Projections of the cubic lattice and applications

Antonio Campello

University of Campinas, Brazil

Workshop on Algebraic Coding Theory, EPFL

September 8, 2011
Summary
Summary

- Motivation
Summary

- Motivation
- A central result
Summary

- Motivation
- A central result
- Dense projection-lattices
Summary

- Motivation
- A central result
- Dense projection-lattices
- Extensions/Applications
Definitions

A lattice $\Lambda$ is a discrete set of points of the form:

$$\Lambda = \{ \alpha_1 b_1 + \ldots + \alpha_m b_m \mid \alpha_i \in \mathbb{Z} \},$$

where $b_i \in \mathbb{R}^n$ are linearly independent vectors.
Definitions

A lattice $\Lambda$ is a discrete set of points of the form:

$$\Lambda = \left\{ \alpha_1 b_1 + \ldots + \alpha_m b_m \mid \alpha_i \in \mathbb{Z} \right\},$$

where $b_i \in \mathbb{R}^n$ are linearly independent vectors.

Generator matrix: $B = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}$, Gram matrix: $A = BB^tr$.

The dual lattice $\Lambda^*$ is the set of all $y \in \mathbb{R}^n$ such that

$$\langle x, y \rangle \in \mathbb{Z} \ \forall \ x \in \Lambda.$$
Definitions

Shortest vector: \( \mathbf{x}^* \in \Lambda \) such that \( \| \mathbf{x}^* \| = \min_{0 \neq \mathbf{x} \in \Lambda} \| \mathbf{x} \| = \lambda_1. \)

Density: \[ \frac{\text{Vol. of a sphere of radius } \frac{\lambda_1}{2}}{\text{Vol. of a fundamental region}} = \frac{\text{Vol}(B(\frac{\lambda_1}{2}))}{\sqrt{\text{det } A}} \]
Definitions

Shortest vector: $x^* \in \Lambda$ such that $\|x^*\| = \min_{0 \neq x \in \Lambda} \|x\| = \lambda_1$.

Density: \[
\frac{\text{Vol. of a sphere of radius } \lambda_1/2}{\text{Vol. of a fundamental region}} = \frac{\text{Vol}(B(\lambda_1/2))}{\sqrt{\det A}}
\]

Two lattices $\in \mathbb{R}^n$ with generator matrices $G_1$ and $G_2$ are equivalent if there is $U$, $Q$ and $c$ such that $G_1 = cU G_2 Q$. 
Definitions

The cubic lattice $\mathbb{Z}^n$ has generator/Gram matrix equal to the identity matrix $I_n$. Its projection onto the hyperplane $\langle x, v \rangle = 0$, $v \in \mathbb{Z}^n$ is an $(n - 1)$-dimensional lattice.
Definitions

The cubic lattice $\mathbb{Z}^n$ has generator/Gram matrix equal to the identity matrix $I_n$. Its projection onto the hyperplane $\langle x, v \rangle = 0$, $v \in \mathbb{Z}^n$ is an $(n - 1)$-dimensional lattice.
Definitions

The cubic lattice $\mathbb{Z}^n$ has generator/Gram matrix equal to the identity matrix $I_n$. Its projection onto the hyperplane $\langle x, v \rangle = 0$, $v \in \mathbb{Z}^n$ is an $(n - 1)$-dimensional lattice.
Definitions

The cubic lattice $\mathbb{Z}^n$ has generator/Gram matrix equal to the identity matrix $I_n$. Its projection onto the hyperplane $\langle x, v \rangle = 0$, $v \in \mathbb{Z}^n$ is an $(n - 1)$-dimensional lattice.

Density = $K(\lambda_1/2)^{n-1} \|v\|$
Definitions

The cubic lattice \( \mathbb{Z}^n \) has generator/Gram matrix equal to the identity matrix \( \mathbf{I}_n \). Its projection onto the hyperplane \( \langle \mathbf{x}, \mathbf{v} \rangle = 0 \), \( \mathbf{v} \in \mathbb{Z}^n \) is an \( (n-1) \)-dimensional lattice.

Density = \( K(\lambda_1/2)^{n-1} \|\mathbf{v}\| \)

What is the maximum possible density?
Motivation

“Curves on a sphere, shift-map dynamics, and error control for continuous alphabet sources” [V. Vaishampayan and S. Costa, 2003]

Codes continuous alphabet source + AWGN channel $\rightarrow$ curves in $N$-dimensional Euclidean space.
Motivation

“Curves on a sphere, shift-map dynamics, and error control for continuous alphabet sources” [V. Vaishampayan and S. Costa, 2003]

Codes continuous alphabet source + AWGN channel $\rightarrow$ curves in $N$-dimensional Euclidean space.

$$f(x) = \Phi \left( \frac{2\pi}{\sqrt{n}} ax \right), \ a \in \mathbb{Z}^n,$$

where

$$\Phi : \mathbb{R}^n \rightarrow \mathbb{R}^{2n}$$

$$\Phi(u) = \frac{1}{\sqrt{n}}(\cos(\sqrt{n}u_1), \sin(\sqrt{n}u_1), \ldots, \cos(\sqrt{n}u_n), \sin(\sqrt{n}u_n))$$

$f(x)$ is a curve
Motivation

“Curves on a sphere, shift-map dynamics, and error control for continuous alphabet sources” [V. Vaishampayan and S. Costa, 2003]

Codes continuous alphabet source + AWGN channel $\rightarrow$ curves in $N$-dimensional Euclidean space.

\[
f(x) = \Phi \left( \frac{2\pi}{\sqrt{n}} a x \right), \quad a \in \mathbb{Z}^n, \text{ where}
\]

\[
\Phi : \mathbb{R}^n \rightarrow \mathbb{R}^{2n}
\]

\[
\Phi(u) = \frac{1}{\sqrt{n}} (\cos(\sqrt{nu_1}), \sin(\sqrt{nu_1}), \ldots, \cos(\sqrt{nu_n}), \sin(\sqrt{nu_n}))
\]

$f(x)$ is a curve on a torus
Motivation

“Curves on a sphere, shift-map dynamics, and error control for continuous alphabet sources” [V. Vaishampayan and S. Costa, 2003]

Codes continuous alphabet source $+$ AWGN channel $\rightarrow$ curves in $N$-dimensional Euclidean space.

$$f(x) = \Phi \left( \frac{2\pi}{\sqrt{n}} ax \right), \ a \in \mathbb{Z}^n,$$

where

$$\Phi : \mathbb{R}^n \rightarrow \mathbb{R}^{2n}$$

$$\Phi(u) = \frac{1}{\sqrt{n}} (\cos(\sqrt{nu_1}), \sin(\sqrt{nu_1}), \ldots, \cos(\sqrt{nu_n}), \sin(\sqrt{nu_n}))$$

$f(x)$ is a curve on a torus on a sphere $\in \mathbb{R}^{2n}$. 
Motivation

Performance:

\[ \frac{2\pi}{\sqrt{n}} \parallel a \parallel \]

The minimum distance (between laps) can be approximated by

\[ \Delta a = \min_{v \neq k a, k \in \mathbb{Z}} \parallel a - v \parallel = \min_{v \neq k a, k \in \mathbb{Z}} \parallel \text{Proj}_{a \perp} v \parallel \]

Shortest non-zero vector of the lattice which is the projection of \( \mathbb{Z}^n \) onto \( a \perp \).
Motivation

Performance:

- *Stretch* of the curve \((2\pi/\sqrt{n}) \|a\|\)
Motivation

Performance:

➢ *Stretch* of the curve \((2\pi/\sqrt{n})\|a\|

➢ *Minimum distance* \(\delta_a\).

The minimum distance (between laps) can be approximated by

\[
\Delta a = \min_{v \neq k a, k \in \mathbb{Z}} \|a - v\| = \min_{v \neq k a, k \in \mathbb{Z}} \|\text{Proj}_{a^\perp}v\|
\]

Shortest non-zero vector of the lattice which is the projection of \(\mathbb{Z}_n\) onto \(a^\perp\).
Motivation

Performance:

- *Stretch* of the curve \((2\pi/\sqrt{n}) \|a\|
- *Minimum distance* \(\delta_a\).

The minimum distance (between laps) can be approximated by

\[
\Delta_a = \min_{v \neq ka, k \in \mathbb{Z}} \min_{x} \|ax - v\|
\]

\[
= \min_{v \neq ka, k \in \mathbb{Z}} \|\text{Proj}_{a^\perp} v\|
\]

Shortest non-zero vector of the lattice which is the projection of \(\mathbb{Z}^n\) onto \(a^\perp\).
Motivation

Performance:

- *Stretch* of the curve \( \frac{2\pi}{\sqrt{n}} \|a\| \)
- *Minimum distance* \( \delta_a \).

The minimum distance (between laps) can be approximated by

\[
\Delta_a = \min_{v \neq ka, k \in \mathbb{Z}} \min_x \|ax - v\|
\]

\[
= \min_{v \neq ka, k \in \mathbb{Z}} \|\text{Proj}_{a^\perp}v\|
\]

Shortest non-zero vector of the lattice which is the projection of \( \mathbb{Z}^n \) onto \( a^\perp \).

Objective

*Maximize* \( \Delta_a \) s.t. \( \|a\| \geq l_0 \Rightarrow \) Maximize the density of the projection-lattice.
A central result

“A note on projecting the cubic lattice” [N. Sloane, V. Vaishampayan and S. Costa, 2010, Discrete and Computational Geometry]
A central result

“A note on projecting the cubic lattice” [N. Sloane, V. Vaishampayan and S. Costa, 2010, Discrete and Computational Geometry]

Theorem (Informal)

Every \( (n-1) \)-dimensional lattice \( \Lambda \) can be approximated by a sequence of lattices which are, up to similarity, projections of \( \mathbb{Z}^n \) onto \( a \perp \) for an integer vector \( a \).
A central result

“A note on projecting the cubic lattice” [N. Sloane, V. Vaishampayan and S. Costa, 2010, Discrete and Computational Geometry]

Theorem (Informal)

Every \((n - 1)\)-dimensional lattice \(\Lambda\) can be approximated by a sequence of lattices which are, up to similarity, projections of \(\mathbb{Z}^n\) onto \(a^\perp\) for an integer vector \(a\).

Idea of the proof: Sequence of lattices \(\Lambda_w^*\) converging to the dual of \(\Lambda\) and such that each \(\Lambda_w^*\) is the dual of a projection-lattice. Lift the target lattice to \(\mathbb{Z}^n\).
A central result

Theorem

Let $\Lambda$ be an $(n - 1)$-dimensional lattice with Gram matrix $A$. For any $\epsilon > 0$, there exist a nonzero vector $v \in \mathbb{Z}^n$, a basis $B$ for the $(n - 1)$-dimensional lattice $\Lambda_v$ and a number $c$ such that if $A_v$ denotes the Gram matrix of $B$, then

$$\|A - cA_v\|_\infty < \epsilon$$
A central result

**Theorem**

Let \( \Lambda \) be an \((n - 1)\)-dimensional lattice with Gram matrix \( A \). For any \( \varepsilon > 0 \), there exist a nonzero vector \( \mathbf{v} \in \mathbb{Z}^n \), a basis \( B \) for the \((n - 1)\)-dimensional lattice \( \Lambda_\mathbf{v} \) and a number \( c \) such that if \( A_\mathbf{v} \) denotes the Gram matrix of \( B \), then

\[
\| A - cA_\mathbf{v} \|_\infty < \varepsilon
\]

In fact, \( \| A - cA_\mathbf{v} \|_\infty = O \left( \frac{1}{\| \mathbf{v} \|^{1/(n-1)}} \right) \).
Can we do better?
Can we do better?

Idea: perturbations of the original sequences with matrices of small entries, ensuring

- The sequence still converges to the dual of the target lattice
Can we do better?

Idea: perturbations of the original sequences with matrices of small entries, ensuring

- The sequence still converges to the dual of the target lattice
- Each element is still the dual of a projection-lattice
Can we do better?

Idea: perturbations of the original sequences with matrices of small entries, ensuring

- The sequence still converges to the dual of the target lattice
- Each element is still the dual of a projection-lattice

\[ \| A - cA_v \|_\infty = O \left( \frac{1}{\| v \|^{2/(n-1)}} \right) \]
A toy example. Target lattice: $\Lambda = \mathbb{Z} \oplus 2\mathbb{Z}$

$$G_w = \begin{bmatrix} w & 1 & 0 \\ 0 & 2w & 1 \end{bmatrix} \sim \begin{bmatrix} w & 1 & 0 \\ -2w^2 & 0 & 1 \end{bmatrix} \therefore v = (1, -w, 2w^2)$$
A toy example. Target lattice: \( \Lambda = \mathbb{Z} \oplus 2\mathbb{Z} \)

\[
G_w = \begin{bmatrix} w & 1 & 0 \\ 0 & 2w & 1 \end{bmatrix} \sim \begin{bmatrix} w & 1 & 0 \\ -2w^2 & 0 & 1 \end{bmatrix} \therefore v = (1, -w, 2w^2)
\]

\[
\left\| G \cdot G^t - \frac{1}{w^2} G_w \cdot G_w^t \right\|_\infty = \frac{2}{w} = O \left( \frac{1}{\|v\|^{1/2}} \right)
\]
A toy example. Target lattice: $\Lambda = \mathbb{Z} \oplus 2\mathbb{Z}$

$$G_w = \begin{bmatrix} w & 1 & 0 \\ 0 & 2w & 1 \end{bmatrix} \sim \begin{bmatrix} w & 1 & 0 \\ -2w^2 & 0 & 1 \end{bmatrix} \therefore v = (1, -w, 2w^2)$$

$$\left\| G.G^t - \frac{1}{w^2} G_w.G^t \right\|_\infty = \frac{2}{w} = O \left( \frac{1}{\|v\|^{1/2}} \right)$$

Now, take

$$G_w = \begin{bmatrix} w & 1 & 0 \\ -2 & 2w & 1 \end{bmatrix} \sim \begin{bmatrix} w & 1 & 0 \\ -2w^2 - 2 & 0 & 1 \end{bmatrix} \therefore v = (1, -w, 2w^2+2)$$
A toy example. Target lattice: $\Lambda = \mathbb{Z} \oplus 2\mathbb{Z}$

\[
G_w = \begin{bmatrix}
  w & 1 & 0 \\
  0 & 2w & 1 \\
\end{bmatrix} \sim \begin{bmatrix}
  w & 1 & 0 \\
  -2w^2 & 0 & 1 \\
\end{bmatrix} \therefore v = (1, -w, 2w^2)
\]

\[
\left\| G.G^t - \frac{1}{w^2} G_w.G_w^t \right\|_\infty = \frac{2}{w} = O\left(\frac{1}{\|v\|^{1/2}}\right)
\]

Now, take

\[
G_w = \begin{bmatrix}
  w & 1 & 0 \\
  -2 & 2w & 1 \\
\end{bmatrix} \sim \begin{bmatrix}
  w & 1 & 0 \\
  -2w^2 - 2 & 0 & 1 \\
\end{bmatrix} \therefore v = (1, -w, 2w^2 + 2)
\]

\[
\left\| G.G^t - \frac{1}{w^2} G_w.G_w^t \right\|_\infty = \frac{5}{w^2} = O\left(\frac{1}{\|v\|}\right)
\]
A sufficient condition

Let $G = [\bar{G} \ 0]$ be a generator matrix for the target lattice and $A = G G^t$. Consider the optimization problem

$$
\min \| G P^t A + A P G^t - \alpha A \|
$$

s. t. $| \det H_w | = 1$, $\forall w \in \mathbb{N}$  \hspace{1cm} (1)

$P \in \mathbb{Z}^{n-1 \times n}$

$\alpha \in \mathbb{Z}$,

for $H_w = (wG^* + P)_{(1,\ldots,n-1),(2,\ldots,n)}$. If the minimum is zero, then we can construct an $O(1/ \|v\|^{2/(n-1)})$ sequence.
Explicit constructions

Explicit constructions for some lattices, such as $D_n$, $D_n^*$, $E_7$, $E_8$. Different solutions.
Explicit constructions

Explicit constructions for some lattices, such as $D_n, D_n^*, E_7, E_8$. Different solutions. Example: $E_8$
Explicit constructions

Explicit constructions for some lattices, such as $D_n$, $D_n^*$, $E_7$, $E_8$. Different solutions. Example: $E_8$

Can we do even better?
Explicit constructions

Explicit constructions for some lattices, such as $D_n$, $D^*_n$, $E_7$, $E_8$. Different solutions. Example: $E_8$

Can we do even better? I don’t know.
Extensions

Back to the continuous alphabet source problem...
Extensions

Back to the continuous alphabet source problem...

How can we improve the performance by setting appropriated curves on other surfaces on the Euclidean sphere? (other flat tori)
Extensions

Back to the continuous alphabet source problem...

How can we improve the performance by setting appropriated curves on other surfaces on the Euclidean sphere? (other flat tori)

In progress.
Applications

Given a received vector $x_0$, CVP problem (for projection-lattices)...

What about general lattices?
Applications

Given a received vector $x_0$, CVP problem (for projection-lattices)...

... is equivalent to find the distance from $\mathbb{Z}^n$ to the straight line $x_0 + tv$. 
Applications

Given a received vector $\mathbf{x}_0$, CVP problem (for projection-lattices)...
... is equivalent to find the distance from $\mathbb{Z}^n$ to the straight line $\mathbf{x}_0 + t\mathbf{v}$.
Applications

Given a received vector $x_0$, CVP problem (for projection-lattices)... ... is equivalent to find the distance from $\mathbb{Z}^n$ to the straight line $x_0 + tv$.

What about general lattices?
Merci!