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
Lattices for communication over Gaussian channels

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
Lattices in $\mathbb{R}^n$

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

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

Let $X \sim \text{Unif}(\mathcal{V}(\Lambda))$. Then, $G(\Lambda) = \frac{1}{\text{vol}(\mathcal{V}(\Lambda))^{2/n}} \times \frac{1}{n} \mathbb{E} \|X\|_2^{3/2}$.
Lattices in $\mathbb{R}^n$

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

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

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

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

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

Packing radius: $r_{\text{pack}}(\Lambda)$
Effective radius: $r_{\text{eff}}(\Lambda)$
Lattices in $\mathbb{R}^n$

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, $r_{\text{pack}}(\Lambda) \leq r_{\text{eff}}(\Lambda) \leq r_{\text{cov}}(\Lambda)$
Lattices in $\mathbb{R}^n$

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

$$G(\Lambda) = \frac{1}{\text{vol}(\mathcal{V}(\Lambda))^{2/n}} \times \frac{1}{n} \mathbb{E} \left\| X \right\|^2$$
Components of a lattice code

Lattice $\Lambda$
(In general, could be a coset)

Shaping region $S$
Convex set

Lattice code: $C = \Lambda \cap S$
Nested lattice codes

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

$\Lambda_0$: coarse lattice  $\Lambda$: fine lattice
Nested lattice codes

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

$\Lambda_0$: coarse lattice     $\Lambda$: fine lattice

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

$$R = \frac{1}{n} \log |\Lambda \cap \mathcal{V}(\Lambda_0)|$$

$$= \frac{1}{n} \log \frac{\text{vol}(\mathcal{V}(\Lambda_0))}{\text{vol}(\mathcal{V}(\Lambda))}$$
Nested lattice codes

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

$\Lambda_0$: coarse lattice \hspace{1cm} $\Lambda$: fine lattice

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

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

With dithered transmission:

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

With CLP decoding: $P_e = \text{Pr}[Z_{\text{noise}} \notin \mathcal{V}(\Lambda)]$. 
Properties that we are looking for

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

- **packing** if

\[
\lim_{n \to \infty} \frac{r_{\text{pack}}(\Lambda^{(n)})}{r_{\text{eff}}(\Lambda^{(n)})} \geq \frac{1}{2}.
\]
Properties that we are looking for

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

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

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

\( \text{channel coding} \) if \( \Pr[Z^{(n)} / \in V(\Lambda^{(n)})] \to 0 \) as \( n \to \infty \) for every semi norm-ergodic noise (e.g., AWGN) vectors \( Z^{(n)} \) with \( \sigma^2 := \frac{1}{n} \mathbb{E} \| Z^{(n)} \| \) that satisfy \( \frac{\text{vol}(\Lambda^{(n)})^2}{n^2 \pi e \sigma^2} > 1 \).
Properties that we are looking for

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

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

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

- covering if \( \lim_{n \to \infty} \frac{r_{\text{cov}}(\Lambda^{(n)})}{r_{\text{eff}}(\Lambda^{(n)})} = 1 \).
Properties that we are looking for

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

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

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

for every semi norm-ergodic noise (e.g., AWGN) vectors \( Z^{(n)} \)

with \( \sigma^2 := \frac{1}{n} \mathbb{E} \|Z^{(n)}\| \) 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; Vatedka et al. 2014).
Construction A

Let $C$ be an $(n, k)$ linear code over $\mathbb{F}_p$, for prime $p$. The Construction-A lattice $\Lambda_A(C)$ is defined as

$$\Lambda_A(C) = \{ x \in \mathbb{Z}^n : x \equiv c \mod p \text{ for some } c \in C \}.$$
Construction A

Let $C$ be an $(n, k)$ linear code over $\mathbb{F}_p$, for prime $p$. The Construction-A lattice $\Lambda_A(C)$ is defined as

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

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

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

\begin{figure}
\end{figure}
Construction A

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

The Construction-A lattice $\Lambda_A(C)$ is defined as

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

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

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

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

The Construction-A lattice $\Lambda_A(C)$ is defined as

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

Considering $\{0, 1, \ldots, p - 1\}$ to a subset of $\mathbb{Z}$, we may view $C$ as a subset of $\mathbb{Z}^n$. Then,

$$
\Lambda_A(C) = C + p\mathbb{Z}^n.
$$

Example: $C$ 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 \(n \to \infty\).
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 \(n \to \infty\).

How do we decode??
Lattices with Low Decoding Complexity

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


- **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 \((\Delta_V, \Delta_C)\)-regular LDPC codes to obtain Construction-A lattices. We can then use BP decoding!

- \((\text{di Pietro et al. 2012})\): introduced logarithmic degree LDA lattices, showed goodness for channel coding.
- \((\text{di Pietro et al. 2013a})\): constant degree LDA lattices are good for channel coding.
- \((\text{di Pietro et al. 2013b})\) and \((\text{Tunali et al. 2013})\): simulations showing that LDA lattices go close to Poltyrev limit with BP decoding.
- \((\text{di Pietro 2014})\): 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 $\epsilon, \vartheta$, and $\alpha \leq A$ and $\beta \leq B$ such that

- **Left vertex expansion:**
  
  for any $S \subset L \mid |S| \leq \lceil \epsilon n \rceil \Rightarrow |N(S)| \geq A |S|$

  
  $|S| \leq \lceil n (1 - R) \rceil^\alpha \Rightarrow |N(S)| \geq \alpha |S|$

- **Right vertex expansion:**
  
  for any $T \subset R \mid |T| \leq \vartheta n (1 - R) = \Rightarrow |N(T)| \geq B |T|$

  
  $|T| \leq n (1 - R)^2 = \Rightarrow |N(T)| \geq \beta |T|$
To obtain “good” lattices, we want the Tanner graph of the underlying LDPC code to satisfy certain expansion properties:

There exist positive constants $\epsilon, \vartheta$, and $\alpha \leq A$ and $\beta \leq B$ such that

**Left vertex expansion:** for any $S \subset \mathcal{L}$
- $|S| \leq \lceil \epsilon n \rceil \implies |N(S)| \geq A|S|.$
- $|S| \leq \left\lfloor \frac{n(1-R)}{2\alpha} \right\rfloor \implies |N(S)| \geq \alpha|S|$
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 $\epsilon, \vartheta, \text{ and } \alpha \leq A$ 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 $n \to \infty$.

Throughout, we assume that the hypothesis is satisfied, and the Tanner graph is a good expander.
The \((G, \lambda)\) ensemble of LDA lattices

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

Pick a \((\Delta_V, \Delta_V(1 - R))\)-regular \(G\) 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 $C_0$ and $C$, with $C_0 \subset C$.

Then,

$$\Lambda = \Lambda_A(C) \text{ and } \Lambda_0 = \Lambda_A(C_0).$$
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 $\Lambda$ be a lattice chosen uniformly at random from a $(G, \lambda)$ 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 $\Lambda$ is good for channel coding tends to 1 as $n \to \infty$. 
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 \( \Lambda \) be a lattice chosen uniformly at random from a \((G, \lambda)\) LDA ensemble. If

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

then the probability that \( \Lambda \) is good for channel coding tends to 1 as \( n \to \infty \).
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 \( \Lambda \) be a lattice chosen uniformly at random from a \((G, \lambda)\) LDA ensemble. If

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

then the probability that \( \Lambda \) is good for channel coding tends to 1 as \( n \to \infty \).

Also, (di Pietro 2014) found sufficient conditions on parameters for nested LDA lattices to achieve capacity of AWGN channel.
Proofs of channel coding goodness and packing goodness are very similar.

**Theorem (Vatedka & Kashyap, ITW 15)**

Let $\Lambda$ be a lattice chosen uniformly at random from a $(\mathcal{G}, \lambda)$ LDA ensemble, Furthermore, let

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

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

\[ a \quad p \approx n^\lambda \]
Proofs of channel coding goodness and packing goodness are very similar.

**Theorem (Vatedka & Kashyap, ITW 15)**

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

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

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

\(^a\) $p \approx n^\lambda$
Goodness for MSE quantization

Theorem (Vatedka & Kashyap, ITW 15)

Suppose

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

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

\(^a\) \( p \approx n^\lambda \)
Goodness for MSE quantization

Theorem (Vatedka & Kashyap, ITW 15)

Suppose

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

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

\[ a \quad p \approx n^\lambda \]
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 $(G, \lambda)$ LDA ensemble is good for packing with probability tending to 1 as $n \to \infty$. 
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

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

then the dual of a randomly chosen lattice from a $(\mathcal{G}, \lambda)$ LDA ensemble is good for packing with probability tending to 1 as $n \to \infty$. 
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 $\sim 10000$) 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


References II


