Construction-D lattice from Garcia-Stichtenoth tower code

Elena Kirshanova [1]
based on joint work with E. Malygina[2]

[1]Technology Innovation Institute, [2]I.Kant Baltic Federal University

AGC^{2}T 2023
Center International de Rencontres Mathématique (CIRM), Luminy

Agenda

Part I. Lattice constructions from codes

Part II. Construction-D lattices

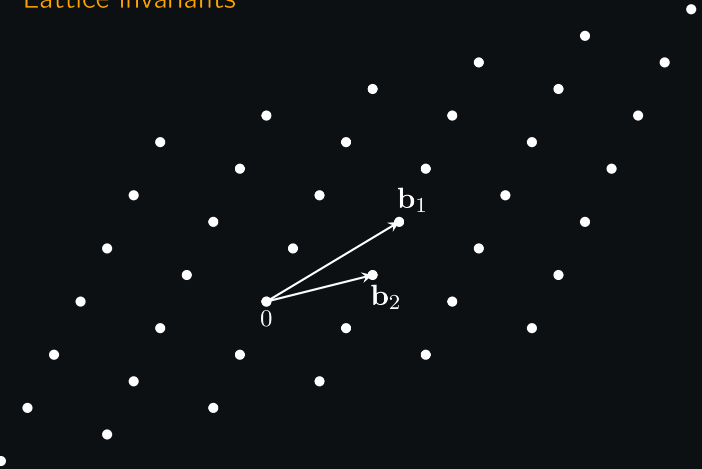
Part III. Garcia-Stichtenoth tower code

Part IV. Construction-D lattice from GS tower code

Part I

Lattice constructions from codes

Lattice invariants



A lattice is a set $\Lambda = \{\sum_{i \leq n} x_i \mathbf{b}_i \ : \ x_i \in \mathbb{Z}\}$ for linearly independent $\mathbf{b}_i \in \mathbb{R}^n$.
$\{\mathbf{b}_i\}_i$ is a basis of Λ

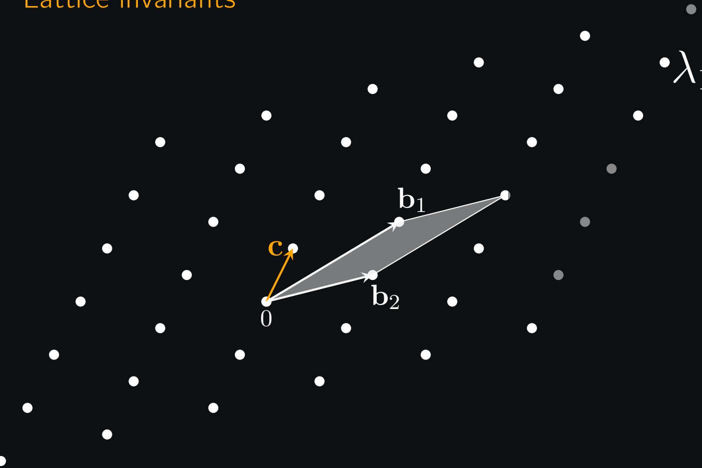
Lattice invariants

Minimum

$$\lambda_1(\Lambda) = \min_{\mathbf{v}\in\Lambda\setminus\mathbf{0}} \|\mathbf{v}\|_2$$

A lattice is a set $\Lambda = \{\sum_{i\leq n} x_i \mathbf{b}_i \ : \ x_i \in \mathbb{Z}\}$ for linearly independent $\mathbf{b}_i \in \mathbb{R}^n$.
$\{\mathbf{b}_i\}_i$ is a basis of Λ

Lattice invariants



Minimum

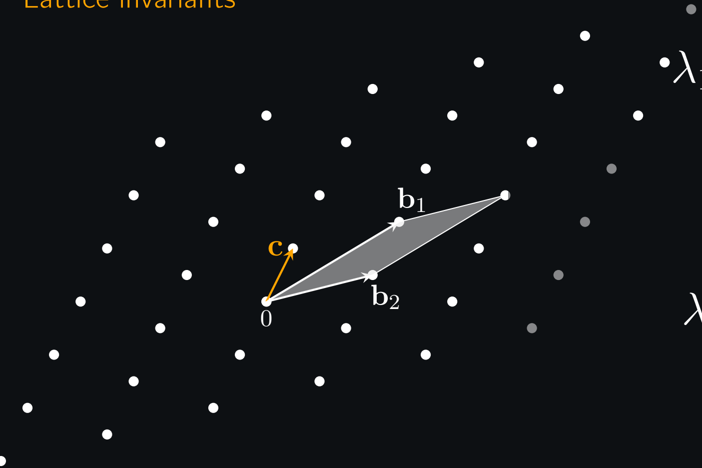
$$\lambda_1(\Lambda) = \min_{\mathbf{v} \in \Lambda \setminus \mathbf{0}} \|\mathbf{v}\|_2$$

Determinant

$$\det(\Lambda) = |\det(\mathbf{b}_i)_i|$$

A lattice is a set $\Lambda = \{\sum_{i \le n} x_i \mathbf{b}_i \; : \; x_i \in \mathbb{Z}\}$ for linearly independent $\mathbf{b}_i \in \mathbb{R}^n$.
$\{\mathbf{b}_i\}_i$ is a basis of Λ

Lattice invariants



Minimum

$$\lambda_1(\Lambda) = \min_{\mathbf{v}\in\Lambda\setminus\mathbf{0}} \|\mathbf{v}\|_2$$

Determinant

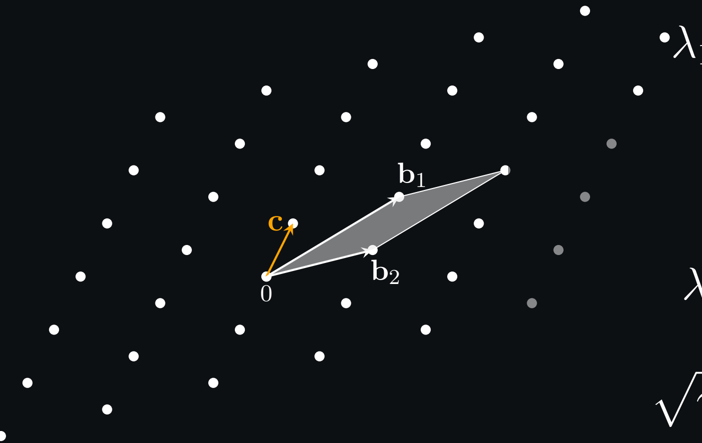
$$\det(\Lambda) = |\det(\mathbf{b}_i)_i|$$

Minkowski bound

$$\lambda_1(\Lambda) \leq \sqrt{n}\cdot\det(\Lambda)^{\frac{1}{n}}$$

A lattice is a set $\Lambda = \{\sum_{i\leq n} x_i\mathbf{b}_i \ : \ x_i \in \mathbb{Z}\}$ for linearly independent $\mathbf{b}_i \in \mathbb{R}^n$.
$\{\mathbf{b}_i\}_i$ is a basis of Λ

Lattice invariants



Minimum

$$\lambda_1(\Lambda) = \min_{\mathbf{v}\in\Lambda\setminus\mathbf{0}} \|\mathbf{v}\|_2$$

Determinant

$$\det(\Lambda) = |\det(\mathbf{b}_i)_i|$$

Minkowski bound

$$\lambda_1(\Lambda) \leq \sqrt{n}\cdot\det(\Lambda)^{\frac{1}{n}}$$

Normalized min. distance

$$\sqrt{\gamma(\Lambda)} = \lambda_1(\Lambda)/\det(\Lambda)^{\frac{1}{n}}$$

A lattice is a set $\Lambda = \{\sum_{i\leq n} x_i\mathbf{b}_i \ : \ x_i \in \mathbb{Z}\}$ for linearly independent $\mathbf{b}_i \in \mathbb{R}^n$.
$\{\mathbf{b}_i\}_i$ is a basis of Λ

Our goal

$$\sqrt{\gamma(\Lambda)} = \lambda_1(\Lambda)/\det(\Lambda)^{\frac{1}{n}} \leq \sqrt{n}$$

We are interested in

1. explicit construction of a lattice with as large $\gamma(\Lambda)$ as possible
2. with an efficient (list-) decoding algorithm (runtime at most $\mathrm{poly}(n)$).

Our goal

$$\sqrt{\gamma(\Lambda)} = \lambda_1(\Lambda)/\det(\Lambda)^{\frac{1}{n}} \leq \sqrt{n}$$

We are interested in

1. explicit construction of a lattice with as large $\gamma(\Lambda)$ as possible
2. with an efficient (list-) decoding algorithm (runtime at most $\mathrm{poly}(n)$).

Why? We might want to use lattice as codes, hence we care about their decoding properties.

A ‘random’ lattice (an example will given later) is expected to achieve $\sqrt{\gamma(\Lambda)} \sim \sqrt{n}$, but we do not know how to efficiently decode them.

State-of-the art on $\sqrt{\gamma(\Lambda)}$ ($\Omega()$ for $\sqrt{\gamma(\Lambda)}$ is omitted)

Lattice Λ	$\sqrt{\gamma(\Lambda)}$
Barnes-Wall lattice [BW]	$n^{1/4}$

Defined by the rows of

$$\mathrm{BW}^k = \begin{bmatrix} 1 & 1 \\ 0 & \phi \end{bmatrix}^{\otimes k} \subset \mathbb{C}^{2^k},$$

where $\phi = 1 + i$

State-of-the art on $\sqrt{\gamma(\Lambda)}$ ($\Omega()$ for $\sqrt{\gamma(\Lambda)}$ is omitted)

Lattice Λ	$\sqrt{\gamma(\Lambda)}$
Barnes-Wall lattice [BW]	$n^{1/4}$
Discrete Logarithm Lattices [DP]	$\frac{\sqrt{n}}{\log n}$

For $(\mathbb{Z}/m\mathbb{Z})^\star$,

p_i – primes, $1 \leq i \leq n$

$\phi : \mathbb{Z}^n \to (\mathbb{Z}/m\mathbb{Z})^\star$

$(x_1, \ldots, x_n) \mapsto \prod_{i=1}^n p_i^{x_i}$

$\Lambda_{\text{dlog}} = \ker \phi$.

State-of-the art on $\sqrt{\gamma(\Lambda)}$ ($\Omega()$ for $\sqrt{\gamma(\Lambda)}$ is omitted)

Lattice Λ	$\sqrt{\gamma(\Lambda)}$
Barnes-Wall lattice [BW]	$n^{1/4}$
Discrete Logarithm Lattices [DP]	$\frac{\sqrt{n}}{\log n}$
Construction-D lattice from BCH codes [MP]	$\sqrt{\frac{n}{\log n}}$

To be defined later

State-of-the art on $\sqrt{\gamma(\Lambda)}$ ($\Omega()$ for $\sqrt{\gamma(\Lambda)}$ is omitted)

Lattice Λ	$\sqrt{\gamma(\Lambda)}$
Barnes-Wall lattice [BW]	$n^{1/4}$
Discrete Logarithm Lattices [DP]	$\frac{\sqrt{n}}{\log n}$
Construction-D lattice from BCH codes [MP]	$\sqrt{\frac{n}{\log n}}$
Construction-A lattice from Reed-Solomon codes [BP]	$\sqrt{\frac{n}{\log n}}$

Constriction-A:

Take $B \in (\mathbb{Z}/q\mathbb{Z})^{n\times m}$ – a generator matrix of a code.

$\Lambda_{\mathsf{A}} = \mathbb{Z}^n B + q\mathbb{Z}^m \subset \mathbb{Z}^m$ is a construction-A lattice.

State-of-the art on $\sqrt{\gamma(\Lambda)}$ ($\Omega()$ for $\sqrt{\gamma(\Lambda)}$ is omitted)

Lattice Λ	$\sqrt{\gamma(\Lambda)}$
Barnes-Wall lattice [BW]	$n^{1/4}$
Discrete Logarithm Lattices [DP]	$\frac{\sqrt{n}}{\log n}$
Construction-D lattice from BCH codes [MP]	$\sqrt{\frac{n}{\log n}}$
Construction-A lattice from Reed-Solomon codes [BP]	$\sqrt{\frac{n}{\log n}}$
Construction-D lattice from subfield subcodes of Garcia-Stichtenoth codes [KM]	$\frac{\sqrt{n}}{(\log n)^{\varepsilon+o(1)}}$

This work

Main result

Theorem: For a constant $\varepsilon > 0$, there is a family of lattices $\mathcal{L} \subset \mathbb{R}^n$ with normalized minimum distance

$$\frac{\lambda_1(\Lambda)}{\det(\Lambda)^{1/n}} = \Omega\left(\frac{\sqrt{n}}{(\log n)^{\varepsilon+o(1)}}\right).$$

These lattices are list decodable to within distance $\sqrt{1/2} \cdot \lambda_1(\Lambda)$ in $\mathrm{poly}(n)$ time.

Part II

Construction-D lattices

Construction-D lattice: Definition

- Fix an integer $L \geq 0$, let

$$C_L \subseteq C_{L-1} \subseteq \ldots \subseteq C_1 \subseteq C_0 = \mathbb{F}_p^n$$

  be a tower of p-ary codes of length n, where $\dim(C_i) = k_i$.

Construction-D lattice: Definition

- Fix an integer $L \geq 0$, let
$$C_L \subseteq C_{L-1} \subseteq \ldots \subseteq C_1 \subseteq C_0 = \mathbb{F}_p^n$$
be a tower of p-ary codes of length n, where $\dim(C_i) = k_i$.
- Let $\mathbf{b}_1, \ldots, \mathbf{b}_n$ be a basis of $\mathbb{F}_p^n$ such that
  1. $\mathbf{b}_1, \ldots, \mathbf{b}_{k_i}$ is a basis of C_i for all $i = 0, \ldots, L$, and
  2. some permutation of $\mathbf{b}_1, \ldots, \mathbf{b}_n$ forms an upper-triangular matrix.

Construction-D lattice: Definition

- Fix an integer $L \geq 0$, let

$$C_L \subseteq C_{L-1} \subseteq \ldots \subseteq C_1 \subseteq C_0 = \mathbb{F}_p^n$$

  be a tower of p-ary codes of length n, where $\dim(C_i) = k_i$.
- Let $\mathbf{b}_1, \ldots, \mathbf{b}_n$ be a basis of $\mathbb{F}_p^n$ such that
  1. $\mathbf{b}_1, \ldots, \mathbf{b}_{k_i}$ is a basis of C_i for all $i = 0, \ldots, L$, and
  2. some permutation of $\mathbf{b}_1, \ldots, \mathbf{b}_n$ forms an upper-triangular matrix.
- Define a set of distinguished $\mathbb{Z}^n$ representatives of $\mathbf{c}_i = \sum_{j=1}^{k_i} a_j \mathbf{b}_j \in C_i$ as

$$\overline{\mathbf{c}}_i = \sum_{j=1}^{k_i} \overline{a}_j \overline{\mathbf{b}}_j \in \mathbb{Z}^n \quad \text{where } \overline{a}_j \in \{0, \ldots p-1\} \subset \mathbb{Z}.$$

Construction-D lattice: Definition

- Fix an integer $L \geq 0$, let
$$C_L \subseteq C_{L-1} \subseteq \ldots \subseteq C_1 \subseteq C_0 = \mathbb{F}_p^n$$
be a tower of p-ary codes of length n, where $\dim(C_i) = k_i$.
- Let $\mathbf{b}_1, \ldots, \mathbf{b}_n$ be a basis of $\mathbb{F}_p^n$ such that
  1. $\mathbf{b}_1, \ldots, \mathbf{b}_{k_i}$ is a basis of C_i for all $i = 0, \ldots, L$, and
  2. some permutation of $\mathbf{b}_1, \ldots, \mathbf{b}_n$ forms an upper-triangular matrix.
- Define a set of distinguished $\mathbb{Z}^n$ representatives of $\mathbf{c}_i = \sum_{j=1}^{k_i} a_j \mathbf{b}_j \in C_i$ as
$$\overline{\mathbf{c}}_i = \sum_{j=1}^{k_i} \overline{a}_j \overline{\mathbf{b}}_j \in \mathbb{Z}^n \quad \text{where } \overline{a}_j \in \{0, \ldots p-1\} \subset \mathbb{Z}.$$
- Let $\mathcal{L}_0 = \mathbb{Z}^n$, and for each $i = 1, \ldots, L$ define
$$\Lambda_i = \overline{C}_i + p\Lambda_{i-1}, \quad \overline{C}_i = \{\overline{c}_i \ : \ c_i \in C_i\}.$$
- The construction-D for the tower $\{C_i\}$ is $\Lambda = \Lambda_L$.

Properties of construction-D lattices

For

$$C_L \subseteq C_{L-1} \subseteq \ldots \subseteq C_1 \subseteq C_0 = \mathbb{F}_p^n$$

with $\dim C_i = k_i$ and $d(C_i) \geq p^{2i}$, we know

1. the minimum of $\Lambda = \Lambda_L$: $\lambda_1(\Lambda) = p^L$,
2. an upper bound on the determinant of Λ: $\det(\Lambda) \leq (p-1)^{n-k_L} p^{\sum_{i=1}^{L}(n-k_i)}$

Properties of construction-D lattices

For
$$C_L \subseteq C_{L-1} \subseteq \ldots \subseteq C_1 \subseteq C_0 = \mathbb{F}_p^n$$
with $\dim C_i = k_i$ and $d(C_i) \geq p^{2i}$, we know

1. the minimum of $\Lambda = \Lambda_L$: $\lambda_1(\Lambda) = p^L$,
2. an upper bound on the determinant of Λ: $\det(\Lambda) \leq (p-1)^{n-k_L} p^{\sum_{i=1}^{L}(n-k_i)}$

If we know an efficient list-decoding algorithm for C_i's, then

3. there is an efficient list decoding algorithm on Λ with decoding radius $\Omega(\lambda_1(\Lambda))$.

See a proof for 1. and 2. in E.S. Barnes, N.J.A. Sloane. New lattice packings of spheres.
See an algorithm for 3. in E.Mook, C.Peikert. Lattice (list) decoding near Minkowski's inequality.

Part III

Garcia-Stichtenoth tower code

Definition

Let h in $q = p^h$ be even, hence $q = p^h = r^2$ for $r = p^{h/2}$.

For an integer $e \geq 2$, define the following recursive relations

$$x_{i+1}^r + x_{i+1} = \frac{x_i^r}{x_i^{r-1} + 1}, \quad i = 1, \ldots, e-1.$$

Then $K_e = \mathbb{F}_q(x_1, \ldots, x_e)$ is a function field, and the sequence $K_1, K_2, \ldots$ is known as the Garcia-Stichtenoth tower of function fields.

Definition

Let h in $q = p^h$ be even, hence $q = p^h = r^2$ for $r = p^{h/2}$.

For an integer $e \geq 2$, define the following recursive relations

$$x_{i+1}^r + x_{i+1} = \frac{x_i^r}{x_i^{r-1} + 1}, \quad i = 1, \ldots, e-1.$$

Then $K_e = \mathbb{F}_q(x_1, \ldots, x_e)$ is a function field, and the sequence $K_1, K_2, \ldots$ is known as the Garcia-Stichtenoth tower of function fields.

Properties:

- the genus of K_e is $\mathfrak{g} = \Theta(r^e)$,
- The number of rational points on K_e is $\Omega(r^{e+1})$.

Codes from Garcia-Stichtenoth tower

- $\mathcal{P} = \{P_1, \ldots, P_n\}$ is a set of n distinct rational places of a ff. $F/\mathbb{F}_q$.
- G is a divisor of F such that $\mathsf{supp}(G) \cap \mathcal{P} = \emptyset$. The set

$$C(\mathcal{P}, G) = \{f(P_1), \ldots, f(P_n) : f \in \mathcal{L}(G)\}.$$

defines an n-dimensional $\mathbb{F}_q$-linear code, where $\mathcal{L}$ is the Riemann-Roch space of G.

Codes from Garcia-Stichtenoth tower

- $\mathcal{P} = \{P_1, \ldots, P_n\}$ is a set of n distinct rational places of a ff. $F/\mathbb{F}_q$.
- G is a divisor of F such that $\mathrm{supp}(G) \cap \mathcal{P} = \emptyset$. The set

$$C(\mathcal{P}, G) = \{f(P_1), \ldots, f(P_n) : f \in \mathcal{L}(G)\}.$$

defines an n-dimensional $\mathbb{F}_q$-linear code, where $\mathcal{L}$ is the Riemann-Roch space of G.

Properties of $C(\mathcal{P}, G)$: for $2\mathfrak{g} - 2 < \deg(G) < n$

- dimension $\dim C(\mathcal{P}, G) = \deg(G) - \mathfrak{g} + 1$
- min. distance $d \geq n - \deg(G)$

Codes from Garcia-Stichtenoth tower

- $\mathcal{P} = \{P_1, \ldots, P_n\}$ is a set of n distinct rational places of a ff. $F/\mathbb{F}_q$.
- G is a divisor of F such that $\mathsf{supp}(G) \cap \mathcal{P} = \emptyset$. The set

$$C(\mathcal{P}, G) = \{f(P_1), \ldots, f(P_n) : f \in \mathcal{L}(G)\}.$$

  defines an n-dimensional $\mathbb{F}_q$-linear code, where $\mathcal{L}$ is the Riemann-Roch space of G.

Properties of $C(\mathcal{P}, G)$: for $2\mathfrak{g} - 2 < \deg(G) < n$

- dimension $\dim C(\mathcal{P}, G) = \deg(G) - \mathfrak{g} + 1$
- min. distance $d \geq n - \deg(G)$

Case F is K_e: take $G = \ell P_\infty$ for $\ell > 2r^e - 2$ and $n \approx r^{e+1}$ maximal, obtain

- dimension $\dim C(\mathcal{P}, G) \approx \ell - r^e + 1$
- min. distance $d \geq r^{e+1} - \ell$.

Sequence of codes from Garcia-Stichtenoth tower

To construct

$$C_L \subseteq C_{L-1} \subseteq \ldots \subseteq C_1 \subseteq C_0 = \mathbb{F}_q^n,$$

consider

- a function field K_e of genus $\mathfrak{g}$ for some e,

Sequence of codes from Garcia-Stichtenoth tower

To construct

$$C_L \subseteq C_{L-1} \subseteq \ldots \subseteq C_1 \subseteq C_0 = \mathbb{F}_q^n,$$

consider

- a function field K_e of genus $\mathfrak{g}$ for some e,
- $\{\ell_i\}_i$– a sequence of positive integers satisfying $\ell_i \geq \ell_{i+1}$ for $i = 1, \ldots, L-1$ and $\ell_L > 2\mathfrak{g} - 2$.

Sequence of codes from Garcia-Stichtenoth tower

To construct

$$C_L \subseteq C_{L-1} \subseteq \ldots \subseteq C_1 \subseteq C_0 = \mathbb{F}_q^n,$$

consider

- a function field K_e of genus $\mathfrak{g}$ for some e,
- $\{\ell_i\}_i$– a sequence of positive integers satisfying $\ell_i \geq \ell_{i+1}$ for $i = 1, \ldots, L-1$ and $\ell_L > 2\mathfrak{g} - 2$.
- Then $C_i = C(\mathcal{P}, \ell_i P_\infty)$ are $\mathbb{F}_q$-linear codes with
  - $C_{i+1} \subseteq C_i$.
  - $\dim(C_i) = \ell_i - \mathfrak{g} + 1$,
  - $d(C_i) \geq n - \ell_i$ for $0 < i \leq L$.

Sequence of codes from Garcia-Stichtenoth tower

To construct

$$C_L \subseteq C_{L-1} \subseteq \ldots \subseteq C_1 \subseteq C_0 = \mathbb{F}_q^n,$$

consider

- a function field K_e of genus $\mathfrak{g}$ for some e,
- $\{\ell_i\}_i$– a sequence of positive integers satisfying $\ell_i \geq \ell_{i+1}$ for $i = 1, \ldots, L-1$ and $\ell_L > 2\mathfrak{g} - 2$.
- Then $C_i = C(\mathcal{P}, \ell_i P_\infty)$ are $\mathbb{F}_q$-linear codes with
  - $C_{i+1} \subseteq C_i$.
  - $\dim(C_i) = \ell_i - \mathfrak{g} + 1$,
  - $d(C_i) \geq n - \ell_i$ for $0 < i \leq L$.

Using the result of Shum et al. [SAKSD], we know how to construct a basis for C_i in time $\mathcal{O}((n \log_q n)^3)$.

Part IV

Construction-D lattice from GS tower code

Subfield subcodes

C – $\mathbb{F}_q$ code for $q = p^h$. Its subfield subcode $C|_{\mathbb{F}_p}$ is defined as

$$C|_{\mathbb{F}_p} = C \cap \mathbb{F}_p^n.$$

Properties of $C|_{\mathbb{F}_p}$:

- minimal distance: $d(C|_{\mathbb{F}_p}) \geq d(C)$,
- dimension $\dim_{\mathbb{F}_p}(C|_{\mathbb{F}_p}) \geq n - h(n-k)$ (see [Sti])

Sequence of subfield subcodes from GS tower

Let $\widetilde{C}_i = C(\mathcal{P}, \ell_i P_\infty)|_{\mathbb{F}_p}$ for $0 < i \leq L$, $q = p^h$. Then

$$\widetilde{C}_L \subseteq \widetilde{C_{L-1}} \subseteq \ldots \subseteq \widetilde{C}_1 \subseteq \widetilde{C}_0 = \mathbb{F}_p^n$$

is a sequence of p-ary codes s.t.

- $\dim(\widetilde{C}_i) \geq n - h(n - \ell_i + \mathfrak{g} - 1)$
- $d(\widetilde{C}_i) > n - \ell_i$

Choosing e, h, L, ℓ_i, 'appropriately', gives us a construction-D lattice with the normalized minimum distance as in the main result.

Choices of the parameters to achieve the claimed min. distance

Theorem: **For a constant $\varepsilon > 0$, there is a family of lattices $\mathcal{L} \subset \mathbb{R}^n$ with normalized minimum distance**

$$\frac{\lambda_1(\Lambda)}{\det(\Lambda)^{1/n}} = \Omega\left(\frac{\sqrt{n}}{(\log n)^{\varepsilon+o(1)}}\right).$$

These lattices are list decodable to within distance $\sqrt{1/2} \cdot \lambda_1(\Lambda)$ in $\mathrm{poly}(n)$ time.

Choices of the parameters to achieve the claimed min. distance

Theorem: **For a constant $\varepsilon > 0$, there is a family of lattices $\mathcal{L} \subset \mathbb{R}^n$ with normalized minimum distance**

$$\frac{\lambda_1(\Lambda)}{\det(\Lambda)^{1/n}} = \Omega\left(\frac{\sqrt{n}}{(\log n)^{\varepsilon+o(1)}}\right).$$

These lattices are list decodable to within distance $\sqrt{1/2} \cdot \lambda_1(\Lambda)$ in $\mathrm{poly}(n)$ time.

Proof sketch:

1. Fix a prime p and a parameter $\kappa(\varepsilon)$

Choices of the parameters to achieve the claimed min. distance

Theorem: **For a constant $\varepsilon > 0$, there is a family of lattices $\mathcal{L} \subset \mathbb{R}^n$ with normalized minimum distance**

$$\frac{\lambda_1(\Lambda)}{\det(\Lambda)^{1/n}} = \Omega\left(\frac{\sqrt{n}}{(\log n)^{\varepsilon+o(1)}}\right).$$

These lattices are list decodable to within distance $\sqrt{1/2} \cdot \lambda_1(\Lambda)$ in $\mathrm{poly}(n)$ time.

Proof sketch:

1. Fix a prime p and a parameter $\kappa(\varepsilon)$
2. Let $r \approx \log_p \kappa$ be a power of p and $e \approx \log_r \kappa$. Set $q = r^2 = p^h$.

Choices of the parameters to achieve the claimed min. distance

Theorem: **For a constant $\varepsilon > 0$, there is a family of lattices $\mathcal{L} \subset \mathbb{R}^n$ with normalized minimum distance**

$$\frac{\lambda_1(\Lambda)}{\det(\Lambda)^{1/n}} = \Omega\left(\frac{\sqrt{n}}{(\log n)^{\varepsilon+o(1)}}\right).$$

These lattices are list decodable to within distance $\sqrt{1/2} \cdot \lambda_1(\Lambda)$ in $\mathrm{poly}(n)$ time.

Proof sketch:

1. Fix a prime p and a parameter $\kappa(\varepsilon)$
2. Let $r \approx \log_p \kappa$ be a power of p and $e \approx \log_r \kappa$. Set $q = r^2 = p^h$.
3. Choose $n \approx r^{e+1}$ rational points on K_e

Choices of the parameters to achieve the claimed min. distance

Theorem: **For a constant $\varepsilon > 0$, there is a family of lattices $\mathcal{L} \subset \mathbb{R}^n$ with normalized minimum distance**

$$\frac{\lambda_1(\Lambda)}{\det(\Lambda)^{1/n}} = \Omega\left(\frac{\sqrt{n}}{(\log n)^{\varepsilon+o(1)}}\right).$$

These lattices are list decodable to within distance $\sqrt{1/2} \cdot \lambda_1(\Lambda)$ in $\mathrm{poly}(n)$ time.

Proof sketch:

1. Fix a prime p and a parameter $\kappa(\varepsilon)$
2. Let $r \approx \log_p \kappa$ be a power of p and $e \approx \log_r \kappa$. Set $q = r^2 = p^h$.
3. Choose $n \approx r^{e+1}$ rational points on K_e
4. Set $\ell_i = n - p^{2i}$ and $L = \lfloor \frac{1}{2} \log_p(n/h - \mathfrak{g}) \rfloor$

Choices of the parameters to achieve the claimed min. distance

Theorem: **For a constant $\varepsilon > 0$, there is a family of lattices $\mathcal{L} \subset \mathbb{R}^n$ with normalized minimum distance**

$$\frac{\lambda_1(\Lambda)}{\det(\Lambda)^{1/n}} = \Omega\left(\frac{\sqrt{n}}{(\log n)^{\varepsilon+o(1)}}\right).$$

These lattices are list decodable to within distance $\sqrt{1/2} \cdot \lambda_1(\Lambda)$ in $\mathrm{poly}(n)$ time.

Proof sketch:

1. Fix a prime p and a parameter $\kappa(\varepsilon)$
2. Let $r \approx \log_p \kappa$ be a power of p and $e \approx \log_r \kappa$. Set $q = r^2 = p^h$.
3. Choose $n \approx r^{e+1}$ rational points on K_e
4. Set $\ell_i = n - p^{2i}$ and $L = \lfloor \frac{1}{2} \log_p(n/h - \mathfrak{g}) \rfloor$

The choice of L ensures that $\dim(\widetilde{C}_L) > 0$ and that

$$\lambda_1(\Lambda) = p^L > \sqrt{\frac{n}{\log \log n}}.$$

The choice of ℓ_i leads to $\det(\Lambda)^{1/n} \leq (\log_p(n))^{\varepsilon}$.

What about decoding?

- We know how to efficiently decode C_i's thanks to Guruswami-Sudan [GS] list decoding algorithm
- There is a soft decision decoding technique due to Koetter-Vardy [KV] that allows to decode BCH codes using a Reed-Solomon decoder.

Idea: adapt Guruswami-Sudan decoding to soft decision decoding.

What about decoding?

- We know how to efficiently decode C_i's thanks to Guruswami-Sudan [GS] list decoding algorithm
- There is a soft decision decoding technique due to Koetter-Vardy [KV] that allows to decode BCH codes using a Reed-Solomon decoder.

Idea: adapt Guruswami-Sudan decoding to soft decision decoding.

In hard decision a decoder receives on input $\mathbf{y} \in \mathbb{R}^n$ and outputs a list of vectors close (in ℓ_2 norm) to $\mathbf{y}$.

In soft decision a decoder receives on a *reliability matrix* $\Pi \in \mathbb{R}^{|\mathbb{F}_q| \times n}$, where $\Pi_{i,j}$ describes the probability that the transmitted codeword has symbol $\alpha_i \in \mathbb{F}_q$ in the j-th position. It outputs a list of vectors that are 'related' to Π.

Where do we get Π from?

- it is either given by the communication channel (original motivation for soft decision decoding)
- or it can be constructed from the received word $\mathbf{y}$ as shown by Mook-Peikert [MP].

Soft decision decoder for GS subfield subcodes

Where do we get Π from?

- it is either given by the communication channel (original motivation for soft decision decoding)
- or it can be constructed from the received word $\mathbf{y}$ as shown by Mook-Peikert [MP].

An adaptation of Koetter-Vardy decoder for BCH to GS codes gives

Theorem For $\varepsilon > 0$, R – code rate, and d – min. distance of GS codes defined over $\mathbb{F}_q$, there exists an algorithm for decoding $\widetilde{C} \subset \mathbb{F}_p^n$, receiving on input $\mathbf{y} \in \mathbb{R}^n$, calls Koetter-Vardy soft-decision decoder and outputs codewords $\mathbf{c} \in \widetilde{C}$ that satisfy

$$\|\mathbf{y} - \mathbf{c}\| < (1 - \varepsilon)\frac{d}{2},$$

in time polynomial in $n, \log q$, and $1/\varepsilon$.

From decoding subfield subcodes to decoding Λ_L

Theorem (Mook-Peikert [MP]) Let $L \geq 0$ be an integer and let Λ_L be a construction-D lattice built from a tower

$$\widetilde{C}_L \subseteq \widetilde{C}_{L-1} \subseteq \ldots \subseteq \widetilde{C}_1 \subseteq \widetilde{C}_0 = \mathbb{F}_p^n.$$

Let $\mathcal{D}_i$ be a list decoder for $\widetilde{C}_i$ that decodes up to Euclidean distance $e_i = p^i e_0$ for some $0 < e_0 < p/2$ for all $0 \leq i \leq L$.

From decoding subfield subcodes to decoding Λ_L

Theorem (Mook-Peikert [MP]) Let $L \geq 0$ be an integer and let Λ_L be a construction-D lattice built from a tower

$$\widetilde{C}_L \subseteq \widetilde{C}_{L-1} \subseteq \ldots \subseteq \widetilde{C}_1 \subseteq \widetilde{C}_0 = \mathbb{F}_p^n.$$

Let $\mathcal{D}_i$ be a list decoder for $\widetilde{C}_i$ that decodes up to Euclidean distance $e_i = p^i e_0$ for some $0 < e_0 < p/2$ for all $0 \leq i \leq L$.

Then there is an algorithm that given on input $\mathbf{y} \in \mathbb{R}^n$ and access to $\mathcal{D}_i$, outputs a list of vectors $\mathbf{v} \in \Lambda_L$ s.t.

$$\|\mathbf{y} - \mathbf{v}\| \leq \lambda_1(\Lambda_L)/\sqrt{2}.$$

If $\mathcal{D}_i$ run in $\mathrm{poly}(n, \log p)$ time, then this algorithm also runs in $\mathrm{poly}(n, \log p)$ time.

From decoding subfield subcodes to decoding Λ_L

Theorem (Mook-Peikert [MP]) Let $L \geq 0$ be an integer and let Λ_L be a construction-D lattice built from a tower

$$\widetilde{C}_L \subseteq \widetilde{C}_{L-1} \subseteq \ldots \subseteq \widetilde{C}_1 \subseteq \widetilde{C}_0 = \mathbb{F}_p^n.$$

Let $\mathcal{D}_i$ be a list decoder for $\widetilde{C}_i$ that decodes up to Euclidean distance $e_i = p^i e_0$ for some $0 < e_0 < p/2$ for all $0 \leq i \leq L$.

Then there is an algorithm that given on input $\mathbf{y} \in \mathbb{R}^n$ and access to $\mathcal{D}_i$, outputs a list of vectors $\mathbf{v} \in \Lambda_L$ s.t.

$$\|\mathbf{y} - \mathbf{v}\| \leq \lambda_1(\Lambda_L)/\sqrt{2}.$$

If $\mathcal{D}_i$ run in $\mathrm{poly}(n, \log p)$ time, then this algorithm also runs in $\mathrm{poly}(n, \log p)$ time.

Conclusion: we have an efficient algorithm to decode Λ_L.

More details on soft decision decoding

Input to decoder: reliability matrix Π, $\mathcal{P} = \{P_1, \ldots, P_n\}$

Precomputation: convert $\Pi \in \mathbb{R}^{|\mathbb{F}_q| \times n}$ into a *multiplicity* matrix $M \in \mathbb{Z}^{|\mathbb{F}_q| \times n}$.

Assume $\mathbb{F}_q = [\alpha_1, \ldots, \alpha_q]$.

More details on soft decision decoding

Input to decoder: reliability matrix Π, $\mathcal{P} = \{P_1, \ldots, P_n\}$

Precomputation: convert $\Pi \in \mathbb{R}^{|\mathbb{F}_q| \times n}$ into a *multiplicity* matrix $M \in \mathbb{Z}^{|\mathbb{F}_q| \times n}$.

Assume $\mathbb{F}_q = [\alpha_1, \ldots, \alpha_q]$.

All known algebraic decoders work in two steps:

I. **(Soft) Interpolation step.** Goal: find a polynomial $Q(y) \in K[y]$ s.t.:

1. $Q(\alpha_i)[P_j]$ is zero of multiplicity $M_{i,j}$ for all $M_{i,j} > 0$.
2. $Q(f) \in \mathcal{L}(\ell P_\infty)$ for any $f \in \mathcal{L}(\ell P_\infty)$.

Idea: Assign $M_{i,j} = 0$ for i's that index elements form $\mathbb{F}_q \setminus \mathbb{F}_p$.

More details on soft decision decoding

Input to decoder: reliability matrix Π, $\mathcal{P} = \{P_1, \ldots, P_n\}$

Precomputation: convert $\Pi \in \mathbb{R}^{|\mathbb{F}_q| \times n}$ into a *multiplicity* matrix $M \in \mathbb{Z}^{|\mathbb{F}_q| \times n}$.

Assume $\mathbb{F}_q = [\alpha_1, \ldots, \alpha_q]$.

All known algebraic decoders work in two steps:

I. **(Soft) Interpolation step.** Goal: find a polynomial $Q(y) \in K[y]$ s.t.:

1. $Q(\alpha_i)[P_j]$ is zero of multiplicity $M_{i,j}$ for all $M_{i,j} > 0$.
2. $Q(f) \in \mathcal{L}(\ell P_\infty)$ for any $f \in \mathcal{L}(\ell P_\infty)$.

Idea: Assign $M_{i,j} = 0$ for i's that index elements form $\mathbb{F}_q \setminus \mathbb{F}_p$.

II. **Factorisation step**: factor $Q(y)$ over K to obtain factors of the form $(y - f_i)^r$, where f_i's form a list of potential encoded messages.

Open problems and directions

- Other choices of codes may be better (tried Goppa codes but received the same quality as construction-D from BCH codes)?
- Other ways to map a code over $\mathbb{F}_{p^h}$ to a code over $\mathbb{F}_p$ (tried trace codes but could not get a good bound on the minimum distance)?

Open problems and directions

- Other choices of codes may be better (tried Goppa codes but received the same quality as construction-D from BCH codes)?
- Other ways to map a code over $\mathbb{F}_{p^h}$ to a code over $\mathbb{F}_p$ (tried trace codes but could not get a good bound on the minimum distance)?

Thank you! Q?

The preprint can be found at
`https://crypto-kantiana.com/elena.kirshanova/Papers/DLattice.pdf`

References

- [BP] H. Bennett, C. Peikert, C. Hardness of the (Approximate) Shortest Vector Problem: A Simple Proof via Reed-Solomon Codes.
- [BW] E. S. Barnes, G. E. Wall. Some extreme forms defined in terms of abelian groups
- [DP] L. Ducas, C. Pierrot. Polynomial time bounded distance decoding near Minkowski bound in discrete logarithm lattices.
- [GaSt] A. Garcia, H. Stichtenoth. On the asymptotic behaviour of some towers of function fields over finite field
- [GuSu] V. Guruswami, M. Sudan. Improved decoding of Reed-Solomon and algebraic-geometric codes.
- [KV] R. Kotter, A. Vardy. Algebraic soft-decision decoding of Reed-Solomon codes.
- [MP] E. Mook, C. Peikert. Lattice (list) decoding near Minkowski's inequality.
- [SAKSD] K.W.Shum, I.Aleshnikov, P.V.Kumar, H.Stichtenoth, V.Deolalikar. A low-complexity algorithm for the construction of algebraic-geometric codes better than the Gilbert-Varshamov bound.
- [Sti] H. Stichtenoth Algebraic Function Fields and Codes.