ (Eisenstein integers), $\mathscr{H}$ (Hurwitz quaternionic integers), $\mathscr{I}$ (icosian ring), and $O_{\mathbb{K}}$ (algebraic integers).

$C[n,k]_p$ should be correctly embedded in the ring (via a group homomorphism Φ).

Leech & Sloane's Construction A (1)

Building lattices out of error-correcting codes: 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

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

The ring can be $\mathbb{Z}$ (relative integers), $\mathbb{Z}[i]$ (Gaussian integers), $\mathbb{Z}[\omega]$ (Eisenstein integers), $\mathscr{H}$ (Hurwitz quaternionic integers), $\mathscr{I}$ (icosian ring), and $O_{\mathbb{K}}$ (algebraic integers).

$C[n,k]_p$ should be correctly embedded in the ring (via a group homomorphism Φ).

Leech & Sloane's Construction A (2)

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

Construction A can be thought of as

- drawing p^k points representing the codewords of C inside the cube $[0,p[^n$
- then paving the whole space $\mathbb{R}^n$ by translating the cube by multiples of p in all directions.

The theta series of Λ coincides with the theta series of C inside the ball of radius $(p-1)/2$ centered on the origin.

- A number field $\mathbb{K}$. Consider the canonical embedding $\sigma : O_{\mathbb{K}} \to \mathbb{R}^{[\mathbb{K}:\mathbb{Q}]}$, the homomorphism $\Phi : \mathbb{F}_p \to \Lambda_{O_{\mathbb{K}}}$, $\Lambda_{O_{\mathbb{K}}} = \sigma(O_{\mathbb{K}})$, and $\Lambda_I = \sigma(I)$, for I ideal in $O_{\mathbb{K}}$ where $p = |O_{\mathbb{K}}/I|$,

$$\Lambda = \Phi(C[m,k]_p) + \Lambda_I^m, \quad m = n/[\mathbb{K}:\mathbb{Q}].$$

Leech & Sloane's Construction A (2)

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

Construction A can be thought of as

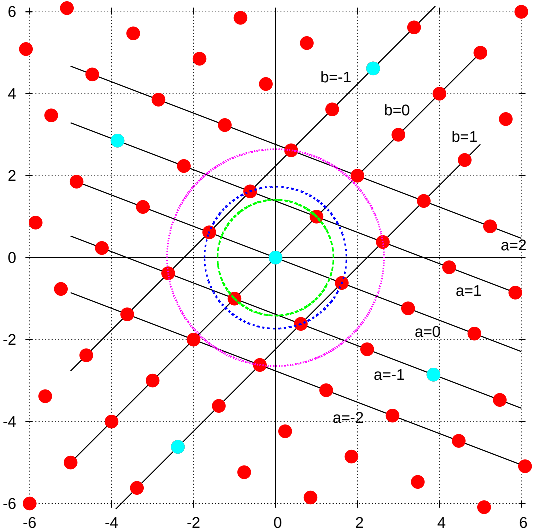
- drawing p^k points representing the codewords of C inside the cube $[0,p[^n$
- then paving the whole space $\mathbb{R}^n$ by translating the cube by multiples of p in all directions.

The theta series of Λ coincides with the theta series of C inside the ball of radius $(p-1)/2$ centered on the origin.

- A number field $\mathbb{K}$. Consider the canonical embedding $\sigma : O_{\mathbb{K}} \rightarrow \mathbb{R}^{[\mathbb{K}:\mathbb{Q}]}$, the homomorphism $\Phi : \mathbb{F}_p \rightarrow \Lambda_{O_{\mathbb{K}}}$, $\Lambda_{O_{\mathbb{K}}} = \sigma(O_{\mathbb{K}})$, and $\Lambda_I = \sigma(I)$, for I ideal in $O_{\mathbb{K}}$ where $p = |O_{\mathbb{K}}/I|$,

$$\Lambda = \Phi(C[m,k]_p) + \Lambda_I^m, \quad m = n/[\mathbb{K}:\mathbb{Q}].$$

Construction A from quadratic number fields



The bidimensional real lattices $\Lambda_{O_{\mathbb{K}}}$ and $\Lambda_{\mathcal{I}}$ built from the field $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ and $O_{\mathbb{K}}/\mathcal{I}$ shown on the first three shells ($p = 11$), $I = (-1 + 3\phi)O_{\mathbb{K}}$.

Leech & Sloane's Construction A (3)

The even unimodular Gosset lattice E_8 (one of the most beautiful lattices!) is built via Construction A with different rings (SPLAG, Conway and Sloane, 1999)

$$E_8 = [8,4,4]_2 + 2\mathbb{Z}^8 \qquad \text{over } \mathbb{Z}$$

$$E_8 = [4,1,4]_2 + \phi[4,3,2]_2 + \phi^2\mathbb{Z}[i]^4 \qquad \text{Construction B over } \mathbb{Z}[i] \text{ with } \phi = 1+i$$

$$E_8 = [4,3,2]_3 + \pi\mathbb{Z}[\omega]^4 \qquad \text{over } \mathbb{Z}[\omega] \text{ with } \pi = \sqrt{-3}$$

$$E_8 = [2,1,2]_4 + \phi\mathscr{H}^2 \qquad \text{over } \mathscr{H} \text{ with } \phi = 1+i$$

$$E_8 = \mathscr{I} \qquad \text{over } \mathscr{I} \text{ (1-dimensional over the icosian)}$$

$$E_8 = \sigma(I) \qquad \text{canonical embedding of the ideal } (5, \theta-2) \text{ in } \mathbb{Q}(\theta = e^{i2\pi/20})$$

E_8 is the densest lattice in $\mathbb{R}^8$, Hermite constant is 2, and kissing number is 240.

Leech & Sloane's Construction A (4)

- A lattice point can be written as $x = zG_\Lambda \in \Lambda$, where $z \in \mathbb{Z}^n$ and the $n \times n$ generator matrix is G_Λ in the form

$$G_\Lambda = \begin{pmatrix} U & P \\ 0 & pI_{n-k} \end{pmatrix}.$$

Here $G_\mathcal{C} = (U|P)$, U is unimodular, e.g. $U = I_k$.

- Λ is the union of p^k cosets, then its fundamental volume is

$$vol(\Lambda) = |\det(G_\Lambda)| = p^{n-k}.$$

- The minimum Euclidean distance of Λ satisfies:

$$\min\{p^2, d_{Hmin}(\mathcal{C})\} \quad \leq \quad d^2_{Emin}(\Lambda) \quad \leq \quad p^2.$$

- An upper bound on Hermite constant $\gamma(\Lambda) = \frac{d^2_{Emin}}{vol^{2/n}} =\leq \frac{p^2}{\sqrt[n/2]{p^{n-k}}} = p^{2R}$, where $R = k/n$. $\gamma(\Lambda)$ is also referred to as the fundamental gain.

Poltyrev limit for infinite constellations (1)

Theorem (Poltyrev 1994)

Given the AWGN channel with channel noise variance σ^2, there exists a sequence of n-dimensional lattices of constant volume V for which the decoding probability can be made as small as wanted for a sufficiently large value of n, if and only if

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

$\sigma^2_{\max}$ is often referred to as Poltyrev limit/capacity.

For Construction A lattices with a p-ary code

$$\sigma^2_{\max} = \frac{p^{2(1-R)}}{2\pi e}.$$

Our aim is to achieve a vanishing decoding probability with any $\delta > 0$ for

$$\sigma^2 = \sigma^2_{\max}(1-\delta)^2.$$

Poltyrev limit for infinite constellations (2)

Lemma (Typical Norm of Gaussian Noise)

Consider n *i.i.d. random Gaussian variables* $X_1, \ldots, X_n$, $X_i \sim \mathcal{N}(0, \sigma^2)$. *Let* $\rho = \sqrt{\sum_{i=1}^n X_i^2}$. *Then, for every* $\varepsilon > 0$,

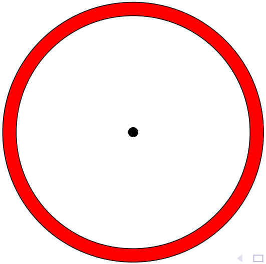
$$\lim_{n\to\infty} \mathcal{P}\left\{\sigma\sqrt{n}\,(1-\varepsilon) \leq \rho \leq \sigma\sqrt{n}\,(1+\varepsilon)\right\} = 1.$$

Simple proof based on Chebyshev's inequality, take $\zeta = \log n$:

$$\mathcal{P}\left\{|\rho^2 - n\sigma^2| > \zeta\sqrt{2n}\sigma^2\right\} \leq \frac{1}{\zeta^2}, \quad \text{then} \quad \lim_{n\to\infty} \mathcal{P}\left\{\rho^2 \leq \sigma^2 n\left(1+\zeta\sqrt{\frac{2}{n}}\right)\right\} = 1.$$

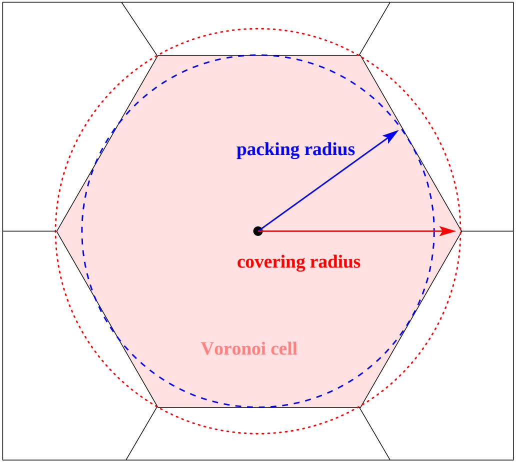
In high dimensions

$n \gg 1$



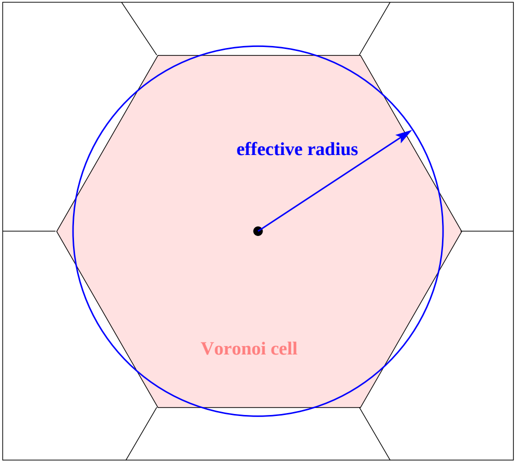
Poltyrev limit for infinite constellations (3)

Geometrical interpretation of Poltyrev limit.



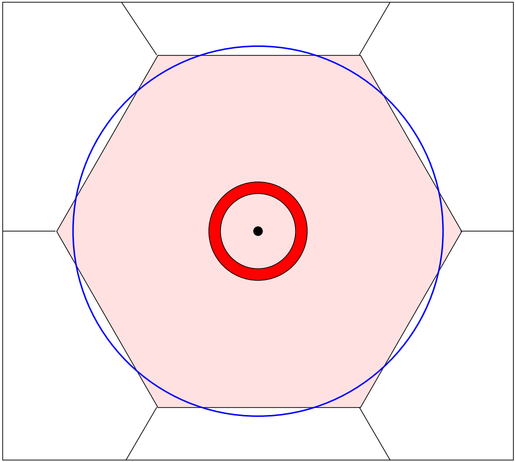
Poltyrev limit for infinite constellations (3)

Geometrical interpretation of Poltyrev limit. $V_n \rho_{eff}^n = vol(\Lambda)$.



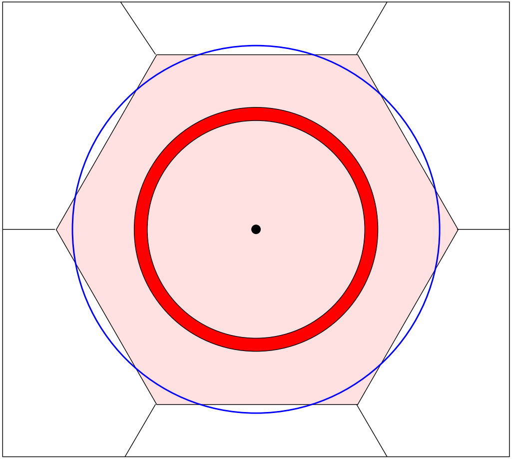
Poltyrev limit for infinite constellations (3)

Geometrical interpretation of Poltyrev limit. Small noise variance.



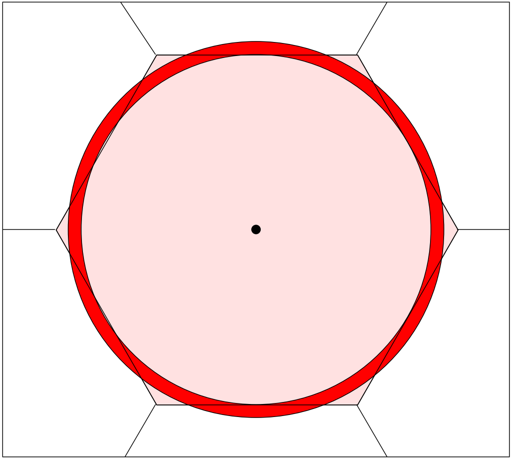
Poltyrev limit for infinite constellations (3)

Geometrical interpretation of Poltyrev limit. Larger noise variance.



Poltyrev limit for infinite constellations (3)

Geometrical interpretation. Limit is reached, $\sigma^2_{\max} = \frac{1}{2\pi e}$ for $vol = 1$.



Lemma on counting points and inequalities (1)

Lemma (Number of Integer Points in a Ball)

Let $\mathcal{B}_{c,n}(\rho)$ denotes the $n-$dimensional ball centered at c of radius ρ. Then,

$$|\mathbb{Z}^n \cap \mathcal{B}_{c,n}(\rho)| \leq \frac{1}{\sqrt{\pi n}} \left(\frac{\sqrt{2\pi e}\rho}{\sqrt{n}} \left(1 + \frac{\sqrt{n}}{2\rho}\right)\right)^n .$$

Proof:

For $z \in \mathbb{Z}^n$, let C_z be the cube of volume 1 centered at z.
The diagonal of C_z is $\sqrt{n}$. Then a ball centered at c of radius $\rho + \frac{\sqrt{n}}{2}$ will include all cubes of integer points z inside $\mathcal{B}_{c,n}(\rho)$,

$$|\mathbb{Z}^n \cap B_{\mathbf{c},n}(\rho)| \leq \mathrm{Vol}\left(B_{\mathbf{c},n}\left(\rho + \frac{\sqrt{n}}{2}\right)\right) = \mathrm{Vol}\left(B_{\mathbf{c},n}(\rho)\right)\left(1 + \frac{\sqrt{n}}{2\rho}\right)^n .$$

and by Stirling's formula we have

$$\mathrm{Vol}(B_{\mathbf{c},n}(\rho)) = \frac{(\sqrt{\pi}\rho)^n}{\Gamma\left(\frac{n}{2}+1\right)} \sim \frac{1}{\sqrt{\pi n}} \left(\frac{\sqrt{2\pi e}\rho}{\sqrt{n}}\right)^n .$$

Lemma on counting points and inequalities (2)

Take $\sigma^2 = \sigma^2_{\max}(1-\delta)^2 = \frac{p^{2(1-R)}}{2\pi e}(1-\delta)^2$.

Lemma (Integer Points to be Excluded)

Let $z = (z_1, \ldots, z_n) \in \mathbb{Z}^n$ such that $z_i \in p\mathbb{Z} \setminus \{0\}$ for some i. Then

$$\lim_{n\to\infty} \mathcal{P}\{\|\eta\|^2 \geq \|\eta - z\|^2\} = 0.$$

Proof:
Force to zero all components of z which are not multiple of p to get $\tilde{z} \in p\mathbb{Z}^n \setminus \{\mathbf{0}\}$.

$$\begin{aligned}
\mathcal{P}\{\|\eta\|^2 \geq \|\eta - z\|^2\} &\leq \mathcal{P}\{\|\eta\|^2 \geq \|\eta - \tilde{z}\|^2\} \\
&\leq \mathcal{P}\{|\eta_i| \geq p/2, \exists i \in \{1, 2, \ldots, n\}\} \\
&\leq 2nQ\left(\frac{p}{2\sigma}\right) \\
&\leq 2n \exp\left(\frac{\pi e p^{2R}}{4(1-\delta)^2}\right),
\end{aligned}$$

where $Q(x) \leq \exp(-x^2/2)$ is the Gaussian tail function. The upper bound decreases to 0 if $p = (\log n)^a$ and $2aR \geq 1$.

Lemma on counting points and inequalities (3)

Lemma (Bounds of the binomial coefficient)

Let n be a natural number and let $0 < \theta < 1$ be any rational number such that θn is natural, too. If $H(x) = -x\log(x) - (1-x)\log(1-x)$ is the binary entropy function, then:

$$\frac{1}{\sqrt{8n\theta(1-\theta)}} 2^{nH(\theta)} \leq \binom{n}{\theta n} \leq \frac{1}{\sqrt{2\pi n\theta(1-\theta)}} 2^{nH(\theta)}.$$

I spare you the proof :-),
see the book "The Theory of Error-Correcting Codes", by MacWillams and Sloane, 1977, page 309.

Other classical upper bounds of the binomial coefficient, useful in the sequel, for $k \in \mathbb{N}$ smaller than n,

$$\binom{n}{k} \leq \min\left\{ n^k, n^{n-k}, \left(\frac{n \cdot e}{k}\right)^k \right\}.$$

LDA Algebraic Construction (1)

A linear binary $[n=7, k=4]_2$ code.
The $k \times n$ generator matrix:

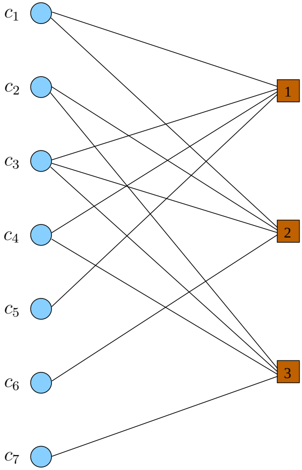
$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

The $(n-k) \times n$ parity-check matrix:

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Consider the parity-check matrix H as the incidence matrix of a bipartite graph, the (Tanner graph) of the code.

Tanner Graph



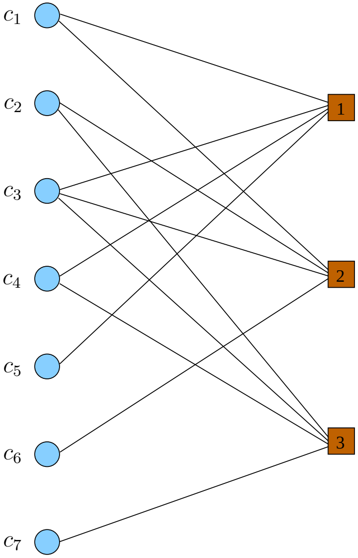
LDA Algebraic Construction (2)

n vertices

(variable nodes)

$\downarrow$

columns of H



$n - k$ vertices

(check nodes)

$\downarrow$

rows of H

LDA Algebraic Construction (3)

An LDPC code is defined by a sparse parity-check matrix H.
Let $\Lambda = C[n,k]_p + p\mathbb{Z}^n$, where p is an odd prime.
You may build a sparse H from units in a ring for p non-prime.

Definition

If $C[n,k]_p$ is a low-density parity-check (LDPC) code defined over $\mathbb{F}_p$, then Λ is called an LDA lattice.

LDA lattices studied by J.J. Boutros, L. Brunel, N. di Pietro, Y.-C. Huang, N. Kashyap, K. Narayanan, and G. Zémor, since 2011 for the Gaussian channel and for physical-layer network coding.

- LDA ensemble achieves Poltyrev limit $\sigma^2_{\max} = \frac{1}{2\pi e}$ (infinite constellations).
- LDA ensemble achieves Shannon capacity $\frac{1}{2}\log(1+\frac{P}{\sigma^2})$ (finite constellations).

See di Pietro, Zémor, Boutros, IEEE-IT-2018 and references therein.

LDA Algebraic Construction (3)

An LDPC code is defined by a sparse parity-check matrix H.
Let $\Lambda = C[n,k]_p + p\mathbb{Z}^n$, where p is an odd prime.
You may build a sparse H from units in a ring for p non-prime.

Definition

If $C[n,k]_p$ is a low-density parity-check (LDPC) code defined over $\mathbb{F}_p$, then Λ is called an LDA lattice.

LDA lattices studied by J.J. Boutros, L. Brunel, N. di Pietro, Y.-C. Huang, N. Kashyap, K. Narayanan, and G. Zémor, since 2011 for the Gaussian channel and for physical-layer network coding.

- LDA ensemble achieves Poltyrev limit $\sigma^2_{\max} = \frac{1}{2\pi e}$ (infinite constellations).
- LDA ensemble achieves Shannon capacity $\frac{1}{2}\log(1+\frac{P}{\sigma^2})$ (finite constellations).

See di Pietro, Zémor, Boutros, IEEE-IT-2018 and references therein.

GLD Algebraic Construction

Definition

• Let $\Lambda_0 \subset \mathbb{R}^{n_0}$ be a rank-n_0 real lattice (n_0 small). Consider the direct sum $\Lambda_0^{\oplus L}$. Then, a rank-n GLD lattice is $\Lambda = \bigcap_{i=1}^{J} \pi_i \left(\Lambda_0^{\oplus L}\right)$, for $n = L \times n_0$, $J \geq 2$, and $\{\pi_i\}_{i=1}^{J}$ are random permutations uniformly selected from $\mathcal{S}_n$.

• If $C[n,k]_p = \bigcap_{i=1}^{J} \pi_i \left(C_0^{\oplus L}\right)$ is a GLD code, then its associated GLD lattice is $\Lambda = C[n,k] + p\mathbb{Z}^n$, with $\Lambda_0 = C_0[n_0,k_0]_p + p\mathbb{Z}^{n_0}$.

GLD lattices studied by M. Bollauf, J.J. Boutros, N. di Pietro, Y.-C. Huang, and N. Mir, since 2014 for the Gaussian channel and for fading channels.

- GLD ensemble achieves Poltyrev limit (infinite constellations).
- Alphabet size is $p = (\log n)^a$ for GLD, but $p = n^\lambda$ for LDA.

See Bollauf, Boutros, Mir, IEEE-ITW-2019 Sweden and references therein.

GLD Algebraic Construction

Definition

• Let $\Lambda_0 \subset \mathbb{R}^{n_0}$ be a rank-n_0 real lattice (n_0 small). Consider the direct sum $\Lambda_0^{\oplus L}$. Then, a rank-n GLD lattice is $\Lambda = \bigcap_{i=1}^{J} \pi_i\left(\Lambda_0^{\oplus L}\right)$, for $n = L \times n_0$, $J \geq 2$, and $\{\pi_i\}_{i=1}^{J}$ are random permutations uniformly selected from $\mathcal{S}_n$.

• If $C[n,k]_p = \bigcap_{i=1}^{J} \pi_i\left(C_0^{\oplus L}\right)$ is a GLD code, then its associated GLD lattice is $\Lambda = C[n,k] + p\mathbb{Z}^n$, with $\Lambda_0 = C_0[n_0,k_0]_p + p\mathbb{Z}^{n_0}$.

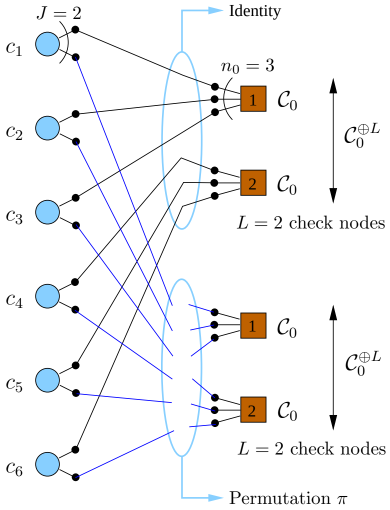
GLD lattices studied by M. Bollauf, J.J. Boutros, N. di Pietro, Y.-C. Huang, and N. Mir, since 2014 for the Gaussian channel and for fading channels.

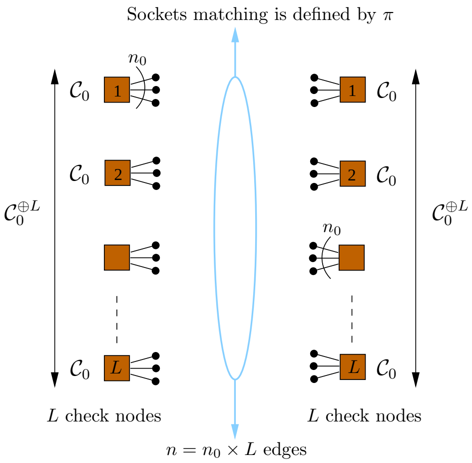
- GLD ensemble achieves Poltyrev limit (infinite constellations).
- Alphabet size is $p = (\log n)^a$ for GLD, but $p = n^{\lambda}$ for LDA.

See Bollauf, Boutros, Mir, IEEE-ITW-2019 Sweden and references therein.

GLD Tanner graphs, $\mathcal{C}_{gld} = \mathcal{C}_0^{\oplus L} \bigcap \pi(\mathcal{C}_0^{\oplus L})$

Tanner graphs, used for iterative decoding and analyzing cycles and weight.





Remarks - LDA versus GLD

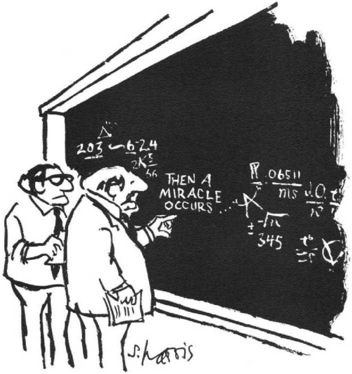
The capacity theorems for LDA lattices are proven using graph expansion properties. These expansion properties are usually pessimistic (here, for a high enough expansion factor D the check nodes degree increases at least as D^2). The complete LDA proof is extremely long, see Lemma 12 and Theorem 3 in di Pietro, Zémor, Boutros 2018.

In the sequel we are going to show the Poltyrev goodness of GLD lattices via a new technique called the buckets approach. We also rely on the asymptotic goodness of the constituent p-ary code.
More details in Bollauf, Boutros, Mir 2019.

GLD lattices achieve Poltyrev limit (1)

Theorem (Bollauf, Boutros, Mir 2019)

Consider a random GLD lattices ensemble over $\mathbb{F}_p$. Suppose that $p = (\log n)^a$ for some exponent $a > \frac{1}{2R}$. Moreover, assume that the minimum Hamming distance of the random GLD codes underlying the GLD lattices is lower bounded by Δn for some constant $\Delta > 0$. Then a random lattice of the family can be ML decoded with vanishing error probability for every channel noise variance $\sigma^2 < \sigma^2_{\max}$.



"I THINK YOU SHOULD BE MORE EXPLICIT HERE IN STEP TWO."

GLD lattices achieve Poltyrev limit (2)

Proof of GLD Poltyrev goodness:

- Lattice symmetry, $y = 0 + \eta$. Λ admits a closest-point decoder (maximum likelihood decoder).
- GLD coding rate is $R = k/n = 1 - J((1 - R_0)$, R_0 is the coding rate of the elementary code $\mathcal{C}_0[n_0, k_0, d_0]$.
- Lemma on typical norm of Gaussian noise, $\rho = \sigma\sqrt{n}(1+\varepsilon) = \frac{p^{J(1-R_0)}}{\sqrt{2\pi e}}\sqrt{n}(1-\delta)(1+\varepsilon) = \frac{p^{J(1-R_0)}}{\sqrt{2\pi e}}\sqrt{n}\kappa$.
- The decoding ball is $\mathcal{B} = \mathcal{B}_{y,n}(\rho)$, centered on y with radius ρ.
- Let $\aleph$ be the number of non-zero lattice points in $\mathcal{B}$, then

$$\mathcal{P}_e \;\leq\; \mathcal{P}(\aleph \geq 1) \;\leq\; \mathbb{E}[\aleph]$$

- Sum inside the noise sphere (remember the lemma on the excluded points)

$$\mathbb{E}[\aleph] = \sum_{x \in \mathbb{Z}^n \cap \mathcal{B}} \mathbb{E}[\mathbb{1}_{[x\in\Lambda]}] = \sum_{x \in \mathbb{Z}^n \cap \mathcal{B}} \mathcal{P}\{x \in \Lambda\}.$$

GLD lattices achieve Poltyrev limit (3)

- Introduce the Hamming weight ℓ of x. The error probability is upper-bounded as

$$\mathcal{P}_e \leq \sum_{x \in \mathbb{Z}^n \cap \mathcal{B}} \mathcal{P}\{x \in \Lambda\} \leq \sum_{\ell=\lceil \Delta n \rceil}^{n} \sum_{\substack{x \in \mathbb{Z}^n \cap \mathcal{B}: \\ W(x)=\ell}} \mathcal{P}\{x \in \Lambda\}$$

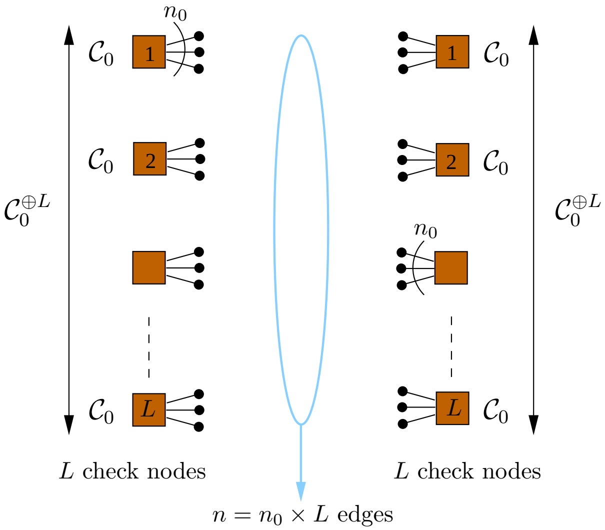
$$= \sum_{\ell=\lceil \Delta n \rceil}^{n} \sum_{\substack{x \in \mathbb{Z}^n \cap \mathcal{B}: \\ W(x)=\ell}} \left(\mathcal{P}\{x \bmod p \in \mathcal{C}_0^{\oplus L}\}\right)^J$$

- For a weight ℓ, there are b active buckets in the direct sum $\mathcal{C}_0^{\oplus L}$,

$$\mathcal{P}_e \leq \sum_{\ell=\lceil \Delta n \rceil}^{n} \sum_{\substack{x \in \mathbb{Z}^n \cap \mathcal{B}: \\ W(x)=\ell}} \left(\sum_{b=b_{\min}}^{b_{\max}} \frac{\mathcal{P}\{B=b\}}{p^{b(n_0-k_0)}} \right)^J .$$

- We used the fact that one active bucket $\mathcal{C}_0$ has its parity-check satisfied with probability $\frac{1}{p^{n_0-k_0}}$. We just need to find $\mathcal{P}\{B=b\}$ to complete the proof!

Probability of active buckets (1)



Probability of active buckets (2)

$$\mathcal{P}\{B=b\} = \frac{\binom{n/n_0}{b}}{\binom{n}{\ell}} \sum_{\substack{\{\ell_i\}: \\ \sum_{i=1}^{b} \ell_i = \ell}} \prod_{i=1}^{b} \binom{n_0}{\ell_i},$$

for $b \in [b_{\min}, b_{\max}]$, where $b_{\min} = \lceil \frac{\ell}{n_0} \rceil$ and $b_{\max} = \min(\lfloor \frac{\ell}{d_0} \rfloor, \frac{n}{n_0})$.

Corollary (Upper Bound of the Probability of Active Buckets)

The probability of b active buckets after throwing ℓ apples is bounded from above as

$$\mathcal{P}\{B=b\} \leq \frac{\binom{n/n_0}{b}}{\binom{n}{\ell}} \times c(\ell, b) \times \min\left\{ n_0^{\ell}, n_0^{bn_0-\ell}, (\tfrac{n_0 e}{d_0})^{\ell} \right\}.$$

$c(\ell, b)$ is the number of restricted compositions of ℓ with b parts solved via a saddle-point technique (Daniels-Good 1954-1957). See Bollauf, Boutros, Mir 2019.
Exercise: Think about $c(5,2)$ and $c(10,3)$ for $n_0 = 4$.

GLD lattices achieve Poltyrev limit (5)

- After using the lemma on the number of integer points in $\mathcal{B}_{c,n}$ and the previous corollary, where we denote $r = \ell/b$, $\omega = \ell/n \in [\Delta, 1]$, and $c(\ell, b)^{1/\ell} \sim C(t_0, r)$, we get

$$\mathcal{P}_e \leq \sum_{\ell=\lceil \Delta n \rceil}^{n} \binom{n}{\ell} |\mathbb{Z}^\ell \cap \mathcal{B}_{y,\ell}(\rho)| \left(\sum_{b=b_{\min}}^{b_{\max}} \frac{\mathcal{P}\{B=b\}}{p^{b(n_0-k_0)}} \right)^J$$

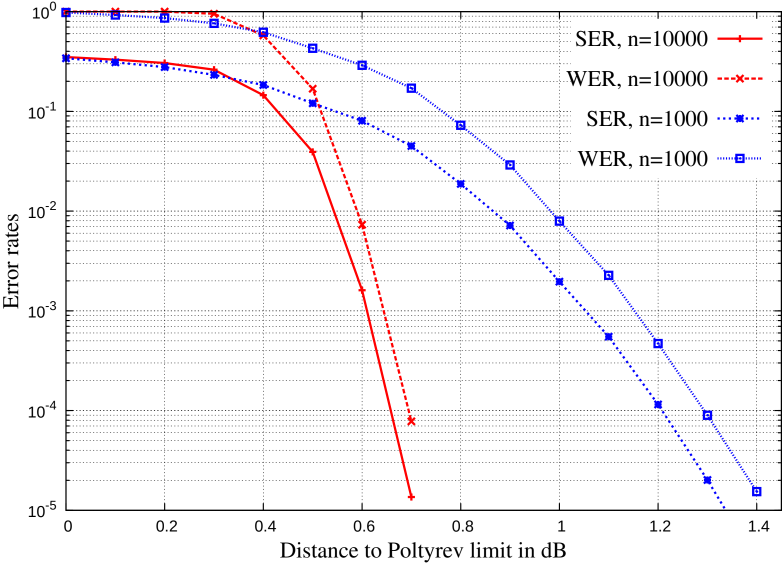
$$\leq \sum_{\ell=\Delta n}^{n} \left[\sum_{b=b_{\min}}^{b_{\max}} \left(\underbrace{\frac{e^{\frac{H(\omega n_0/r)}{\omega n_0}} C(t_0, r) \min\left\{ n_0, n_0^{\frac{n_0}{r}-1} \right\}}{p^{(n_0-k_0)\left(\frac{1}{r}-\frac{1}{n_0}\right)} \omega^{\frac{1}{2J}} e^{\frac{H(\omega)}{\omega}\frac{J-1}{J}}}}_{F_p(\omega, r)} \kappa \right)^{\ell} \right]^J$$

$$\rightarrow 0.$$

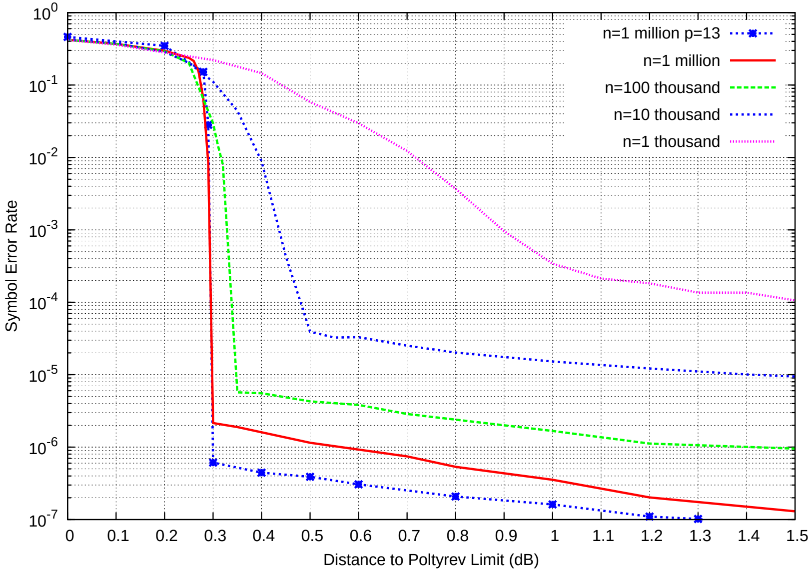
$\square$

- Note: $F_1(\omega, r) < 1$ for $r_c(\omega) < r \leq n_0$ and bounded from above by a constant for $r \leq r_c(\omega)$.

AWGN performance (LDA, regular-(2,5) LDPC, $p = 11$)



AWGN ensemble performance (GLD, $C_0[3,2]_p$, $p = 11$)



Conclusions

- In presence of Gaussian noise, in order to decode lattice points with a vanishing error probability, the noise variance per dimension must not exceed $\frac{1}{2\pi e}$ (Poltyrev limit).

- We showed how GLD lattices can achieve this limit, with $n \to \infty$ and $p = (\log n)^a$, under maximum-likelihood decoding (closest-point!).

- True computer performance showed here for dimensions between 1000 and 100000 is obtained via iterative probabilistic decoding on the lattice/code Tanner graph, with complexity $O(n \times p^{n_0 - k_0 + 1})$.

- Application of such lattices from p-ary codes in cryptography?

Papers related to this talk (1)

GLD lattices:

■ “New Bounds for GLD Lattices and Codes,” M. Bollauf, J.J. Boutros, and N. Mir, IEEE Information Theory Workshop 2019. PDF file.
■ “Non-Binary GLD Codes and their Lattices,” N. di Pietro, N. Basha, and J.J. Boutros, IEEE Information Theory Workshop 2015. PDF file.
■ “Spectral Thinning in GLD Lattices,” J.J. Boutros, N. di Pietro, and Y.-C. Huang, Information Theory and Applications 2015. PDF file.
■ “Generalized Low-Density (GLD) Lattices,” J.J. Boutros, N. di Pietro, and N. Basha, IEEE Information Theory Workshop 2014. PDF file.

LDA lattices:

■ “LDA Lattices Without Dithering Achieve Capacity on the Gaussian Channel,” N. di Pietro, G. Zémor, and J.J. Boutros, IEEE Transactions on Information Theory 2018. PDF file.
■ “Leech Constellations of Construction-A Lattices,” N. di Pietro and J.J. Boutros, IEEE Transactions on Communications 2017. PDF file.
■ “New results on Construction A Lattices based on Very Sparse Parity-Check Matrices,” N. di Pietro, G. Zémor, and J.J. Boutros, IEEE International Symposium on Information Theory 2013. PDF file.
■ “Integer Low-Density Lattices based on Construction A,” N. di Pietro, J.J. Boutros, G. Zémor, and L. Brunel, IEEE Information Theory Workshop 2012. PDF file.

Papers related to this talk (2)

Papers by other authors:

■ “Construction of Capacity-Achieving Lattice Codes: Polar Lattices,” L. Liu, Y. Yan , C. Ling, and X. Wu, IEEE Transactions on Communications 2019. PDF file.

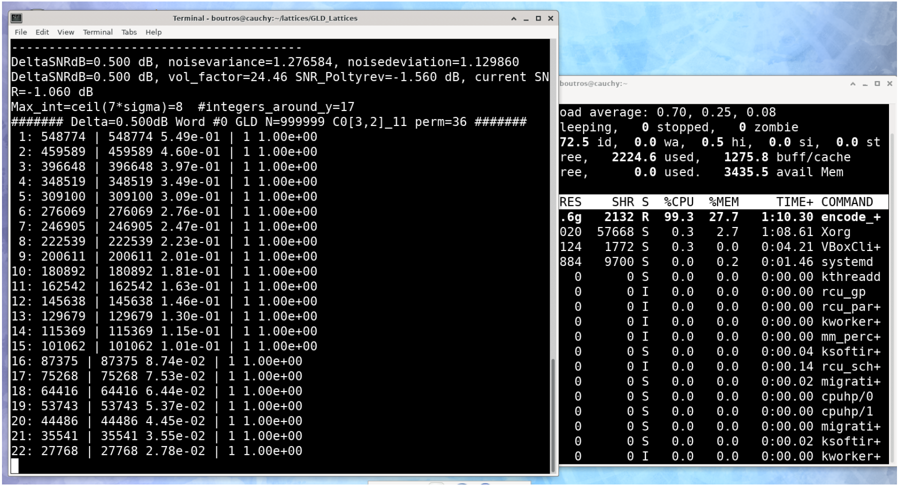
■ “Construction π_A and π_D Lattices: Construction, Goodness, and Decoding Algorithms,” Y.-C. Huang and K.R. Narayanan, IEEE Transactions on Information Theory 2017. PDF file.

■ “Some Goodness Properties of LDA Lattices,” S. Vatedka and N. Kashyap, Problems of Information Transmission 2017. PDF file.

■ “Lattices Over Eisenstein Integers for Compute-and-Forward,” N.E. Tunali, Y.-C. Huang, J.J. Boutros, and K.R. Narayanan, IEEE Transactions on Information Theory 2015. PDF file.

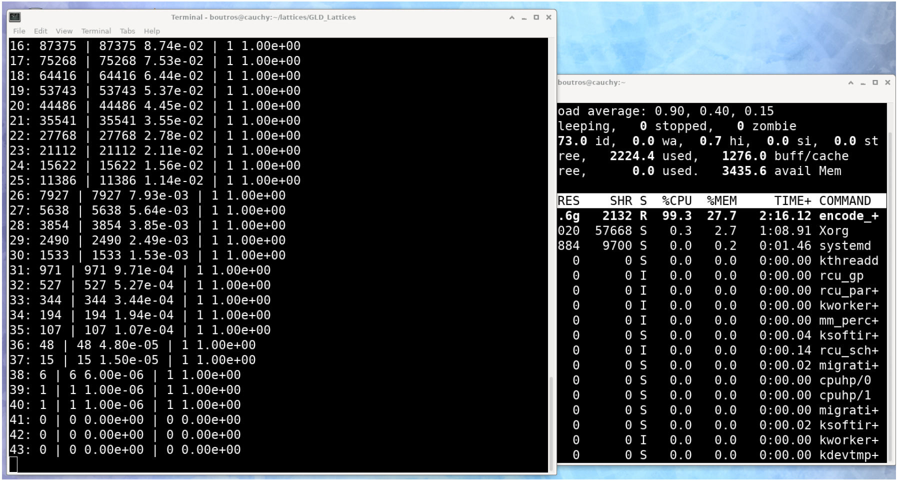
■ “Lattices from Codes for Harnessing Interference: An Overview and Generalizations,” Y.-C. Huang and K.R. Narayanan, IEEE Information Theory Workshop 2014. PDF file.

Screen copy of the live demo (1)



Iterative decoding of a GLD lattice in 1 million dimensions.
The Linux operating system has 6GB of RAM and 2 Intel CPU cores.

Screen copy of the live demo (2)



Iterative decoding of a GLD lattice in 1 million dimensions.
The Linux operating system has 6GB of RAM and 2 Intel CPU cores.