

Some “Goodness” Properties of LDA Lattices

Shashank Vatedka and Navin Kashyap

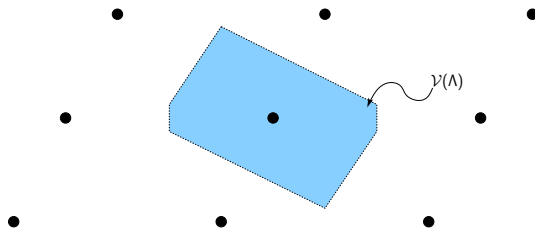
{shashank,nkashyap}@ece.iisc.ernet.in
Department of ECE
Indian Institute of Science
Bangalore, India

Information Theory Workshop
Jerusalem, Israel
2015

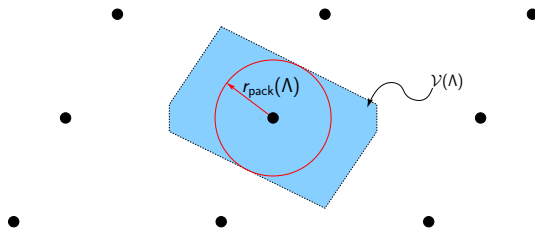


Some problems where lattices yield optimal/near optimal solutions:

- Sphere packing/covering
- Quantization
- AWGN channel
- Dirty paper channel
- Symmetric Gaussian interference channel
- Bidirectional relaying/Physical layer network coding
- Physical-layer security
- ... and more

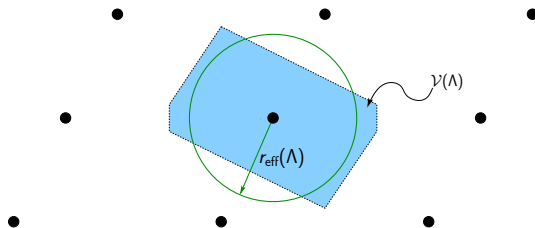


Fundamental Voronoi region: $\mathcal{V}(\Lambda)$



Fundamental Voronoi region: $\mathcal{V}(\Lambda)$

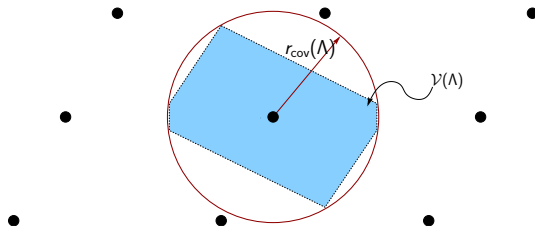
Packing radius: $r_{\text{pack}}(\Lambda)$



Fundamental Voronoi region: $\mathcal{V}(\Lambda)$

Packing radius: $r_{\text{pack}}(\Lambda)$

Effective radius: $r_{\text{eff}}(\Lambda)$



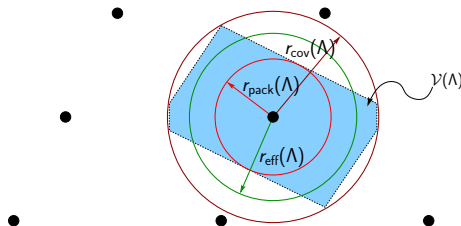
Fundamental Voronoi region: $\mathcal{V}(\Lambda)$

Packing radius: $r_{\text{pack}}(\Lambda)$

Effective radius: $r_{\text{eff}}(\Lambda)$

Covering radius: $r_{\text{cov}}(\Lambda)$

Clearly, $r_{\text{pack}}(\Lambda) \leq r_{\text{eff}}(\Lambda) \leq r_{\text{cov}}(\Lambda)$



Fundamental Voronoi region: $\mathcal{V}(\Lambda)$

Packing radius: $r_{\text{pack}}(\Lambda)$

Effective radius: $r_{\text{eff}}(\Lambda)$

Covering radius: $r_{\text{cov}}(\Lambda)$

Clearly, $r_{\text{pack}}(\Lambda) \leq r_{\text{eff}}(\Lambda) \leq r_{\text{cov}}(\Lambda)$

Normalized second moment (NSM)/Normalized moment of inertia (NMI): $G(\Lambda)$

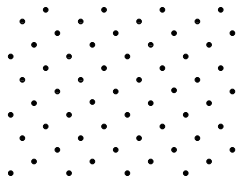
Let $\mathbf{X} \sim \text{Unif}(\mathcal{V}(\Lambda))$. Then,

$$G(\Lambda) = \frac{1}{\text{vol}(\mathcal{V}(\Lambda))^{2/n}} \times \frac{1}{n} \mathbb{E} \|\mathbf{X}\|^2$$

Components of a lattice code

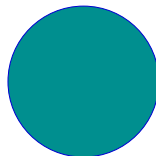
Lattice Λ

(In general, could be a coset)

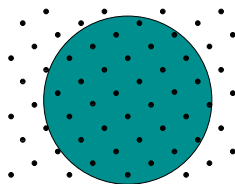


Shaping region \mathcal{S}

Convex set



Lattice code: $\mathcal{C} = \Lambda \cap \mathcal{S}$

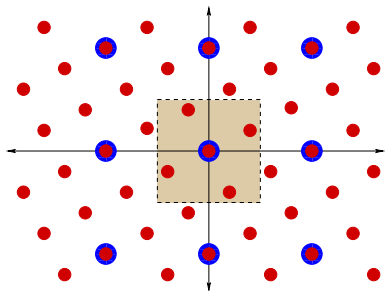


Nested lattice codes

n -dimensional lattices Λ, Λ_0 such that $\Lambda_0 \subset \Lambda$

Λ_0 : coarse lattice

Λ : fine lattice

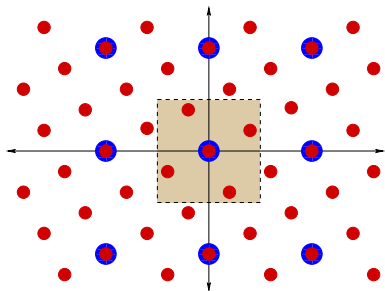


Nested lattice codes

n -dimensional lattices Λ, Λ_0 such that $\Lambda_0 \subset \Lambda$

Λ_0 : coarse lattice

Λ : fine lattice



Shaping region: $\mathcal{V}(\Lambda_0)$

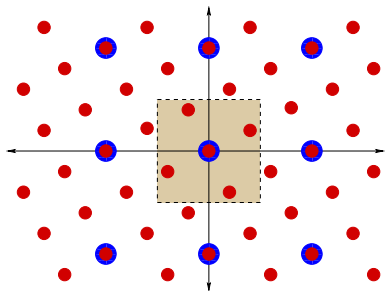
$$\begin{aligned} R &= \frac{1}{n} \log |\Lambda \cap \mathcal{V}(\Lambda_0)| \\ &= \frac{1}{n} \log \frac{\text{vol}(\mathcal{V}(\Lambda_0))}{\text{vol}(\mathcal{V}(\Lambda))} \end{aligned}$$

Nested lattice codes

n -dimensional lattices Λ, Λ_0 such that $\Lambda_0 \subset \Lambda$

Λ_0 : coarse lattice

Λ : fine lattice



Shaping region: $\mathcal{V}(\Lambda_0)$

$$\begin{aligned} R &= \frac{1}{n} \log |\Lambda \cap \mathcal{V}(\Lambda_0)| \\ &= \frac{1}{n} \log \frac{\text{vol}(\mathcal{V}(\Lambda_0))}{\text{vol}(\mathcal{V}(\Lambda))} \end{aligned}$$

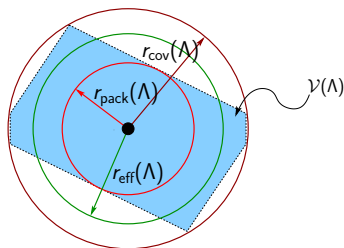
With dithered transmission:

$$P = \frac{1}{n} \mathbb{E} \|\mathbf{X}\|^2 = G(\Lambda_0) (\text{vol}(\mathcal{V}(\Lambda_0)))^{2/n}$$

With CLP decoding: $P_e = \Pr[\mathbf{Z}_{\text{noise}} \notin \mathcal{V}(\Lambda)]$.

Properties that we are looking for

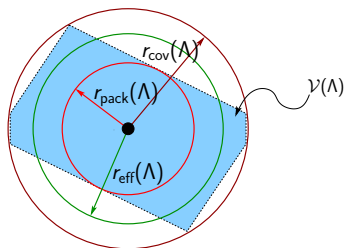
$\{\Lambda^{(n)}\}$ is good for



- **packing** if $\lim_{n \rightarrow \infty} \frac{r_{\text{pack}}(\Lambda^{(n)})}{r_{\text{eff}}(\Lambda^{(n)})} \geq \frac{1}{2}$.

Properties that we are looking for

$\{\Lambda^{(n)}\}$ is good for

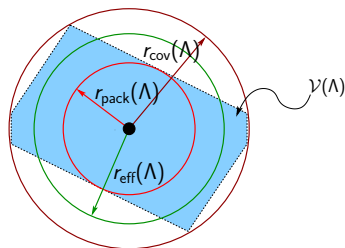


- packing if $\lim_{n \rightarrow \infty} \frac{r_{\text{pack}}(\Lambda^{(n)})}{r_{\text{eff}}(\Lambda^{(n)})} \geq \frac{1}{2}$.

- MSE (mean squared error) quantization if $\lim_{n \rightarrow \infty} G(\Lambda^{(n)}) = \frac{1}{2\pi e}$

Properties that we are looking for

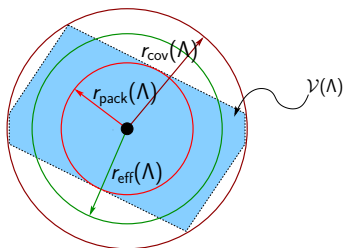
$\{\Lambda^{(n)}\}$ is good for



- **packing** if $\lim_{n \rightarrow \infty} \frac{r_{\text{pack}}(\Lambda^{(n)})}{r_{\text{eff}}(\Lambda^{(n)})} \geq \frac{1}{2}$.
- **MSE (mean squared error) quantization** if $\lim_{n \rightarrow \infty} G(\Lambda^{(n)}) = \frac{1}{2\pi e}$
- **covering** if $\lim_{n \rightarrow \infty} \frac{r_{\text{cov}}(\Lambda^{(n)})}{r_{\text{eff}}(\Lambda^{(n)})} = 1$.

Properties that we are looking for

$\{\Lambda^{(n)}\}$ is good for



- **packing** if $\lim_{n \rightarrow \infty} \frac{r_{\text{pack}}(\Lambda^{(n)})}{r_{\text{eff}}(\Lambda^{(n)})} \geq \frac{1}{2}$.
- **MSE (mean squared error) quantization** if $\lim_{n \rightarrow \infty} G(\Lambda^{(n)}) = \frac{1}{2\pi e}$
- **covering** if $\lim_{n \rightarrow \infty} \frac{r_{\text{cov}}(\Lambda^{(n)})}{r_{\text{eff}}(\Lambda^{(n)})} = 1$.

- **channel coding** if

$$\Pr[\mathbf{Z}^{(n)} \notin \mathcal{V}(\Lambda^{(n)})] \rightarrow 0 \text{ as } n \rightarrow \infty$$

for every semi norm-ergodic noise (e.g, AWGN) vectors $\mathbf{Z}^{(n)}$
with $\sigma^2 := \frac{1}{n} \mathbb{E} \|\mathbf{Z}^{(n)}\|^2$ that satisfy $\frac{\text{vol}(\Lambda^{(n)})^{2/n}}{2\pi e \sigma^2} > 1$.

Nested lattices for communication over Gaussian channels

Suppose we can construct nested lattice pairs such that:

- $\{\Lambda^{(n)}\}$ good for **channel coding**.
- $\{\Lambda_0^{(n)}\}$ good for **MSE quantization/covering**.

Nested lattices for communication over Gaussian channels

Suppose we can construct nested lattice pairs such that:

- $\{\Lambda^{(n)}\}$ good for **channel coding**.
- $\{\Lambda_0^{(n)}\}$ good for **MSE quantization/covering**.

This can be used to construct codes that

- achieve the capacity of the **AWGN** channel and the **dirty paper** channel. (Erez and Zamir 2004; Ordentlich and Erez 2012)
- achieve rates within a constant gap of the capacity of the **bidirectional relay**. (Wilson *et al.* 2010; Nazer and Gastpar 2011a; Nam *et al.* 2010; Ordentlich and Erez 2012)
- achieve rates guaranteed by many lattice-based **physical-layer network coding** schemes for Gaussian networks. (Nazer and Gastpar 2011b; Zhang *et al.* 2006)

Also important components in coding schemes for secure communication over the **Gaussian wiretap** channel (Ling *et al.* 2014) and the **bidirectional relay** (He and Yener 2013; Vattedka *et al.* 2014).

Construction A

Let \mathcal{C} be an (n, k) linear code over \mathbb{F}_p , for prime p .

The **Construction-A lattice** $\Lambda_A(\mathcal{C})$ is defined as

$$\Lambda_A(\mathcal{C}) = \{\mathbf{x} \in \mathbb{Z}^n : \mathbf{x} \equiv \mathbf{c} \bmod p \text{ for some } \mathbf{c} \in \mathcal{C}\}.$$

Construction A

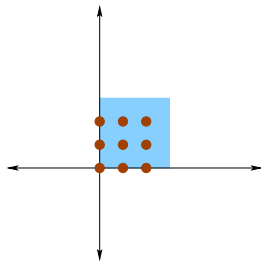
Let \mathcal{C} be an (n, k) linear code over \mathbb{F}_p , for prime p .

The **Construction-A lattice** $\Lambda_A(\mathcal{C})$ is defined as

$$\Lambda_A(\mathcal{C}) = \{\mathbf{x} \in \mathbb{Z}^n : \mathbf{x} \equiv \mathbf{c} \bmod p \text{ for some } \mathbf{c} \in \mathcal{C}\}.$$

Considering $\{0, 1, \dots, p-1\}$ to a subset of \mathbb{Z} , we may view \mathcal{C} as a subset of \mathbb{Z}^n . Then, $\Lambda_A(\mathcal{C}) = \mathcal{C} + p\mathbb{Z}^n$.

Example: \mathcal{C} is a $(2, 1)$ linear code over \mathbb{F}_3 with generator matrix $\begin{bmatrix} 1 & 2 \end{bmatrix}$.



Construction A

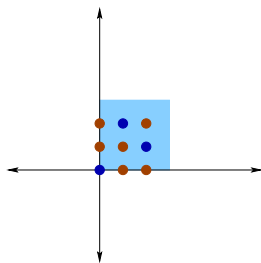
Let \mathcal{C} be an (n, k) linear code over \mathbb{F}_p , for prime p .

The **Construction-A lattice** $\Lambda_A(\mathcal{C})$ is defined as

$$\Lambda_A(\mathcal{C}) = \{\mathbf{x} \in \mathbb{Z}^n : \mathbf{x} \equiv \mathbf{c} \pmod{p} \text{ for some } \mathbf{c} \in \mathcal{C}\}.$$

Considering $\{0, 1, \dots, p-1\}$ to a subset of \mathbb{Z} , we may view \mathcal{C} as a subset of \mathbb{Z}^n . Then, $\Lambda_A(\mathcal{C}) = \mathcal{C} + p\mathbb{Z}^n$.

Example: \mathcal{C} is a $(2, 1)$ linear code over \mathbb{F}_3 with generator matrix $\begin{bmatrix} 1 & 2 \end{bmatrix}$.



Construction A

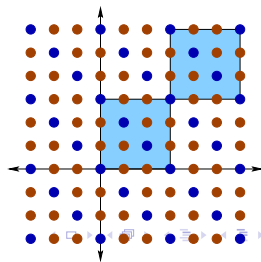
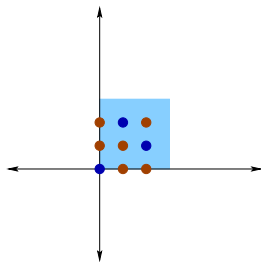
Let \mathcal{C} be an (n, k) linear code over \mathbb{F}_p , for prime p .

The **Construction-A lattice** $\Lambda_A(\mathcal{C})$ is defined as

$$\Lambda_A(\mathcal{C}) = \{\mathbf{x} \in \mathbb{Z}^n : \mathbf{x} \equiv \mathbf{c} \pmod{p} \text{ for some } \mathbf{c} \in \mathcal{C}\}.$$

Considering $\{0, 1, \dots, p-1\}$ to a subset of \mathbb{Z} , we may view \mathcal{C} as a subset of \mathbb{Z}^n . Then, $\Lambda_A(\mathcal{C}) = \mathcal{C} + p\mathbb{Z}^n$.

Example: \mathcal{C} is a $(2, 1)$ linear code over \mathbb{F}_3 with generator matrix $[1 \ 2]$.



Goodness of Construction-A lattices

The (n, k, p) ensemble: For prime p , the ensemble of all Construction-A lattices obtained from (n, k) linear codes over \mathbb{F}_p .

Theorem (Erez et al. 2005, Thm. 5)

Let k and p be suitably chosen functions of n . If $\Lambda^{(n)}$ is a randomly chosen Construction-A lattice from an (n, k, p) ensemble, then, for every $\epsilon > 0$,

$$\frac{r_{\text{pack}}(\Lambda^{(n)})}{r_{\text{eff}}(\Lambda^{(n)})} \geq \frac{1}{2} - \epsilon, \quad \frac{r_{\text{cov}}(\Lambda^{(n)})}{r_{\text{eff}}(\Lambda^{(n)})} \leq 1 + \epsilon,$$

$$G(\Lambda^{(n)}) \leq \frac{1}{2\pi e} + \epsilon, \quad \Pr[\mathbf{Z}^{(n)} \notin \mathcal{V}(\Lambda^{(n)})] \leq \epsilon$$

with probability tending to 1 as $n \rightarrow \infty$.

Goodness of Construction-A lattices

The (n, k, p) ensemble: For prime p , the ensemble of all Construction-A lattices obtained from (n, k) linear codes over \mathbb{F}_p .

Theorem (Erez et al. 2005, Thm. 5)

Let k and p be suitably chosen functions of n . If $\Lambda^{(n)}$ is a randomly chosen Construction-A lattice from an (n, k, p) ensemble, then, for every $\epsilon > 0$,

$$\frac{r_{\text{pack}}(\Lambda^{(n)})}{r_{\text{eff}}(\Lambda^{(n)})} \geq \frac{1}{2} - \epsilon, \quad \frac{r_{\text{cov}}(\Lambda^{(n)})}{r_{\text{eff}}(\Lambda^{(n)})} \leq 1 + \epsilon,$$

$$G(\Lambda^{(n)}) \leq \frac{1}{2\pi e} + \epsilon, \quad \Pr[\mathbf{Z}^{(n)} \notin \mathcal{V}(\Lambda^{(n)})] \leq \epsilon$$

with probability tending to 1 as $n \rightarrow \infty$.

How do we decode??

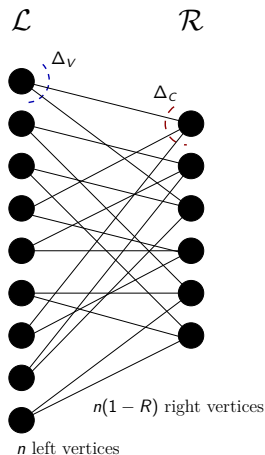
Lattices with Low Decoding Complexity

Some constructions of “good” lattices with low-complexity decoding algorithms.

- **Low Density Construction-A (LDA) Lattices:** Construction A on nonbinary LDPC codes (di Pietro *et al.* 2012).
- **LDPC lattices:** Construction D' on nested binary LDPC codes (Sadeghi *et al.* 2006).
- **Turbo lattices:** Construction D on turbo codes (Sakzad *et al.* 2010).
- **Polar lattices:** Construction D on nested polar codes (Yan *et al.* 2013).
- **Low-Density Lattice Codes (LDLC):** Not obtained from linear codes; The dual lattice has a low-density generator matrix (Sommer *et al.* 2008).

Low-density Construction-A (LDA) lattices

Use (Δ_V, Δ_C) -regular LDPC codes to obtain Construction-A lattices. We can then use BP decoding!

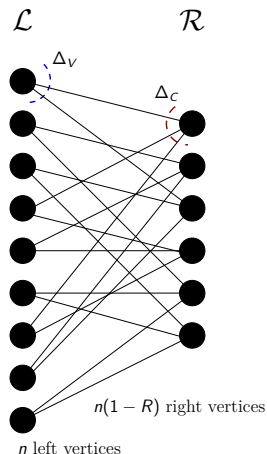


- (di Pietro *et al.* 2012): introduced **logarithmic degree** LDA lattices, showed goodness for channel coding.
- (di Pietro *et al.* 2013a): **constant degree** LDA lattices are good for channel coding.
- (di Pietro *et al.* 2013b) and (Tunali *et al.* 2013): simulations showing that LDA lattices go close to Poltyrev limit with BP decoding.
- (di Pietro 2014): nested LDA lattices **achieve capacity of AWGN channel** with CLP decoding.

The Tanner graph

To obtain “good” lattices, we want the Tanner graph of the underlying LDPC code to satisfy certain **expansion properties**:

There exist positive constants ϵ, ϑ , and $\alpha \leq A$ and $\beta \leq B$ such that



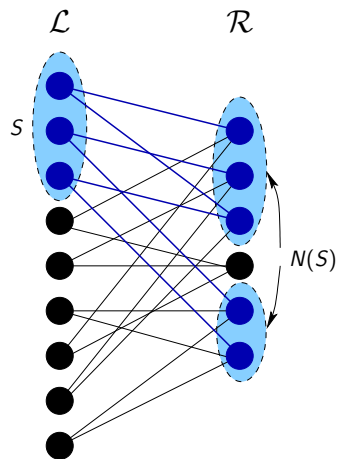
The Tanner graph

To obtain “good” lattices, we want the Tanner graph of the underlying LDPC code to satisfy certain **expansion properties**:

There exist positive constants ϵ, ϑ , and $\alpha \leq A$ and $\beta \leq B$ such that

Left vertex expansion: for any $S \subset \mathcal{L}$

- $|S| \leq \lceil \epsilon n \rceil \implies |N(S)| \geq A|S|$.
- $|S| \leq \left\lceil \frac{n(1-R)}{2\alpha} \right\rceil \implies |N(S)| \geq \alpha|S|$



The Tanner graph

To obtain “good” lattices, we want the Tanner graph of the underlying LDPC code to satisfy certain **expansion properties**:

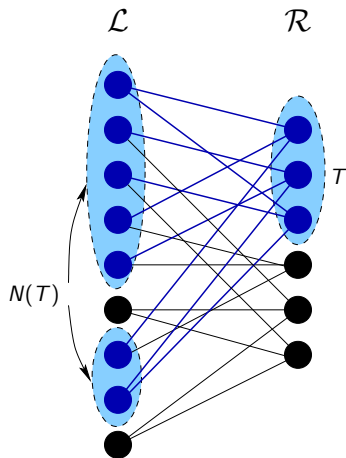
There exist positive constants ϵ, ϑ , and $\alpha \leq A$ and $\beta \leq B$ such that

Left vertex expansion: for any $S \subset \mathcal{L}$

- $|S| \leq \lceil \epsilon n \rceil \implies |N(S)| \geq A|S|$.
- $|S| \leq \left\lceil \frac{n(1-R)}{2\alpha} \right\rceil \implies |N(S)| \geq \alpha|S|$

Right vertex expansion: for any $T \subset \mathcal{R}$

- $|T| \leq \vartheta n(1-R) \implies |N(T)| \geq B|T|$
- $|T| \leq \frac{n(1-R)}{2} \implies |N(T)| \geq \beta|T|$



Random graphs are good expanders

Fix constants $1 \leq \alpha \leq A$ and $\frac{1}{1-R} < \beta \leq \min\left(\frac{2}{1-R}, B\right)$, and $0 < \vartheta, \epsilon < 1/2$.

Lemma (di Pietro 2014, Lem. 3.3)

If

$$\Delta_V > f(\alpha, A, \beta, B, \epsilon, \vartheta, R),$$

then the *probability* that a $(\Delta_V, \Delta_V(1-R))$ -regular graph is a *good expander goes to one* as $n \rightarrow \infty$.

Throughout, we assume that the hypothesis is satisfied, and the Tanner graph is a good expander.

The (\mathcal{G}, λ) ensemble of LDA lattices

Let $\lambda > 0$ and p be the smallest prime greater than n^λ .

Pick a $(\Delta_V, \Delta_V(1 - R))$ -regular \mathcal{G} which is a good expander.

- Let \hat{H} be the corresponding adjacency (parity-check) matrix.

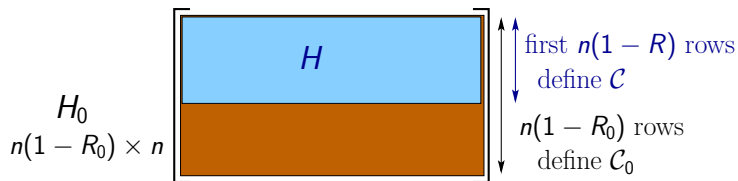
$$\hat{H} = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix},$$

- Replace the 1's with iid $\text{Unif}(\mathbb{F}_p)$ rvs.

$$H = \begin{pmatrix} h'_{11} & h'_{12} & 0 & 0 & h'_{15} & 0 \\ 0 & h'_{22} & 0 & h'_{24} & 0 & h'_{26} \\ 0 & 0 & h'_{33} & h'_{34} & h'_{35} & 0 \\ h'_{41} & 0 & h'_{43} & 0 & 0 & h'_{46} \end{pmatrix}.$$

- Apply Construction A on the code defined by H .

Nested LDA lattices



Pick nested LDPC codes \mathcal{C}_0 and \mathcal{C} , with $\mathcal{C}_0 \subset \mathcal{C}$.

Then,

$$\Lambda = \Lambda_A(\mathcal{C}) \text{ and } \Lambda_0 = \Lambda_A(\mathcal{C}_0).$$

Parameters of the LDA ensemble

We choose the parameters so as to satisfy:

- $0 < R < 1$
- $1 < \alpha \leq A$
- $A > 2(1 + R)$
- $\epsilon = \frac{1-R}{A+1-R}$
- $\frac{1}{1-R} < \beta \leq \min \left\{ B, \frac{2}{1-R} \right\}$
- $B > 2 \frac{(1+R)}{(1-R)}$
- $\vartheta = \frac{1}{B(1-R)+1}$
- $\Delta_V > f(\alpha, A, \beta, B, \epsilon, \vartheta, R)$

For example,

- $R = 1/3$
- $\alpha = 2.7$
- $A = 3$
- $\epsilon = 0.182$
- $\beta = 1.6$
- $B = 5$
- $\vartheta = 0.231$
- $\Delta_V = 21$

Goodness for channel coding

Recall: $p \approx n^\lambda$.

The following result was proved by di Pietro:

Theorem (di Pietro 2014, Theorem 3.2)

Let Λ be a lattice chosen uniformly at random from a (\mathcal{G}, λ) LDA ensemble. If

$$\lambda > \max \left\{ \frac{1}{2(\alpha - 1 + R)}, \frac{3}{2(A - 1 + R)}, \frac{1}{B(1 - R) - 1} \right\},$$

then the probability that Λ is good for channel coding tends to 1 as $n \rightarrow \infty$.

Goodness for channel coding

Recall: $p \approx n^\lambda$.

The following result was proved by di Pietro:

Theorem (di Pietro 2014, Theorem 3.2)

Let Λ be a lattice chosen uniformly at random from a (\mathcal{G}, λ) LDA ensemble. If

$$\lambda > \max \left\{ 0.2679, 0.6429, 0.4286 \right\},$$

then the probability that Λ is good for channel coding tends to 1 as $n \rightarrow \infty$.

Goodness for channel coding

Recall: $p \approx n^\lambda$.

The following result was proved by di Pietro:

Theorem (di Pietro 2014, Theorem 3.2)

Let Λ be a lattice chosen uniformly at random from a (\mathcal{G}, λ) LDA ensemble. If

$$\lambda > \max \left\{ 0.2679, 0.6429, 0.4286 \right\},$$

then the probability that Λ is good for channel coding tends to 1 as $n \rightarrow \infty$.

Also, (di Pietro 2014) found sufficient conditions on parameters for nested LDA lattices to **achieve capacity of AWGN channel**.

Packing Goodness

Proofs of channel coding goodness and packing goodness are very similar.

Theorem (Vatedka & Kashyap, ITW 15)

Let Λ be a lattice chosen uniformly at random from a (\mathcal{G}, λ) LDA ensemble, Furthermore, let^a

$$\lambda > \max \left\{ \frac{1}{2(\alpha - 1 + R)}, \frac{3}{2(A - 1 + R)}, \frac{1}{B(1 - R) - 1} \right\}.$$

Then, the probability that Λ is good for packing tends to 1 as $n \rightarrow \infty$.

^a $p \approx n^\lambda$

Packing Goodness

Proofs of channel coding goodness and packing goodness are very similar.

Theorem (Vatedka & Kashyap, ITW 15)

Let Λ be a lattice chosen uniformly at random from a (\mathcal{G}, λ) LDA ensemble, Furthermore, let^a

$$\lambda > \max \left\{ 0.2679, 0.6429, 0.4286 \right\}.$$

Then, the probability that Λ is good for packing tends to 1 as $n \rightarrow \infty$.

^a $p \approx n^\lambda$

Theorem (Vatedka & Kashyap, ITW 15)

Suppose^a

$$\lambda > \max \left\{ \frac{1}{R}, \frac{1}{1-R}, \frac{2}{A-2(1+R)}, \frac{2}{B(1-R)-2(1+R)}, \right. \\ \left. 2 \left(1 - \frac{1}{AB-1} - \frac{1}{A} \right)^{-1} \right\}.$$

Let Λ be randomly chosen from a (\mathcal{G}, λ) LDA ensemble. Then, the probability that Λ is good for MSE quantization tends to 1 as $n \rightarrow \infty$.

^a $p \approx n^\lambda$

Theorem (Vatedka & Kashyap, ITW 15)

Suppose^a

$$\lambda > \max \left\{ 3.0, 1.5, 6.0, 3.0, 3.36 \right\}.$$

Let Λ be randomly chosen from a (\mathcal{G}, λ) LDA ensemble. Then, the probability that Λ is good for MSE quantization tends to 1 as $n \rightarrow \infty$.

^a $p \approx n^\lambda$

Packing goodness of the duals

Motivation: Perfect secrecy in an honest-but-curious bidirectional relay setting.

To achieve best known rates in presence of Gaussian noise, need (Vatedka *et al.* 2014; Vatedka and Kashyap 2015)

- $\{\Lambda^{(n)}\}$ to be good for **channel coding**
- $\{\Lambda_0^{(n)}\}$ to be good for **MSE quantization**
- **duals** of $\{\Lambda_0^{(n)}\}$ to be good for **packing**

Theorem (Vatedka & Kashyap, ITW 15)

If

$$\lambda > \max \left\{ \frac{1}{2(1-R)}, \frac{2B + 3/2}{B(1-R) - 1} \right\},$$

then the dual of a randomly chosen lattice from a (\mathcal{G}, λ) LDA ensemble is good for packing with probability tending to 1 as $n \rightarrow \infty$.

Packing goodness of the duals

Motivation: Perfect secrecy in an honest-but-curious bidirectional relay setting.

To achieve best known rates in presence of Gaussian noise, need (Vatedka *et al.* 2014; Vatedka and Kashyap 2015)

- $\{\Lambda^{(n)}\}$ to be good for **channel coding**
- $\{\Lambda_0^{(n)}\}$ to be good for **MSE quantization**
- **duals** of $\{\Lambda_0^{(n)}\}$ to be good for **packing**

Theorem (Vatedka & Kashyap, ITW 15)

If

$$\lambda > \max \left\{ 0.75, \mathbf{4.928} \right\},$$

then the dual of a randomly chosen lattice from a (\mathcal{G}, λ) LDA ensemble is good for packing with probability tending to 1 as $n \rightarrow \infty$.

- So far, assumed CLP decoder was used.
- Using BP decoder, complexity would be $O(np \log p)$.
We want p to be as small as possible.
- Turns out we cannot make p any less than n^4 for our proofs to go through.
- Although this means order of complexity is polynomial in n , still too high!
- **Simulation results** in (di Pietro *et al.* 2013b; Tunali *et al.* 2013) used much smaller values of p ($p = 11$ for blocklength ~ 10000) but obtained good performance.
- Better proof techniques required.

LDA lattices: an attractive option

Has a natural **low-complexity decoding** algorithm!

- Good for **packing**
- Good for **MSE quantization**
- Good for **channel coding**
- **Duals** are good for **packing**

Open:

- Are LDA lattices good for **covering**?
- **Error exponents** with CLP decoder?
- Performance with **BP decoding**?

Full version: <http://arxiv.org/abs/1410.7619>







U. Erez and R. Zamir, “Achieving $1/2 \log(1 + \text{SNR})$ on the AWGN channel with lattice encoding and decoding,” *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2293–2314, 2004.







O. Ordentlich and U. Erez, “A simple proof for the existence of “good” pairs of nested lattices,” in *2012 IEEE 27th Convention of Electrical & Electronics Engineers in Israel (IEEEI)*, IEEE, 2012, pp. 1–12.







M. Wilson, K. Narayanan, H. Pfister, and A. Sprintson, “Joint physical layer coding and network coding for bidirectional relaying,” *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5641–5654, 2010.

-  B. Nazer and M. Gastpar, “Compute-and-forward: harnessing interference through structured codes,” *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6463–6486, 2011.
-  W. Nam, S.-Y. Chung, and Y. H. Lee, “Capacity of the Gaussian two-way relay channel to within 1/2 bit,” *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5488–5494, 2010.
-  B. Nazer and M. Gastpar, “Reliable physical layer network coding,” *Proceedings of the IEEE*, vol. 99, no. 3, pp. 438–460, 2011.
-  S. Zhang, S. C. Liew, and P. P. Lam, “Hot topic: physical-layer network coding,” in *Proceedings of the 12th annual international conference on Mobile computing and networking*, 2006, pp. 358–365.

-  C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehle, “Semantically secure lattice codes for the Gaussian wiretap channel,” *IEEE Transactions on Information Theory*, vol. 60, no. 10, pp. 6399–6416, 2014.
-  X. He and A. Yener, “Strong secrecy and reliable byzantine detection in the presence of an untrusted relay,” *IEEE Transactions on Information Theory*, vol. 59, no. 1, pp. 177–192, 2013.
-  S. Vatedka, N. Kashyap, and A. Thangaraj, “Secure compute-and-forward in a bidirectional relay,” *accepted, IEEE Transactions on Information Theory*, 2014. [Online]. Available: <http://arxiv.org/abs/1206.3392>.
-  U. Erez, S. Litsyn, and R. Zamir, “Lattices which are good for (almost) everything,” *IEEE Transactions on Information Theory*, vol. 51, no. 10, pp. 3401–3416, 2005.

References IV

-  N. di Pietro, J. Boutros, G. Zemor, and L. Brunel, “Integer low-density lattices based on Construction A,” in *2012 IEEE Information Theory Workshop (ITW)*, 2012, pp. 422–426.
-  M.-R. Sadeghi, A. Banihashemi, and D. Panario, “Low-density parity-check lattices: construction and decoding analysis,” *IEEE Transactions on Information Theory*, vol. 52, no. 10, pp. 4481–4495, 2006.
-  A. Sakzad, M.-R. Sadeghi, and D. Panario, “Construction of turbo lattices,” in *2010 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2010, pp. 14–21.
-  Y. Yan, C. Ling, and X. Wu, “Polar lattices: where Arikan meets Forney,” in *2013 IEEE International Symposium on Information Theory (ISIT)*, 2013, pp. 1292–1296.

-  N. Sommer, M. Feder, and O. Shalvi, “Low-density lattice codes,” *IEEE Transactions on Information Theory*, vol. 54, no. 4, pp. 1561–1585, 2008.
-  N. di Pietro, G. Zemor, and J. Boutros, “New results on Construction-A lattices based on very sparse parity-check matrices,” in *2013 IEEE International Symposium on Information Theory (ISIT)*, 2013, pp. 1675–1679.
-  N. di Pietro, J. Boutros, G. Zemor, and L. Brunei, “New results on low-density integer lattices,” in *2013 Information Theory and Applications Workshop (ITA)*, 2013, pp. 1–6.
-  N. Tunali, K. Narayanan, and H. Pfister, “Spatially-coupled low density lattices based on Construction A with applications to compute-and-forward,” in *Information Theory Workshop (ITW), 2013 IEEE*, 2013, pp. 1–5.

References VI



N. di Pietro, “On infinite and finite lattice constellations for the additive white Gaussian noise channel,” [PhD thesis](#), University of Bordeaux, 2014.



S. Vatedka and N. Kashyap, “Nested lattice codes for secure bidirectional relaying with asymmetric channel gains,” in [IEEE Information Theory Workshop, Jerusalem, Israel, 2015](#).