CODES AND LATTICES IN CRYPTOGRAPHY: REAL TWINS OR DISTANT COUSINS?

CAIPI '24

Maxime Bombar, Kévin Carrier, André Chailloux, Alain Couvreur, Thomas Debris-Alazard, Léo Ducas, Charles Meyer-Hilfiger, Maxime Remaud, Nicolas Resch, Jean-Pierre Tillich, Wessel van Woerden

December 02, 2024

Inria, École Polytechnique

CODES AND LATTICES: REAL TWINS OR DISTANT COUSINS?

- Code: subspace of $\mathbb{F}_q^n$
- Lattice: discrete subgroup of $\mathbb{R}^n$

Code- and Lattice-based cryptography: Error-based Cryptography

$\longrightarrow$ Security relies on the difficulty to solve a noisy linear set of equations!

$\left(\text{Decoding \& LWE Problems}\right)$

Many similarities between codes and lattices in cryptography

But orthogonal approaches...

CODES AND LATTICES: HISTORICALLY ORTHOGONAL APPROACHES

Two different stories:

Code-based cryptography:

1. Shannon: random codes are optimal for communication (but hard to decode)
2. Seeking for easily decodable codes
3. McEliece encryption using Goppa codes
4. Alekhnovitch encryption using random codes

Hard Problem:

Decoding Random Code

Lattice-based cryptography:

1. Schnorr-Adleman: factoring with lattices, compute short vectors (hard problem)
2. Chor-Rivest Knapsack Cryptosystem
3. Ajtai worst-to-average case reduction
4. LWE is harder than finding short lattice vectors by Regev

Hard Problem:

Compute Short Lattice Vectors

DIFFERENT CRYPTOGRAPHIC APPLICATIONS

Codes and lattices found different applications to build cryptographic schemes

- Random (q-ary) lattices are used to build encryption schemes, but don't forget Alekhnovitch that purely relies on random codes
- Random lattices are used to build hash-and-sign schemes, but random codes are used in MPC-in-the-head signatures
- Structured lattices are used to build fully homomorphic schemes, but structured codes are used in MPC constructions

DIFFERENT CRYPTOGRAPHIC APPLICATIONS

Codes and lattices found different applications to build cryptographic schemes

- Random (q-ary) lattices are used to build encryption schemes, but don't forget Alekhnovitch that purely relies on random codes
- Random lattices are used to build hash-and-sign schemes, but random codes are used in MPC-in-the-head signatures
- Structured lattices are used to build fully homomorphic schemes, but structured codes are used in MPC constructions

$\longrightarrow$ It seems that codes and lattices are used for dual constructions!

Codes and lattices offer different degrees of freedom for designs

But do they also rely on opposite foundations, sources of hardness?

DIFFERENT CRYPTOGRAPHIC APPLICATIONS

Codes and lattices found different applications to build cryptographic schemes

- Random (q-ary) lattices are used to build encryption schemes, but don't forget Alekhnovitch that purely relies on random codes
- Random lattices are used to build hash-and-sign schemes, but random codes are used in MPC-in-the-head signatures
- Structured lattices are used to build fully homomorphic schemes, but structured codes are used in MPC constructions

$\longrightarrow$ It seems that codes and lattices are used for dual constructions!

Codes and lattices offer different degrees of freedom for designs

But do they also rely on opposite foundations, sources of hardness? Spoil: no!

BUT CODES AND LATTICES ARE REAL TWINS

Codes and lattices: real twins!

My goal: to convince you by using the correct common language

My approach: start from the foundations, proofs and sources of hardness for code- and lattice-based cryptography

- Decoding Random Code and LWE problems enjoy the same combinatorial properties
- Worst-to-average case reductions are within the same framework
- The Fourier theory is the same up to the right dictionary!

Even in a broader context:

Via this common language, codes and lattices share exactly the same asymptotic packing bounds!

WHY IS IT IMPORTANT?

Origin of trust in cryptography

Studying sources of hardness:

reductions $\Longleftrightarrow$ cryptanalysis

Did all techniques used for codes have also been considered for lattices, and reciprocally?

Beyond scientific curiosity:

Common language will hint us at how complete each state of the art is

ROADMAP

- Decoding Random Codes versus LWE
- Worst-to-average-case reduction: same framework
- Gaussian and Bernoulli? About noises in code- and lattice-based cryptography
- One smoothing parameter to rule them all
- A common source of hardness: quantum Regev's reduction
- A little bit about packing bounds

DECODING **VERSUS** LWE

Vectors are in row notation

Code:

A $[n, k]$-code $\mathcal{C}$ is a subspace of $\mathbb{F}_q^n$

n : length $\quad$ k : dimension

- Basis/Generator matrix rep.: rows of $\mathbf{A} \in \mathbb{F}_q^{k \times n}$ form a basis,

$$\mathcal{C} = \left\{ \mathbf{sA} : \ \mathbf{s} \in \mathbb{F}_q^k \right\}$$

- Knapsack/Parity-check rep.: $\mathcal{C}$ as null space of a full-rank $\mathbf{H} \in \mathbb{F}_q^{(n-k) \times n}$,

$$\mathcal{C} = \left\{ \mathbf{c} \in \mathbb{F}_q^n : \ \mathbf{Hc}^\top = \mathbf{0} \right\}$$

Hamming weight:

$$\forall \mathbf{x} \in \mathbb{F}_q^n, \quad |\mathbf{x}| \stackrel{\text{def}}{=} \{ i \in [1, n] : \ x_i \neq 0 \}$$

Crucial remark:

Hamming weight independent of element size: $|(1, 1, 0, 0, 2) = |(9, 6, 3, 0, 0)| = 3$

SOME NOTATION: BERNOULLI DISTRIBUTION

- $X \leftarrow \mathcal{S}$: X picked uniformly at random in $\mathcal{S}$
- $\mathbf{e} \leftarrow \mathrm{Ber}(p)^{\otimes n}$: the e_i's are independent and $\mathbb{P}(e_i = x) = \begin{cases} 1-p & \text{if } x = 0 \\ \frac{p}{q-1} & \text{if } x \neq 0 \end{cases}$

Chernoff's bound: $\mathrm{Ber}(p)^{\otimes n}$ concentrates over words of Hamming weight $\approx np$

Given $\mathbf{e} \leftarrow \mathrm{Ber}(p)^{\otimes n}$,

$$\mathbb{E}(|\mathbf{e}|) = np \quad \text{and} \quad \mathbb{P}\left(\left||\mathbf{e}| - np\right| \geq \varepsilon n\right) \leq 2\, e^{-\varepsilon n^2}$$

"*Bernoulli* $\Longleftrightarrow$ *Gaussian*"

THE DECODING PROBLEM

DP(n, k, t) primal rep.

- **Input:** $(\mathbf{A}, \mathbf{y} \stackrel{\text{def}}{=} \mathbf{sA} + \mathbf{e})$ where $\mathbf{A} \leftarrow \mathbb{F}_q^{k \times n}$, $\mathbf{s} \leftarrow \mathbb{F}_q^k$ and $\mathbf{e} \leftarrow \mathrm{Ber}(t/n)^{\otimes n}$
- **Aim:** recovering $\mathbf{x} \in \mathbb{F}_q^n$ such that: $\begin{cases} |\mathbf{x}| \approx t \\ \mathbf{y} - \mathbf{x} \in \{\mathbf{s}'\mathbf{A} : \ \mathbf{s}' \in \mathbb{F}_q^k\} \end{cases}$

- How many solutions (of weight $\approx t$) do we expect?

  $\longrightarrow$ It will impact the running-time of decoding algorithms!

- Are there other equivalent representations of DP(n, k, t)?

  $\longrightarrow$ Yes! The dual/parity-check/knapsack representation!

PRIMAL VERSUS DUAL REPRESENTATIONS

DP(n, k, t) dual rep.

- **Input:** $(\mathbf{H}, \mathbf{s} \stackrel{\text{def}}{=} \mathbf{H}\mathbf{e}^\top)$ where $\mathbf{H} \leftarrow \mathbb{F}_q^{(n-k)\times n}$ and $\mathbf{e} \leftarrow \mathrm{Ber}(t/n)^{\otimes n}$
- **Aim:** recovering $\mathbf{x}$ such that: $\begin{cases} |\mathbf{x}| \approx t \\ \mathbf{H}\mathbf{x}^\top = \mathbf{s}^\top \end{cases}$

Proposition: dual and primal DP are equivalent

$\forall$ algorithm solving dual-DP(n, k, t) with prob. ε (over the inputs) can be turned into an algorithm solving primal-DP(n, k, t) with prob.

$$\geq \varepsilon - O(q^{\min(k, n-k)})$$

and reciprocally.

Proof: use statistical distance arguments + given $\mathcal{C}$ with basis $\mathbf{A}$ and parity-check matrix $\mathbf{H}$,

- $\mathbf{y} = \mathbf{s}\mathbf{A} + \mathbf{e} \longrightarrow \mathbf{H}\mathbf{y}^\top = \underbrace{\mathbf{H}(\mathbf{s}\mathbf{A})^\top}_{=\mathbf{0} \text{ as } \mathbf{s}\mathbf{A}\in\mathcal{C}} + \mathbf{H}\mathbf{e}^\top = \mathbf{H}\mathbf{e}^\top$
- $\mathbf{s}^\top = \mathbf{H}\mathbf{e}^\top \stackrel{\text{lin. algebra}}{\longrightarrow} \mathbf{y}$ s.t $\mathbf{H}\mathbf{y}^\top = \mathbf{s}^\top = \mathbf{H}\mathbf{e}^\top$, thus $\underbrace{\mathbf{H}(\mathbf{y}-\mathbf{e})^\top = \mathbf{0}}_{\mathbf{y}-\mathbf{e}\in\mathcal{C}}$ and $\mathbf{y} = \mathbf{s}\mathbf{A} + \mathbf{e}$

RANDOM CODES

How many solutions in $\mathrm{DP}(n, k, t)$ *do we expect?*

$\longrightarrow$ Study of random codes

Random code:

$\mathcal{C}$ is said to be a random $[n, k]$-code if,

$$\mathcal{C} = \left\{ \mathbf{c} \in \mathbb{F}_q^m : \mathbf{H}\mathbf{c}^\top = 0 \right\} \quad \text{where } \mathbf{H} \leftarrow \mathbb{F}_q^{(n-k)\times n}$$

Up to $O(q^{-\min(k,n-k)})$ losses in probabilities: equivalent to choose a basis $\mathbf{A} \in \mathbb{F}_q^{k\times n}$ randomly or $\mathcal{C}$ uniformly among the $[n, k]$-codes

DETERMINANT OF A CODE

"Determinant" of a code: inverse of its volume/density

$$\det(\mathcal{C}) = \frac{q^n}{q^k} = \frac{\sharp \mathbb{F}_q^n}{\sharp \mathcal{C}}$$

An important computation:

$$\forall \mathbf{x} \neq 0,\ \forall \mathbf{s} \in \mathbb{F}_q^{n-k}, \quad \mathbb{P}_{\mathbf{H}}(\mathbf{H}\mathbf{x}^\top = \mathbf{s}^\top) = \frac{1}{q^{n-k}} = \frac{1}{\det(\mathcal{C})}$$

$$\mathbb{E}_{\mathbf{H}}\left(\mathbf{c} \in \mathcal{C} :\ |\mathbf{c}| = t\right) = \frac{\sharp \mathcal{S}_t}{\det(\mathcal{C})} \quad \text{and} \quad \mathbb{E}_{\mathbf{H}}\left(\text{solutions to DP}(n,k,t)\right) = 1 + \frac{\sharp \mathcal{S}_t}{\det(\mathcal{C})}$$

where $\mathcal{S}_t$ Hamming-sphere of radius t

GILBERT-VARSHAMOV BOUND

Minimum distance of a random code? Largest t for which one solution to $\mathrm{DP}(n,k,t)$ *is expected?*

$$\mathbb{E}_{\mathsf{H}}\left(\mathbf{c}\in\mathcal{C}:\ |\mathbf{c}|=t\right)=\frac{\sharp\mathcal{S}_t}{\det(\mathcal{C})}\quad\text{and}\quad\mathbb{E}_{\mathsf{H}}\left(\text{solutions to }\mathrm{DP}(n,k,t)\right)=1+\frac{\sharp\mathcal{S}_t}{\det(\mathcal{C})}$$

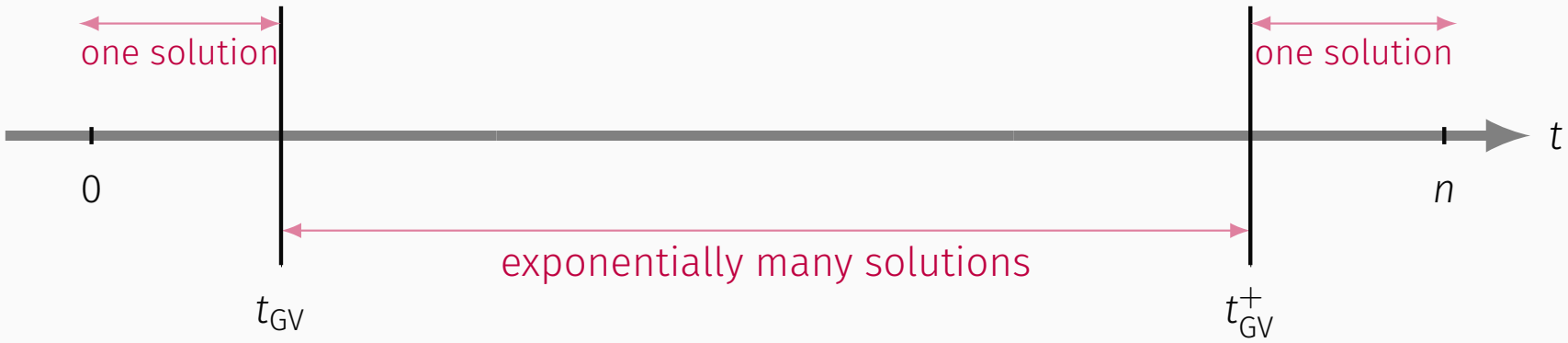
Gilbert-Varshamov bound: t_{GV} such that

$$\sharp\mathcal{S}_{t_{\mathrm{GV}}}\approx\det(\mathcal{C})\iff t_{\mathrm{GV}}=\ h^{-1}\left(1-k/n\right)\left(1+o(1)\right)\quad(h\text{ binary-entropy})$$

$\longrightarrow$ Random codes have minimum distance t_{GV} with overwhelming probability

"Codes with minimum distance $t_{\mathrm{GV}}\iff$ Gaussian heuristic"

TWO REGIMES OF PARAMETERS



Be careful: usually in code-based cryptography

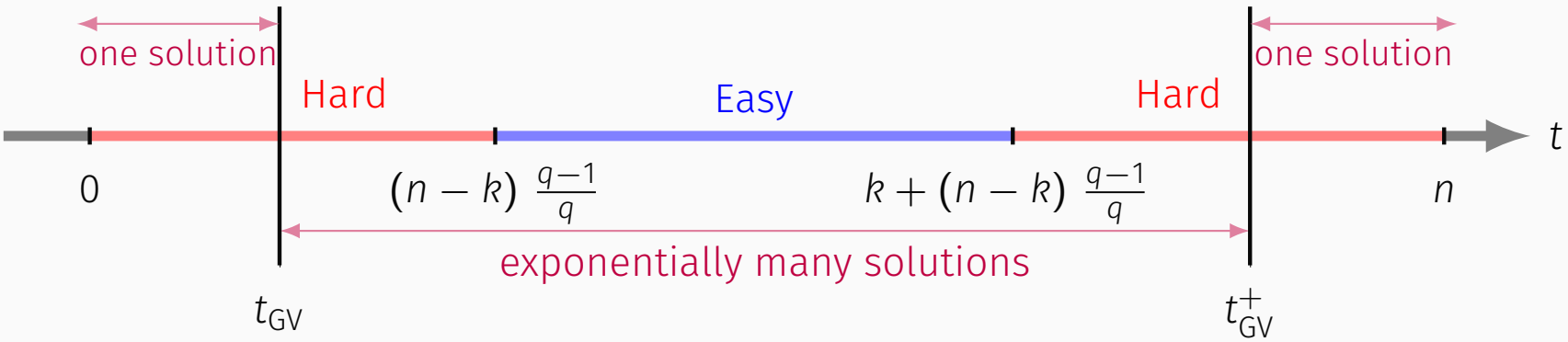
same name to DP(n, k, t) whatever is $t \leq t_{GV}$ or $t \geq t_{GV}$ though very different behaviour

"DP(n, k, t) *with* $t \leq t_{GV} \iff$ LWE"

"DP(n, k, t) *with* $t \geq t_{GV} \iff$ ISIS"

ALGORITHMIC HARDNESS

Best attacks to solve DP(n, k, t): complexity $2^{\alpha(k/n)\, t\, (1+o(1))}$ where $\alpha(k/n)$ constant



- Information Set Decoding Algorithms
- Dual attacks
- Algebraic attacks **but not competitive with usual parameters**

A PARALLEL STORY: LATTICES

Meanwhile lattices are making their own ways

Lattice:

Discrete subgroup Λ of $\mathbb{R}^n$

$\longrightarrow$ Usually in lattice-based cryptography, particular lattices: q-ary lattices

- Lattices admit a basis rep.: $\mathbf{A} \in \mathbb{R}^{k \times n}$ being full-rank,

$$\Lambda = \mathbb{Z}^k \cdot \mathbf{A} = \left\{ \mathbf{s}\mathbf{A} : \ \mathbf{s} \in \mathbb{Z}^k \right\}$$

Determinant of lattice:

Given Λ with basis $\mathbf{A}$, its determinant is (independent of basis choice),

$$\det \Lambda \stackrel{\text{def}}{=} \sqrt{\det \mathbf{A}\mathbf{A}^\top}$$

Euclidean norm:

$$\forall \mathbf{x} \in \mathbb{R}^n, \quad |\mathbf{x}|_2 \stackrel{\text{def}}{=} \sqrt{\sum_{i=1}^{n} x_i^2}$$

SOME NOTATION: GAUSSIAN DISTRIBUTION

- $\mathbf{e} \leftarrow \text{Gauss}(\sigma)^{\otimes m}$: $e_i \in \mathbb{R}$ are independent and their density distribution $\frac{1}{\sigma} \mathrm{e}^{-\pi \frac{|x|_2^2}{\sigma^2}}$

Be careful:

- $\text{Gauss}(\sigma)^{\otimes n}$ is a distribution over $\mathbb{R}^n$
- $\text{Gauss}(\sigma)^{\otimes n}$ will also denote the Gaussian modulo q, *i.e.*

$$\forall x \in \mathbb{Z}/q\mathbb{Z} = \{-(q-1)/2, \ldots, (q-1)/2\}, \mathbb{P}(e_i = x) = \frac{\sum_{k \in \mathbb{Z}} \mathrm{e}^{-\pi \frac{|x+kq|_2^2}{\sigma^2}}}{N} \approx \frac{1}{\sigma} \mathrm{e}^{-\pi \frac{|x|_2^2}{\sigma^2}}$$

Chernoff's bound: $\text{Gauss}(\sigma)$ concentrates over words of norm $\approx \sqrt{n}\,\sigma/\sqrt{2\pi}$

Given $\mathbf{e} \leftarrow \text{Gauss}(\sigma)^{\otimes n}$,

$$\mathbb{E}(|\mathbf{e}|_2) = \sqrt{n}\frac{\sigma}{\sqrt{2\pi}} \quad \text{and} \quad \mathbb{P}\left(\left||\mathbf{e}|_2 - \sqrt{n}\,\frac{\sigma}{\sqrt{2\pi}}\right| \geq \varepsilon\sqrt{n}\frac{\sigma}{\sqrt{2\pi}}\right) \leq 2\,\mathrm{e}^{-\varepsilon^2 n}$$

Current lattice-based cryptography:

work modulo q!

LWE(q, n, k, σ):

- **Input:** $(\mathbf{A}, \mathbf{sA} + \mathbf{e})$ where $\mathbf{A} \leftarrow (\mathbb{Z}/q\mathbb{Z})^{k \times n}$, $\mathbf{s} \leftarrow (\mathbb{Z}/q\mathbb{Z})^{k}$ and $\mathbf{e} \leftarrow \text{Gauss}(\sigma)^{\otimes n}$
- **Aim:** recovering $\mathbf{e}$

Remark:

Parameters in LWE are chosen to ensure unicity of the solution: "$\sqrt{n}\frac{\sigma}{2\pi} \leq t_{\text{GV}}$"

But why is LWE *a lattice problem?*

$\longrightarrow$ First reason: construction A

THE CONSTRUCTION A

The first (and powerful) tool to build lattices: ***lift a code*** $\mathcal{C} \subseteq (\mathbb{Z}/q\mathbb{Z})^n$ ***into*** $\mathbb{R}^n$

q-ary lattices:

Given $\mathbf{A} \in (\mathbb{Z}/q\mathbb{Z})^{k \times n}$, the following lattice is said q-ary

$$\Lambda_q(\mathbf{A}) = (\mathbb{Z}/q\mathbb{Z})^k \cdot \mathbf{A} + q \cdot \mathbb{Z}^n = \left\{ \mathbf{y} \in \mathbb{Z}^n : \ \exists \mathbf{s} \in (\mathbb{Z}/q\mathbb{Z})^n, \ \mathbf{y} = \mathbf{sA} \bmod q \right\}$$

- Basis/Generator matrix rep.: rows of $\mathbf{A}$ form a basis modulo q of the lattice $\Lambda_q(\mathbf{A})$
- Knapsack/Parity-check rep.: $\Lambda_q(\mathbf{A})$ is null-space of some $\mathbf{H} \in (\mathbb{Z}/q\mathbb{Z})^{(n-k) \times n}$,

$$\Lambda_q(\mathbf{A}) = \left\{ \mathbf{x} \in \mathbb{Z}^n : \ \mathbf{H}\mathbf{x}^\top = 0 \bmod q \right\} \subseteq \mathbb{Z}^n$$

When lifting in $\mathbb{R}^n$ an LWE-instance: from a target, find a close vector in $\Lambda_q(\mathbf{A})$

Two models of random lattices:

- As in LWE: random q-ary lattice, $\Lambda_q(\mathbf{A})$ where $\mathbf{A} \leftarrow \mathbb{Z}/(q\mathbb{Z})^{k\times n}$

  $\longrightarrow$ The underlying code in LWE is random!

- Probability measure μ over the set of $\Lambda \subseteq \mathbb{R}^n$ with fixed determinant

Models are combinatorially consistent with random codes:

$\mathrm{Vol}(B_w)$ the volume of Euclidean ball with radius w,

- From random codes, for LWE:

$$\mathbb{E}_{\mathbf{A}}\Big(\mathbf{x} \in \Lambda_q(\mathbf{A}) :\ 0 < |\mathbf{x}|_2 \le w\Big) = \frac{\mathrm{Vol}(B_w)}{\det \Lambda_q(\mathbf{A})}(1+o(1))\Big(= \frac{\mathrm{Vol}(B_w)}{\det \mathcal{C}(\mathbf{A})}(1+o(1))\Big)$$

- From Minkowski-Hlawka-Siegel, for random lattices $\Lambda \subseteq \mathbb{R}^n$ with fixed $\det(\cdot)$,

$$\mathbb{E}_{\mu}\Big(\mathbf{x} \in \Lambda :\ 0 < |\mathbf{x}|_2 \le w\Big) = \frac{\mathrm{Vol}(B_w)}{\det \Lambda}$$

TWO REGIMES OF PARAMETERS: GAUSSIAN HEURISTIC

$V_w \stackrel{\text{def}}{=} \text{Vol}\left(\mathcal{B}_w\right)$: volume of the Euclidean ball with radius w

$$V_w = \frac{\pi^{n/2}}{(n/2+1)!} w^n \approx \pi^{n/2} \left(\frac{2e}{n}\right)^{n/2} w^n = \left(\frac{2e\pi w^2}{n}\right)^{n/2}$$

"Gilbert-Varhsamov bound for lattices": t_{GE}

$$V_{t_{\text{GE}}} \approx \det(\Lambda) \iff t_{\text{GE}} = \sqrt{n/(2\pi e)}\ \det(\Lambda)^{1/n}$$

ALGORITHMIC HARDNESS

Best attacks to solve LWE: complexity $O\left(2^{x \log_2 x}\right)$ where $x = \frac{k \log q}{\log_2^2 q/\sigma}$

- Basis reduction
- Dual attacks
- Algebraic attacks, Arora-Ge algorithm

To conclude:

Decoding and LWE problems

- designed from the same object: random codes
- enjoying the same combinatorial properties

But why are they believed to be hard?

Both problems enjoy worst-to-average-case reductions via the same framework!

PROOF OF HARDNESS

Decoding *and* LWE *are* ***average*** *problems*

Aim: worst-to-average-case reduction

Turn any algorithm solving Decoding/LWE with prob ε (over the inputs) into an algorithm solving a problem for any fixed input, *i.e.*

$$\text{Decoding/LWE} \underset{\text{(harder)}}{\geq} \text{worst-case problem}$$

Worst-to-average case reduction

We are given a fixed instance

$(\mathbf{G}, \mathbf{xG} + \mathbf{r})$ where weight/norm of $\mathbf{r}$ is w

and we want to recover $\mathbf{r}$.

But, we have an algorithm $\mathcal{A}$ solving Decoding/LWE with probability ε

$\left(\text{it does not solve for any } \mathbf{A}, \mathbf{s}, \mathbf{e}\right)$

$$\mathbb{P}_{\mathbf{A},\mathbf{s},\mathbf{e}}\left(\mathcal{A}(\mathbf{A}, \mathbf{sA} + \mathbf{e}) = \mathbf{e}\right) = \varepsilon$$

$$\langle \mathbf{a}, \mathbf{b} \rangle \stackrel{\text{def}}{=} \sum a_i b_i$$

Key-idea:

From $(\mathbf{G}, \mathbf{y} \stackrel{\text{def}}{=} \mathbf{x}\mathbf{G} + \mathbf{r})$, build a "uniform" instance that will being fed to $\mathcal{A}$

1. $\mathbf{e} \leftarrow \mathcal{D}$ (distribution)
2. Compute,

$$\langle \mathbf{y}, \mathbf{e} \rangle = \langle \mathbf{x}\mathbf{G}, \mathbf{e} \rangle + \langle \mathbf{r}, \mathbf{e} \rangle = \langle \underbrace{\mathbf{x}}_{\text{secret}}, \mathbf{e}\mathbf{G}^\top \rangle + \underbrace{\langle \mathbf{r}, \mathbf{e} \rangle}_{\text{noise}}$$

To build a truly LWE/Decoding instance:

- We would like $\mathbf{e}\mathbf{G}^\top$ "very close to uniform"
- Need to analyze noise distribution $e = \langle \mathbf{r}, \mathbf{e} \rangle$ (the easy part)

The example of the Bernoulli in $\mathbb{F}_2^n$:

If $\mathbf{e} \leftarrow \mathrm{Ber}^{\otimes n}(p)$, then $\langle \mathbf{r}, \mathbf{e} \rangle$ sum of w independent Bernoulli

$$\langle \mathbf{r}, \mathbf{e} \rangle \leftarrow \mathrm{Ber}\left(\frac{1}{2}\left(1 - (1-2p)^w\right)\right) \quad \text{(pilling-up lemma)}$$

CLOSENESS: STATISTICAL DISTANCE

Statistical distance:

Given two random variables X, Y with distributions f, g,

$$\Delta(\mathsf{X}, \mathsf{Y}) = \Delta(f, g) = \frac{1}{2} \sum_x |f(x) - g(x)| \quad \left(= \frac{1}{2} \int_{\mathbb{R}^n} |f(x) - g(x)| \, dx, \text{ continuous case} \right)$$

$\longrightarrow$ It captures the differences between two random variables

- **Data processing inequality:** for any function/algorithm h

$$\Delta(h(\mathsf{X}), h(\mathsf{Y})) \leq \Delta(\mathsf{X}, \mathsf{Y})$$

- For any event $\mathcal{E}$,

$$|\mathbb{P}(\mathsf{X} \in \mathcal{E}) - \mathbb{P}(\mathsf{Y} \in \mathcal{E})| \leq \Delta(\mathsf{X}, \mathsf{Y})$$

If an algorithm succeeds with inputs X *and probability* ε*, then it succeeds given* Y *with probability* $\geq \varepsilon - \Delta(\mathsf{X}, \mathsf{Y})$

OUR AIM

1. We want the following to be small:

$$\alpha \stackrel{\text{def}}{=} \Delta\Big((\mathbf{e}\mathbf{G}^\top, \langle \mathbf{x}, \mathbf{e}\mathbf{G}^\top\rangle + \langle \mathbf{r}, \mathbf{e}\rangle), (\underbrace{\mathbf{a}}_{\text{uniform}}, \langle \mathbf{x}, \mathbf{a}\rangle + \underbrace{e}_{\text{same distrib as } \langle \mathbf{r}, \mathbf{e}\rangle})\Big)$$

True LWE/Decoding *instance*

2. Then we feed $(\mathbf{e}\mathbf{G}^\top, \langle \mathbf{x}, \mathbf{e}\mathbf{G}^\top\rangle + \langle \mathbf{r}, \mathbf{e}\rangle)$ to the Decoding/LWE-solver $\mathcal{A}$ with prob. ε
3. If we give n samples to $\mathcal{A}$, it will recover $\mathbf{x}$ with prob. $\geq \varepsilon - n\alpha$

A simplification:

We will target $\Delta\left(\mathbf{e}\mathbf{G}^\top, \underbrace{\mathbf{a}}_{\text{uniform}}\right)$ to be small when $\mathbf{G}$ is fixed but $\mathbf{e}$ random variable

A GEOMETRICAL INTERPRETATION: PRIMAL REPRESENTATION

$$\text{Aim: } \Delta\left(\mathbf{e}\mathbf{G}^\top, \underbrace{\mathbf{a}}_{\text{uniform}}\right) \text{ small}$$

Which object is $\mathbf{e}\mathbf{G}^\top$*?*

$\longrightarrow$ Let us take the code $\mathcal{C} \subseteq \mathbb{F}_q^n$ point of view

$$\mathcal{C} = \left\{\mathbf{c} : \ \mathbf{c}\mathbf{G}^\top = \mathbf{0}\right\}$$

$\mathbf{e}\mathbf{G}^\top$ *defines a coset of* $\mathcal{C}$

Primal representation:

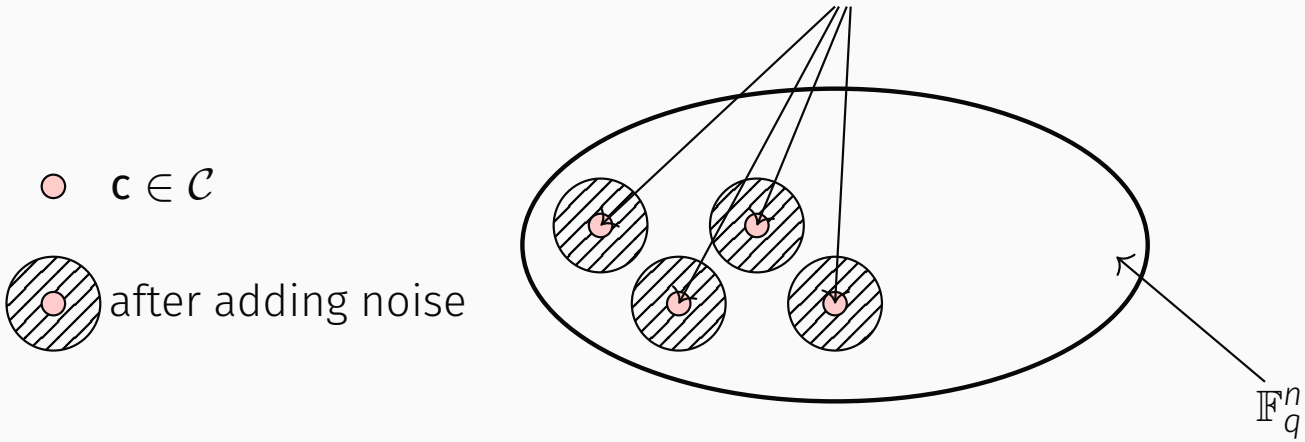
$\mathbf{e}\mathbf{G}^\top$ uniform $\iff$ uniform in $\mathbb{F}_q^n/\mathcal{C}$, *i.e.* uniform modulo $\mathcal{C}$

(for a lattice Λ, asking a distribution to be uniform modulo Λ (fund. parallelepiped))

$\mathbf{e}\mathbf{G}^\top$ uniform for $\mathbf{e} \leftarrow \mathcal{D} \iff \mathbf{c} + \mathbf{e}$ uniform in $\mathbb{F}_q^n$ where $\mathbf{c} \leftarrow \mathcal{C}$ and $\mathbf{e} \leftarrow \mathcal{D}$

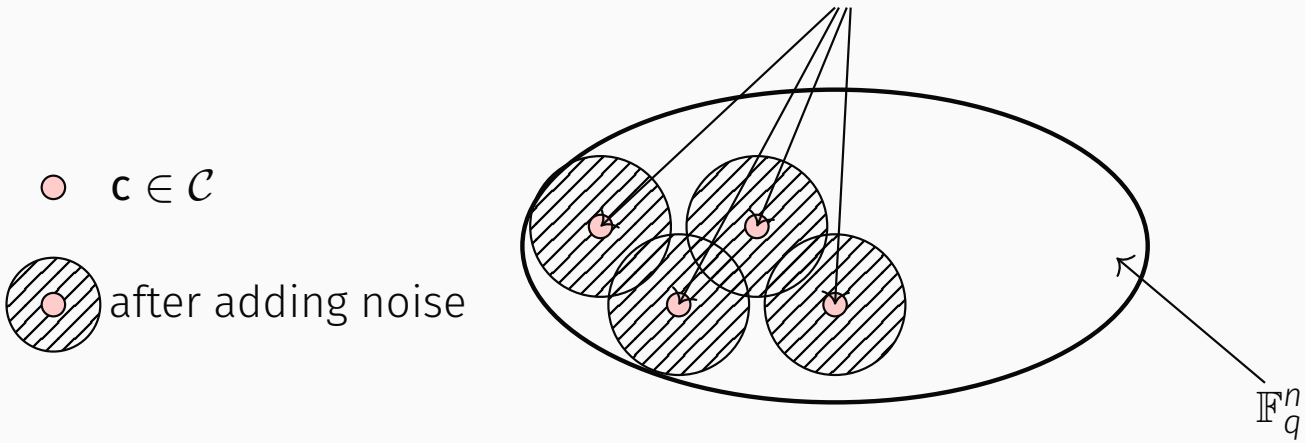
$\mathbf{c} + \mathbf{e}$ uniform in $\mathbb{F}_q^n$ where $\mathbf{c} \leftarrow \mathcal{C}$ and $\mathbf{e} \leftarrow \mathcal{D}$

Starting from codewords and adding noise



$\mathbf{c} + \mathbf{e}$ uniform in $\mathbb{F}_q^n$ where $\mathbf{c} \leftarrow \mathcal{C}$ and $\mathbf{e} \leftarrow \mathcal{D}$

Starting from codewords and adding noise



ABOUT THE NOISE DISTRIBUTION

THE NOISE: OUR BEST FRIEND TO UNIFORMIZE

Our aim:

To find $\mathbf{e} \leftarrow \mathcal{D}$ such that $\mathbf{c} + \mathbf{e}$ is close (stat. distance) to uniform when $\mathbf{c} \leftarrow \mathcal{C}$

Some simplification: $\mathbf{e} \in \mathbb{F}_2^n$ and $\mathcal{C}$ fixed $[n, K]$-binary code

A first approach:

Choose each bit of $\mathbf{e}$ with probability 1/2, then $\mathbf{c} + \mathbf{e}$ is uniform

But, doing this is useless: $\langle \mathbf{r}, \mathbf{e} \rangle$ will be a uniform noise...

Therefore, impossible to solve $(\mathbf{e}\mathbf{G}^\top, \langle \mathbf{x}, \mathbf{e}\mathbf{G}^\top \rangle + \underbrace{\langle \mathbf{r}, \mathbf{e} \rangle}_{\text{noise}})$

$\longrightarrow$ We need to carefully choose the noise!

BERNOULLI AND GAUSSIAN: A NATURAL CHOICE?

A natural choice:

- $\mathrm{Berp}(p)^{\otimes n}$ for codes
- $\mathrm{Gauss}(\sigma)^{\otimes n}$ for lattices

Natural choice? Why?

$\longrightarrow$ Distributions are not natural, but the problem we aim to solve is!

BERNOULLI AND GAUSSIAN: A NATURAL CHOICE?

A natural choice:

- $\mathrm{Berp}(p)^{\otimes n}$ for codes
- $\mathrm{Gauss}(\sigma)^{\otimes n}$ for lattices

Natural choice? Why?

$\longrightarrow$ Distributions are not natural, but the problem we aim to solve is!

A natural interpretation: heat equation

Noise $\mathbf{e}$ in $\mathbf{c} + \mathbf{e}$: heat after starting from $\mathbf{c}$

$\longrightarrow$ *When does the heat starting from* $\mathbf{c} \in \mathcal{C}$ *will be uniform?*

HEAT EQUATION: THE EUCLIDEAN CASE

$$\Delta \stackrel{\text{def}}{=} \sum_{i=1}^{n} \frac{\partial^2}{\partial x_i^2}$$

Heat equation:

Given $f : \mathbb{R}^n \to \mathbb{R}$, find $u : \mathbb{R}^+ \times \mathbb{R}^n \to \mathbb{R}$ satisfying $\begin{cases} \frac{\partial u}{\partial t} = \Delta u \\ u_{|t=0} = f \end{cases}$

$u(t, \mathbf{x})$ represents the temperature at instant t at the point $\mathbf{x} \in \mathbb{R}^n$

- Heat Kernel as fundamental solution:

$K_{\mathbf{y}}$ be the solution when $f = \delta_{\mathbf{y}}$ (Krnoecker symbol)

$\longrightarrow$ solution u for any f of the Heat Equation: $u(t, \mathbf{x}) \stackrel{\text{def}}{=} K_{\mathbf{0}}(t, \mathbf{x}) \star f$ (convolution)

$\Big($ $K_{\mathbf{0}}(t, \mathbf{x})$ noise at point $\mathbf{x}$ after t steps and starting from $\mathbf{0}$ $\Big)$

The Heat Kernel is a Gaussian:

$$K_{\mathbf{0}}(t, \mathbf{x}) = \frac{1}{(4\pi t)^n} \mathrm{e}^{-\frac{|\mathbf{x}|_2^2}{4t}} \text{ concentrating at norm } \sqrt{2nt}$$

HEAT EQUATION: THE HAMMING CUBE

$$\Delta f(\mathbf{x}) = \sum_{\mathbf{y}\sim\mathbf{x}} \Big(f(\mathbf{y}) - f(\mathbf{x})\Big) \text{ where } \mathbf{y} \sim \mathbf{x} \text{ means } |\mathbf{x}-\mathbf{y}| = 1$$

Heat Equation:

Given $f : \mathbb{F}_2^n \to \mathbb{R}$, find $u : \mathbb{R}^+ \times \mathbb{F}_2^n \to \mathbb{R}$ satisfying $\begin{cases} \frac{\partial u}{\partial t} = \Delta u \\ u_{|t=0} = f \end{cases}$

- Heat Kernel as fundamental solution:

$$K_{\mathbf{y}} \text{ be the solution when } f = \delta_{\mathbf{y}} \quad \text{(Krnoecker symbol)}$$

$$\longrightarrow \text{solution } u \text{ of the Heat equation: } u(t,\mathbf{x}) \stackrel{\text{def}}{=} K_{\mathbf{0}}(t,\mathbf{x}) \star f$$

The Heat Kernel is a Bernoulli:

$$K_{\mathbf{0}}(t,\mathbf{x}) = p^{|\mathbf{x}|}(1-p)^{n-|\mathbf{x}|} \text{ where } p = \tfrac{1-e^{-2t}}{2}$$

CONCLUSION: BERNOULLI AND GAUSSIAN: SAME OBJECTS

Bernoulli and Gaussian magically appeared when trying to understand how to uniformize $\mathbf{e}^\top \mathbf{G}$

Our dictionary:

- ✓ LWE/Decoding: same combinatorial prop. in terms of determinant and volume
- ✓ Same approach to provide worst-to-average case reduction for LWE/Decoding
- ✓ Bernoulli $\longleftrightarrow$ Gaussian

ANOTHER CONCLUSION

Our analogy between Gaussian and Bernoulli arises from the Heat Equation

To uniformize $\mathbf{e}^\top \mathbf{G}$, it motivates spectral considerations, *i.e.* Fourier theory!

SMOOTHING PARAMETER

OUR GOAL

Treating the code case will be simpler (motivated by combinatorial argument)

Given a subspace $\mathcal{C}$ of dimension k of $\mathbb{F}_q^n$: we want to uniformize:

$\mathbf{c} + \mathbf{e}$ **to be uniform** where $\mathbf{c} \leftarrow \mathcal{C}$ and $\mathbf{e} \leftarrow \mathrm{Ber}(p)$ (Bernoulli not mandatory)

$\mathcal{S}_t$ be the Hamming-sphere with radius t

As $\mathrm{Ber}(p)$ concentrated over $\mathcal{S}_{pn}$,

$$\sharp\mathcal{C} \cdot \sharp\mathcal{S}_{pn} \geq q^n \iff \sharp\mathcal{S}_{pn} \geq \mathbf{det}(\mathcal{C}) \iff pn \geq t_{\mathrm{GV}}$$

A lower-bound on the amount of noise:

If noise concentrates on sphere with radius t: necessarily $t \geq t_{\mathrm{GV}}$

SOME NOTATION

Notation:

- unif: uniform distribution of $\mathbb{F}_q^n$
- $1_{\mathcal{C}}$: indicator function of $\mathcal{C}$
- Convolution, $f \star g(\mathsf{x}) \stackrel{\text{def}}{=} \sum_{\mathsf{y} \in \mathbb{F}_q^n} f(\mathsf{y}) g(\mathsf{x} - \mathsf{y})$

If $\mathsf{X} \leftarrow f$ and $\mathsf{Y} \leftarrow g$ are independent, then $\mathsf{X} + \mathsf{Y} \leftarrow f \star g$

Smoothing parameter: smallest p s.t

$$\Delta\left(\frac{1_{\mathcal{C}}}{\sharp \mathcal{C}} \star f_p, \text{unif}\right) = \frac{1}{2} \sum_{\mathsf{x} \in \mathbb{F}_q^n} \left| \frac{1_{\mathcal{C}}}{\sharp \mathcal{C}} \star f_p(\mathsf{x}) - \text{unif}(\mathsf{x}) \right| \text{ negligible where } f_p \stackrel{\text{def}}{=} \text{Ber}(p)$$

I have a dream:

$\Delta\left(\frac{1_{\mathcal{C}}}{\sharp \mathcal{C}} \star f_p, \text{unif}\right)$ is negligible as soon as $pn = t_{\text{GV}}(1 + o(1))$,

CAUCHY-SCHWHARZ: PARSEVAL'S WORLD

We want: $\frac{1_{\mathcal{C}}}{\sharp \mathcal{C}} \star f_p$ close to uniform $\Big(f_p = \mathrm{Ber}(p)\Big)$

So, $x \mapsto \left|\frac{1_{\mathcal{C}}}{\sharp \mathcal{C}} \star f_p(\mathbf{x}) - \mathrm{unif}(\mathbf{x})\right|$ will be roughly constant!

A good idea: Cauchy-Schwarz

$$\sum_{\mathbf{x}\in\mathbb{F}_q^n} \left|\frac{1_{\mathcal{C}}}{\sharp \mathcal{C}} \star f_p(\mathbf{x}) - \mathrm{unif}(\mathbf{x})\right| \; 1 \leq \sqrt{q^n} \sqrt{\sum_{\mathbf{x}\in\mathbb{F}_q^n} \left(\frac{1_{\mathcal{C}}}{\sharp \mathcal{C}} \star f_p(\mathbf{x}) - \mathrm{unif}(\mathbf{x})\right)^2}$$

$\longrightarrow$ The upper-bound: L_2-norm!

A natural approach: Parseval's identity

FOURIER TRANSFORM

- Scalar product and associated norms:

$$\langle f, g\rangle \stackrel{\text{def}}{=} \frac{1}{q^n}\sum_{\mathsf{y}\in\mathbb{F}_q^n} f(\mathsf{y})g(\mathsf{y}) \quad \text{and} \quad \|f\|_2 \stackrel{\text{def}}{=} \sqrt{\langle f, f\rangle}$$

- An Orthonormal Basis, characters (q prime):

$$\chi_{\mathsf{x}}(\mathsf{y}) \stackrel{\text{def}}{=} \mathrm{e}^{2i\pi\langle \mathsf{x},\mathsf{y}/q\rangle}$$

Fourier transform:

Given, $f : \mathbb{F}_q^n \to \mathbb{C}$,

$$\widehat{f}(\mathsf{x}) = \frac{1}{\sqrt{q^n}}\sum_{\mathsf{y}\in\mathbb{F}_q^n} f(\mathsf{y})\chi_{\mathsf{x}}(\mathsf{y}) = \sqrt{q^n}\ \langle f, \chi_{\mathsf{x}}\rangle$$

- Convolution:

$$\widehat{f\star g} = \sqrt{q^n}\ \widehat{f}\cdot\widehat{g}$$

Parseval identity: Fourier transform isometry for L_2

$$\|f-g\|_2 = \|\widehat{f}-\widehat{g}\|_2$$

We need to compute $\widehat{1_{\mathcal{C}}}$

Dual Code:

Given $\mathcal{C} \subseteq \mathbb{F}_q^n$,

$$\mathcal{C}^\star \stackrel{\text{def}}{=} \left\{ \mathbf{x} \in \mathbb{F}_q^n : \ \forall \mathbf{y} \in \mathcal{C} \ \chi_{\mathbf{x}}(\mathbf{y}) = 1 \right\} = \left\{ \mathbf{x} \in \mathbb{F}_q^n : \ \forall \mathbf{y} \in \mathbb{F}_q^n, \ \sum_i x_i y_i = 0 \right\}$$

$$\left(\text{characters of } \mathbb{R}^n \text{: } \chi_{\mathbf{x}}(\mathbf{y}) = \mathrm{e}^{2i\pi \langle \mathbf{x}, \mathbf{y} \rangle}, \mathbf{x} \in \Lambda^\star \iff \forall \mathbf{y}, \mathrm{e}^{2i\pi \langle \mathbf{x}, \mathbf{y} \rangle} = 1 \iff \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z} \right)$$

$\longrightarrow$ Dual code/lattice are defined in this way for Poisson summ. formula to be true

Fourier transform indicator code:

$$\widehat{1_{\mathcal{C}}} = \frac{\sharp \mathcal{C}}{\sqrt{q^n}} \, 1_{\mathcal{C}^\star}$$

SMOOTHING PARAMETER: AN UPPER-BOUND

arbitrary noise distribution f

$$\begin{aligned}
\Delta\left(\frac{1_{\mathcal{C}}}{\sharp\mathcal{C}} \star f, \text{unif}\right) &\leq \sqrt{q^n} \left\| \frac{1_{\mathcal{C}}}{\sharp\mathcal{C}} \star f - \text{unif} \right\|_2 \\
&= \sqrt{q^n} \left\| \frac{\sqrt{q^n}}{\sharp\mathcal{C}} \widehat{1_{\mathcal{C}}} \cdot \widehat{f} - \widehat{\text{unif}} \right\|_2 \\
&= \sqrt{q^n} \left\| \frac{\sqrt{q^n}}{\sqrt{q^n}\sharp\mathcal{C}} \sharp\mathcal{C}\, 1_{\mathcal{C}^\star} \cdot \widehat{f} - \frac{1}{\sqrt{q^n}} \delta_{\mathbf{0}} \right\|_2 \\
&= \sqrt{q^n} \sqrt{\sum_{\mathbf{c}^\star \in \mathcal{C}^\star \setminus \{\mathbf{0}\}} |\widehat{f}(\mathbf{x})|^2}
\end{aligned}$$

Upper-bound:

$$\Delta\left(\frac{1_{\mathcal{C}}}{\sharp\mathcal{C}} \star f, \text{unif}\right) \leq \sqrt{q^n} \sqrt{\textstyle\sum_{\mathbf{c}^\star \in \mathcal{C}^\star \setminus \{\mathbf{0}\}} |\widehat{f}(\mathbf{x})|^2}$$

If $f(x)$ depends only on $|\mathbf{x}|$ (radial),

$$\Delta\left(\frac{1_{\mathcal{C}}}{\sharp\mathcal{C}} \star f, \text{unif}\right) \leq \sqrt{q^n} \sqrt{\textstyle\sum_{t>0} N_t(\mathcal{C}^\star)\, |\widehat{f}(t)|^2}$$

where $N_t(\mathcal{C}^\star) \stackrel{\text{def}}{=} \sharp\{\mathbf{c} \in \mathcal{C}^\star : \ |\mathbf{c}| = t\}$

AN OPTIMAL UPPER-BOUND: THE RANDOM CASE

We need to upper-bound $N_t(\mathcal{C}^\star)$, but how?

AN OPTIMAL UPPER-BOUND: THE RANDOM CASE

We need to upper-bound $N_t(\mathcal{C}^\star)$, but how?

$\longrightarrow$ To understand first if our approach is meaningful, use random codes!

$$\begin{aligned}\mathbb{E}_{\mathcal{C}^\star}\left(\Delta\left(\frac{1_{\mathcal{C}}}{\sharp\mathcal{C}}\star f,\mathrm{unif}\right)\right) &\leq \mathbb{E}_{\mathcal{C}^\star}\left(\sqrt{q^n}\sqrt{\sum_{t>0}N_t(\mathcal{C}^\star)\,|\widehat{f}(t)|^2}\right)\\ &\leq \sqrt{q^n}\sqrt{\sum_{t>0}\mathbb{E}_{\mathcal{C}^\star}\left(N_t(\mathcal{C}^\star)\,|\widehat{f}(t)|^2\right)}\\ &= \sqrt{q^n}\sqrt{\sum_{t>0}\frac{\sharp\mathcal{S}_t}{\det\mathcal{C}^\star}\,|\widehat{f}(t)|^2}\end{aligned}$$

Bernoulli: our dream comes false

Choosing $f(\mathbf{x}) = p^{|\mathbf{x}|}(1-p)^{n-|\mathbf{x}|}$ leads to

$$np \geq \frac{n}{2}\left(1-\sqrt{2^R-1}\right)$$

to ensure $\mathbb{E}_{\mathcal{C}^\star}\left(\Delta\left(\frac{1_{\mathcal{C}}}{\sharp\mathcal{C}}\star f,\mathrm{unif}\right)\right)$ negligible **while**

$$\frac{n}{2}\left(1-\sqrt{2^{k/n}-1}\right) \gg t_{\mathrm{GV}}$$

UNIFORM DISTRIBUTION OVER A SPHERE

Using Bernoulli seems to be non-optimal. Which other distribution concentrating over $\mathcal{S}_{pn}$ could be chosen?

UNIFORM DISTRIBUTION OVER A SPHERE

Using Bernoulli seems to be non-optimal. Which other distribution concentrating over $\mathcal{S}_{pn}$ could be chosen?

$\longrightarrow 1_{\mathcal{S}_w}$ be the uniform distribution over $\mathcal{S}_w$

Krawtchouk polynomials: K_w

$$\widehat{1_{\mathcal{S}_w}}(\mathbf{x}) = \frac{1}{\sqrt{q^n}} K_w(|\mathbf{x}|)$$

Krawtchouk Polynomials enjoy the following fundamental properties

- $\langle K_w/\sqrt{\sharp\mathcal{S}_w}, K_t/\sqrt{\sharp\mathcal{S}_t}\rangle = q^n\ \delta_w^t$
- $(K_w)_w$ form a basis of radial functions

Fundamental consequence:

$$\sqrt{q^n}\sqrt{\sum_{t=0}^{n} \frac{\sharp\mathcal{S}_t}{\det \mathcal{C}^\star} \frac{\widehat{1}_{\mathcal{S}_w}(t)^2}{q^n \sharp\mathcal{S}_w^2}} = \sqrt{\frac{q^n}{\det(\mathcal{C}^\star)\cdot\sharp\mathcal{S}_w} \sum_{t=0}^{n} \frac{\sharp\mathcal{S}_t}{q^n} \left(\frac{K_w(|\mathbf{x}|)}{\sqrt{\sharp\mathcal{S}_w}}\right)^2} = \sqrt{\frac{q^n}{\det(\mathcal{C}^\star)\cdot\sharp\mathcal{S}_w}}$$

Using $f = 1_{\mathcal{S}_w}/\sharp\mathcal{S}_w$,

$$\Delta\left(\frac{q^n}{\sharp\mathcal{C}} 1_{\mathcal{C}} \star f,\ \text{unif}\right) \leq \sqrt{\frac{\det \mathcal{C}}{\sharp\mathcal{S}_w}}$$

$\longrightarrow$ Our dream comes true: $w \geq t_{\text{GV}}$ to ensure a negligible stat. distance

Bernoulli: a good choice!

Using Chernoff bound: $\Delta\left(\text{Ber}^{\otimes n}(p),\ \frac{1_{\mathcal{S}_{pn}}}{\sharp\mathcal{S}_{pn}}\right) \approx 0$

What about lattices?

KRAWTCHOUK VERSUS BESSEL

The same path can be followed for lattices:

1. Gaussian does not lead to the optimal smoothing parameter (Gaussian heuristic)
2. We use the uniform distribution over a ball
3. We recover the optimal parameter: Chernoff + uniform distribution over a ball

$\longrightarrow$ Krawtchouk polynomials were fundamental, we have the lattice-equivalent

$$\Big(\text{dictionary}\Big)$$

Bessel Function:

$$\widehat{1}_{\mathcal{B}_w}(\mathbf{y}) = \sqrt{\tfrac{w}{|\mathbf{y}|_2}}\, J_{n/2}(2\pi w|\mathbf{y}|_2) \text{ where } J_{n/2} \text{ Bessel function}$$

Bessel functions enjoy the same properties as Krawtchouk

- Orthogonal functions
- "Basis for radial functions"

BERNOULLI AND GAUSSIAN: SAME OBJECTS?

Our dictionary:

- ✓ LWE/Decoding: same combinatorial prop. in terms of determinant and volume
- ✓ Same approach to provide worst-to-average case reduction for LWE/Decoding
- ✓ Bernoulli $\longleftrightarrow$ Gaussian
- ✓ Krawtchouk $\longleftrightarrow$ Bessel

But, paradox:

- $\widehat{\text{Gauss}(\sigma)} = \text{Gauss}(1/\sigma)$
- But $\widehat{\text{Ber}}$ is not a Bernoulli...

Fourier theory shows a difference between Bernoulli and Gaussian. Fourier transforms of Bernoulli and Gaussian is not a natural object. Take the square root (next section)!

NON-RANDOM CASE

To get our upper-bound we used: $\mathbb{E}_{\mathcal{C}}\left(\{\mathbf{c} \in \mathcal{C} : \ |\mathbf{c}| = t\}\right) = \frac{\sharp \mathcal{S}_t}{\det \mathcal{C}}$

$\longrightarrow$ What happens for a fixed code/lattice as aimed in the reductions?

Linear programming bounds:

Both for codes and lattices,

$$N_t(\mathcal{C}) \leq \frac{F(d,t)}{\det \mathcal{C}}$$

where d minimum distance of code/lattice.

$\longrightarrow$ Linear programming bounds are obtained in the same way for codes and lattices (next section)

SOURCE OF HARDNESS

Self-reducibility:

Decoding/LWE hardness can be reduced to their worst-case variant

$\longrightarrow$ But is their hardness following from other problems?

An important answer to give:

Lattice-case: finding short vectors is historically believed to be hard, not LWE

Quantum Regev's reduction

SOURCE OF HARDNESS: FIND SHORT CODEWORDS/LATTICES VECTORS

Quantum Regev's reduction:

Any classical algorithm solving Decoding/LWE, can be turned into a quantum algorithm finding short vectors in a code/lattice

Be careful: decoding at distance t implies finding short codewords/lattice vectors of weight

$$f^{\perp}(t)$$

But where is $f^{\perp}$ coming from?

$\longrightarrow$ As for the smoothing parameter it depends of the chosen noise!

$\left(|\mathsf{x}\rangle \right)_{\mathsf{x}\in\mathbb{F}_q^n}$ orthonormal basis of an Hilbert space $\mathcal{H}$ with dimension q^n

Computation:

- Given $h : \mathbb{F}_q^n \to \mathbb{F}_q^n$ one-to-one s.t h and h^{-1} computable in time T,

$$|\mathsf{x}\rangle \longmapsto |h(\mathsf{x})\rangle \text{ computable quantumly in time } O(T)$$

- Given $h : \mathbb{F}_q^n \to \mathbb{F}_q^n$ computable in time T,

$$|\mathsf{x}\rangle\,|\mathsf{y}\rangle \longmapsto |\mathsf{x}\rangle\,|\mathsf{y} + h(\mathsf{x})\rangle \text{ computable quantumly in time } O(T)$$

From quantum computing to classical information: measurement

- Any quantum state $|\psi\rangle \in \mathcal{H}$ has norm 1,

$$|\psi\rangle = \sum_{\mathsf{x}\in\mathbb{F}_q^n} \lambda_{\mathsf{x}}\,|\mathsf{x}\rangle\,,\ (\lambda_{\mathsf{x}})_{\mathsf{x}} \in \mathbb{C},\ \text{then}\ \sum_{\mathsf{x}\in\mathbb{F}_q^n} |\lambda_{\mathsf{x}}|^2 = 1$$

- Extracting from $|\psi\rangle$ classical information,

$$|\psi\rangle \longrightarrow \mathsf{x} \in \mathbb{F}_q^n \text{ with probability } |\lambda_{\mathsf{x}}|^2$$

One of the most useful tool in quantum computing: QFT

Classical and Quantum Fourier transforms over $\mathbb{F}_q^n$ (q prime)

Classical Fourier Transform	Quantum Fourier Transform: QFT
$f = (f(\mathbf{x}))_{\mathbf{x}\in\mathbb{F}_q^n}$	$\lvert\psi_f\rangle = \sum_{\mathbf{x}\in\mathbb{F}_q^n} f(\mathbf{x})\lvert\mathbf{x}\rangle$ $(\lVert f\rVert_2 = 1)$
$\widehat{f}(\mathbf{x}) = \frac{1}{\sqrt{q^n}} \sum_{\mathbf{y}\in\mathbb{F}_q^n} f(\mathbf{y}) e^{2i\pi\langle \mathbf{x},\mathbf{y}\rangle/q}$	$\mathrm{QFT}\lvert\psi\rangle \stackrel{\text{def}}{=} \widehat{\lvert\psi_f\rangle} = \sum_{\mathbf{x}\in\mathbb{F}_q^n} \widehat{f}(\mathbf{x})\lvert\mathbf{x}\rangle$

$\longrightarrow$ In particular: $\forall \mathbf{x} \in \mathbb{F}_q^n$, $\mathbf{QFT}\lvert\mathbf{x}\rangle = \frac{1}{\sqrt{q^n}} \sum_{\mathbf{y}\in\mathbb{F}_q^n} e^{2i\pi\langle \mathbf{x},\mathbf{y}\rangle/q}\lvert\mathbf{y}\rangle$

$\lvert\mathbf{x}\rangle \mapsto \mathrm{QFT}\lvert\mathbf{x}\rangle$ is quantum efficiently computable!

(quantum) Poisson summation formula

QFT and duality: "quantum Poisson summation formula"

$\mathcal{C} \subseteq \mathbb{F}_q^n$ be a code,

$$\mathrm{QFT} \sum_{\mathbf{c}\in\mathcal{C},\mathbf{e}} f(\mathbf{e}) \,|\mathbf{c}+\mathbf{e}\rangle = \sharp\mathcal{C} \cdot \sum_{\mathbf{c}^\star\in\mathcal{C}^\star} \widehat{f}(\mathbf{c}^\star) \,|\mathbf{c}^\star\rangle$$

Fundamental remark:

To compute short $\mathbf{c}^\star \in \mathcal{C}^\star$: build $\sum_{\mathbf{c}\in\mathcal{C},\mathbf{e}} f(\mathbf{e}) \,|\mathbf{c}+\mathbf{e}\rangle$

STARTING THE REDUCTION: A DECODING ORACLE

$$\mathcal{A}(A, sA + e) \longrightarrow e \text{ when } \mathbb{P}(e = x) = |f(x)|^2$$

1. We build,
$$\sum_s |sA\rangle \text{ and } \sum_e f(e)\,|e\rangle$$
2. Combine and sum the above state,
$$\sum_{s,e} f(e)\,|As\rangle\,|sA + e\rangle$$
3. Apply the "Decoding/LWE" solver to remove the first register,
$$\sum_{s,e} f(e)\,|As - \mathcal{A}(A, sA + e)\rangle\,|sA + e\rangle = \sum_{s,e} f(e)\,|0\rangle\,|sA + e\rangle$$

Be careful:

Cheat in the last step: it is important that $|f|^2$ is close to the distribution in Decoding/LWE-problem that $\mathcal{A}$ solves

$$\mathcal{C} = \left\{ \mathsf{sA} : \mathsf{s} \in \mathbb{F}_q^n \right\}$$

1. Apply the QFT,

$$\sum_{\mathsf{s},\mathsf{e}} f(\mathsf{e}) \left|0\right\rangle \left|\mathsf{sA} + \mathsf{e}\right\rangle \xrightarrow{\text{QFT}} \sharp\mathcal{C} \cdot \sum_{\mathsf{c}^\star \in \mathcal{C}^\star} \widehat{f}(\mathsf{c}^\star) \left|0\right\rangle \left|\mathsf{c}^\star\right\rangle$$

2. Measure,

$$\text{we obtain } \mathsf{c}^\star \in \mathcal{C}^\star \text{ with probability } \sharp\mathcal{C} \cdot \left|\widehat{f}(\mathsf{c}^\star)\right|^2$$

$$\longrightarrow \text{Where does } \left|\widehat{f}\right|^2 \text{ concentrate?}$$

CODE-CASE: NOISE DISTRIBUTION

The natural noise choice:

$$f = \sqrt{\mathrm{Ber}(p)}, \text{ i.e. } f(\mathbf{x}) = \sqrt{p^{|\mathbf{x}|}(1-p)^{n-|\mathbf{x}|}}$$

Its Fourier transform:

$$\widehat{f} = \sqrt{\mathrm{Ber}(p^{\perp})} \quad \text{where } p^{\perp} \stackrel{\text{def}}{=} \tfrac{1}{2} - \sqrt{p(1-p)}$$

$\longrightarrow$ Decoding at distance $\approx pn$ implies finding codewords of weight $p^{\perp}n$

Is $p^{\perp}$ admits an interpretation?

CODE-CASE: NOISE DISTRIBUTION

The natural noise choice:

$$f = \sqrt{\mathrm{Ber}(p)}, \text{ i.e. } f(\mathbf{x}) = \sqrt{p^{|\mathbf{x}|}(1-p)^{n-|\mathbf{x}|}}$$

Its Fourier transform:

$$\widehat{f} = \sqrt{\mathrm{Ber}(p^{\perp})} \quad \text{where } p^{\perp} \stackrel{\text{def}}{=} \tfrac{1}{2} - \sqrt{p(1-p)}$$

$\longrightarrow$ Decoding at distance $\approx pn$ implies finding codewords of weight $p^{\perp}n$

Is $p^{\perp}$ admits an interpretation? Yes!

A magic quantity:

$p^{\perp}n$ is the first zero of the Krawtchouk polynomial K_{pn}

AND THE LATTICE-CASE?

As we can expected, exactly the same phenomenon with lattices

but with Bessel functions

Regev's reduction for lattices:

- Solving LWE with noise norm $t \stackrel{\text{def}}{=} \sqrt{n}\frac{\sigma}{\sqrt{2\pi}}$ thanks to Gauss(σ)
- QFT$\sqrt{\text{Gauss}(\sigma)} = \sqrt{\text{Gauss}(1/(2\sigma))}$
- We measure $\mathbf{x}^\star \in \Lambda_q(\mathbf{A})^\star$ of norm,

$$t^\perp = \sqrt{n}\frac{1}{2\sigma\sqrt{2\pi}} = \frac{n}{4\pi t} \text{ which is first zero of } x \mapsto J_{n/2}(2\pi\, t\, x)$$

Our dictionary:

✓ Krawtchouk $\longleftrightarrow$ Bessel

AN INTRIGUING CONNECTION: FIRST LINEAR PROGRAMMING BOUND

$p \mapsto p^{\perp}$ and $t \mapsto t^{\perp}$ magic Krawtchouk/Bessel quantities of Regev's reduction

$\longrightarrow$ They also appear in sphere packing-bound for codes and lattices!

Sphere packing bound:

Fix a d, find the code/lattice $\mathcal{C}$ with minimum distance d and with the largest volume $1/\det(\mathcal{C})$

First-Linear programming bound:

For all code $\mathcal{C}$ (lattice Λ) with minimum distance $\geq d$:

$$\frac{1}{\det \mathcal{C}} \leq \frac{\sharp \mathcal{S}_{d^{\perp}}}{q^n} \quad \text{and} \quad \frac{1}{\det \Lambda} \leq \mathrm{Vol}\left(\mathcal{B}_{d^{\perp}}\right)$$

$\longrightarrow$ These bounds are obtained via exactly the same technique!

FIRST LINEAR PROGRAMMING BOUND

Let $f : \mathbb{F}_2^n \,/\, \mathbb{R}^n \to \mathbb{R}$ be such that

$$(1) : f(\mathbf{x}) \leq 0 \text{ for } |\mathbf{x}| \geq d_{\min}(\mathcal{C}) \quad \text{and} \quad (2) : \widehat{f}(\mathbf{t}) \geq 0 \text{ for all } \mathbf{t}.$$

Then,

$$\frac{1}{\det \mathcal{C}} \,/\, \frac{1}{\det \Lambda} \leq \frac{f(0)}{\widehat{f}(0)}.$$

Proof:

By Poisson,

$$\sum_{\mathbf{x}\in\Lambda} f(\mathbf{x}) = \frac{1}{|\det(\Lambda)|} \sum_{\mathbf{t}\in\Lambda^\star} \widehat{f}(\mathbf{t}).$$

$$\begin{aligned}
\sum_{\mathbf{x}\in\Lambda} f(\mathbf{x}) &= f(0) + \sum_{\mathbf{x}\neq 0, \mathbf{x}\in\Lambda} \underbrace{f(\mathbf{x})}_{\leq 0} \leq f(0) \\
\frac{\hat{f}(0)}{|\det(\Lambda)|} &\leq \frac{1}{|\det(\Lambda)|} \sum_{\mathbf{t}\in\Lambda^\star} \underbrace{\hat{f}(\mathbf{t})}_{\geq 0} \\
&\Downarrow \\
\frac{\hat{f}(0)}{|\det(\Lambda)|} &\leq f(0)
\end{aligned}$$

CONCLUSION

- Fourier theory appears crucially in Regev's reduction: same tools for both codes and lattices
- Bernoulli and Gaussian are the same objects when looking the Fourier transform of their square root

  $\longrightarrow$ They involve first root of Krawtchouk and Bessel!

- Regev's reduction is deeply related to sphere packing bounds

A LITTLE BIT ABOUT PACKING BOUNDS

PACKING BOUNDS

Packing bound:

We will bound $\sharp\mathcal{C}$ as function of its minimum distance

$$\max\left\{\sharp\mathcal{C} : \ \mathcal{C} \subseteq \mathbb{F}_2^n \text{ and minimum distance } d\right\}$$

The most fruitful approach to get the best $\Big($asymptotic$\Big)$ packing bounds:

theory of association schemes

THE ELIAS-BASSALYGO LEMMA

Packing bounds are deeply related to packing bound for spherical codes,

i.e., subsets of $\mathcal{S}_t$ $\left(\text{Hamming sphere with radius } t\right)$

Elias-Bassalygo lemma:

For any $\mathcal{C} \subseteq \mathbb{F}_2^n$ with minimum distance d and any radius t,

$$\sharp\mathcal{C} \leq \frac{2^n}{\binom{n}{t}} \max\left\{\sharp\mathcal{D}_{\text{sph}} : \mathcal{D}_{\text{sph}} \subseteq \mathcal{S}_t \text{ with minimum distance } d\right\}$$

Consequence:

Two approaches to get packing bounds:

1. Bound directly $\sharp\mathcal{C}$ where $\mathcal{C} \subseteq \mathbb{F}_2^n$
2. Bound $\sharp\mathcal{C}_{\text{sph}}$ where $\mathcal{C}_{\text{sph}}$ is a spherical code, *i.e.*, $\mathcal{C}_{\text{sph}} \subseteq \mathcal{S}_t$ and then apply Elias-Bassalygo lemma

$\longrightarrow$ We will consider association schemes with ambiant space $\mathbb{F}_2^n$ or $\mathcal{S}_t$

ASSOCIATION SCHEMES: ADJACENCY MATRICES

Metric space and adjacency matrices:

(X, τ, n) be a finite metric space with $\tau : X \times X \to \{0, \dots, n\}$.

It associated adjacency matrices $\mathbf{D}_i \in \mathbb{C}^{|X| \times |X|}$ are,

$$\forall x, y \in X, \quad \mathbf{D}_i(x, y) \stackrel{\text{def}}{=} \begin{cases} 1 \text{ if } \tau(x, y) = i \\ 0 \text{ otherwise} \end{cases}$$

- Typical cases: $X = \mathbb{F}_2^n$ Hamming scheme or $X = \mathcal{S}_t$ (Hamming sphere with radius t)

  Johnson scheme for the Hamming distance

ASSOCIATION SCHEMES: A TRIANGLE CONDITION

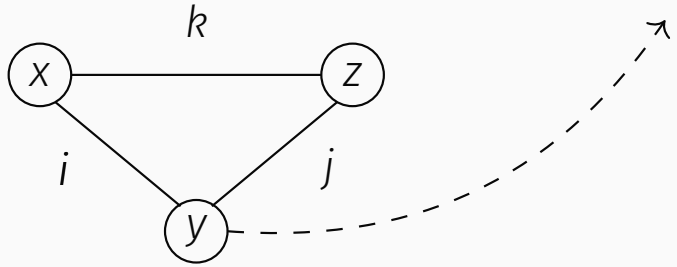
Association scheme:

(X, τ, n) is a (metric) association scheme if there exists an integer $p_{i,j}^k$ s.t,

$$\forall x, z \in X \text{ s.t } \tau(x,z) = k, \quad p_{i,j}^k = \sharp\{y \in X : \ \tau(x,y) = i \text{ and } \tau(y,z) = j\}$$

and $p_{1,k}^{k+1} \neq 0$.

The number of y only depends of i, j and k



Crucial consequences:

- $p_{i,j}^k = p_{j,i}^k$ because τ symmetric as distance
- $\mathbf{D}_i \cdot \mathbf{D}_j = \sum_{k=0}^n p_{i,j}^k \cdot \mathbf{D}_k$

$\longrightarrow$ Vect $(\mathbf{D}_i : \ 0 \leq i \leq n)$ forms a commutative algebra $\subseteq \mathbb{C}^{|X| \times |X|}$

$\mathrm{Vect}\,(\mathbf{D}_i : \ 0 \leq i \leq n)$ forms a commutative algebra $\subseteq \mathbb{C}^{|X|\times|X|}$ and the $\mathbf{D}_i$ are symmetric

$\longrightarrow$ The $\mathbf{D}_i$ share common orthogonal eigenspaces!

The matrices $\mathbf{E}_i$:

It exists orthogonal projectors $\mathbf{E}_j \in \mathbb{C}^{|X|\times|X|}$ such that,

$$\forall i \in \{0,\ldots,n\}, \quad \mathbf{D}_i = \sum_{j=0}^{n} p_i(j)\mathbf{E}_j$$

$\longrightarrow$ Matrices $\mathbf{D}_i$ and $\mathbf{E}_j$ generate the same space!

q-numbers:

$$\forall j \in \{0,\ldots,n\}, \quad \mathbf{E}_j = \frac{1}{|X|}\sum_{i=0}^{n} q_j(i)\mathbf{D}_i$$

$$\mathbf{D}_i = \sum_{j=0}^{n} p_i(j)\mathbf{E}_j \quad \text{and} \quad \mathbf{E}_j = \frac{1}{|X|}\sum_{i=0}^{n} q_j(i)\mathbf{D}_i$$

Fourier transform and its inverse: given $f : \{0, \ldots, n\} \to \mathbb{C}$

$$\widehat{f}(x) \stackrel{\text{def}}{=} \sum_{y=0}^{n} f(y)p_y(x) \quad \text{and} \quad \widetilde{f}(x) \stackrel{\text{def}}{=} \sum_{y=0}^{n} f(y)q_y(x)$$

$$\mathbf{D}^f \stackrel{\text{def}}{=} \sum_{x=0}^{n} f(x)\mathbf{D}_x \quad ; \quad \mathbf{E}^g \stackrel{\text{def}}{=} \sum_{x=0}^{n} g(x)\mathbf{E}_x$$

From the decomposition of the $\mathbf{D}_i$ and $\mathbf{E}_j$ in each basis

$$\mathbf{D}^f = \mathbf{E}^{\widehat{f}} \quad \text{and} \quad \mathbf{E}^f = \mathbf{D}^{\widetilde{f}}$$

Dirac/Bra-ket notation:

$X = \{x_1, \ldots, x_N\}$. For any x_i, the vector $|x_i\rangle$ is zero except at the ith entry where it is 1.

$$|v\rangle = \begin{pmatrix} v_1 \\ \vdots \\ v_N \end{pmatrix} = \sum_{i=1}^{N} v_i |x_i\rangle \quad \text{and} \quad \langle v| = \begin{pmatrix} \overline{v_1} & \ldots & \overline{v_N} \end{pmatrix}$$

CODE AND WEIGHT DISTRIBUTION

Our aim is to upper-bound the size of a code with minimum distance d

- **Code**: given (X, τ, n) an association scheme, **a code** $\mathcal{C}$ is a subset of X.

  Its **minimum distance**:

$$d \stackrel{\text{def}}{=} \min\left(\tau(c, c') : \ c, c' \in \mathcal{C} \text{ and } c \neq c'\right)$$

Given a code $\mathcal{C} \subseteq X$,

$$|\psi_{\mathcal{C}}\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{\sharp\mathcal{C}}} \sum_{c \in \mathcal{C}} |c\rangle$$

- **Weight Distribution:** $a(t) = \frac{1}{\sharp\mathcal{C}} \cdot \sharp\left((c, c') \in \mathcal{C}^2 : \ \tau(c, c') = t\right) = \langle\psi_{\mathcal{C}}| \, \mathsf{D}_t \, |\psi_{\mathcal{C}}\rangle$

$$\sharp\mathcal{C} = \sum_{t=0}^{n} a(t), \quad a(0) = 1 \quad \text{and} \quad a(t) = 0 \text{ if } t \in \{1, \ldots, d-1\}$$

A FIRST LINEAR PROGRAM

Aim: to derive bounds on $\sharp\mathcal{C}$ with minimum distance d

$$\left(a(t) = \frac{\sharp\left((c,c')\in\mathcal{C}^2:\, \tau(c,c')=t\right)}{\sharp\mathcal{C}} \geq 0\,,\, a(0)=1, a(t)=0 \text{ if } t<d \text{ and } \sharp\mathcal{C} = \sum_t a(t)\right)$$

A first linear program:

$$\max \sum_{t\in[\![0,n]\!]} u(t) \text{ under the constraints}$$
$$u(0) = 1$$
$$u(t) = 0 \text{ for } t \in \{1,\ldots,d-1\}$$
$$u(t) \geq 0 \text{ for } t \in \{d,\ldots,n\}$$

$\longrightarrow$ Solving this linear program does not yield interesting bounds: add constraints

Fundamental idea:

Add a constraint coming from the duality!

DUAL DISTRIBUTION AND MACWILLIAMS IDENTITY

$$a(t) = \langle \psi_{\mathcal{C}} | \, \mathsf{D}_t \, | \psi_{\mathcal{C}} \rangle \text{ where } |\psi_{\mathcal{C}}\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{\sharp \mathcal{C}}} \sum_{c \in \mathcal{C}} |c\rangle$$

Dual code distribution:

$$a'(i) \stackrel{\text{def}}{=} \langle \psi_{\mathcal{C}} | \, \mathsf{E}_i \, | \psi_{\mathcal{C}} \rangle = \langle \psi_{\mathcal{C}} | \, \frac{1}{|X|} \sum_{t=0}^{n} q_i(t) \mathsf{D}_t \, | \psi_{\mathcal{C}} \rangle = \sum_{t=0}^{n} q_i(t) a(t)$$

If $\mathcal{C}$ is linear, then

$$a'(i) = \sharp \left\{ (c^\perp, d^\perp) \in \mathcal{C}^\perp : \ \tau(c^\perp, d^\perp) = i \right\}$$

Otherwise, if $\mathcal{C}$ is not linear maybe even not integers... But in any case:

MacWilliams identity:

$$\forall i \in \{0, \ldots, n\}, \quad a'(i) \geq 0$$

Proof: the E_i are projectors, *i.e.*, $\mathsf{E}_i = \sum_t \left| v_t^{(i)} \right\rangle \left\langle v_t^{(i)} \right|$ and,

$$a'(i) = \langle \psi_{\mathcal{C}} | \sum_t \left| v_i^{(t)} \right\rangle \left\langle v_i^{(t)} \right| | \psi_{\mathcal{C}} \rangle = \sum_t \left\langle \psi_{\mathcal{C}} \middle| v_i^{(t)} \right\rangle \left\langle v_i^{(t)} \middle| \psi_{\mathcal{C}} \right\rangle = \sum_t \left| \left\langle \psi_{\mathcal{C}} \middle| v_i^{(t)} \right\rangle \right|^2 \geq 0$$

Delsarte's linear program

Delsarte's Linear Program:

$$\mathrm{DLP}(n,d) \stackrel{\text{def}}{=} \max \sum_{t\in[\![0,n]\!]} u(t) \text{ under the constraints}$$

$$u(0) = 1$$

$$u(t) = 0 \text{ for } t \in \{1,\dots,d-1\}$$

$$u(t) \geq 0 \text{ for } t \in \{d,\dots,n\}$$

$$\sum_{t\in[\![0,n]\!]} u(t)q_i(t) \geq 0 \text{ for } i \in \{0,\dots,n\}.$$

Given a code $\mathcal{C}$ with minimum distance d, its weight distribution $a(t)$ is a solution of Delsarte's linear program,

$$\sharp\mathcal{C} \leq \mathrm{DLP}(n,d)$$

$\longrightarrow$ MacWilliams identity shows that the weight distribution verifies the last condition of Delsarte's Linear Program

Dual Delsarte's Linear Program

Dual Delsarte Linear Program:

Let $d \in \{0, \ldots, n\}$ and $f : \{0, \ldots, n\} \longrightarrow \mathbb{R}$ be a function such that,

$$\widehat{f} \geq 0 \quad , \quad \widehat{f}(0) > 0 \quad , \quad \forall x \geq d,\ f(x) \leq 0.$$

Then,

$$\max\left\{\sharp\mathcal{C} :\ \mathcal{C} \subseteq \mathbb{F}_2^n \text{ and minimum distance } d\right\} \leq \mathrm{DLP}(n, d) \leq |\mathrm{X}| \cdot \frac{f(0)}{\widehat{f}(0)}.$$

Obtained bounds via the choice of a "magic" function f with $\mathrm{X} = \mathbb{F}_2^n$ or $\mathrm{X} = \mathcal{S}_t$

(combined with Elias-Bassalygo lemma),

- Plotkin
- Hamming
- Elias-Bassalygo
- MRRW1&2 (McEliece, Rodemich, Rumsay, Welch) best bounds from '77

$$\mathbf{D}_i = \sum_{j=0}^{n} p_i(j)\mathbf{E}_j \quad \text{and} \quad \mathbf{E}_j = \frac{1}{|X|}\sum_{i=0}^{n} q_j(i)\mathbf{D}_i$$

Fourier Transform and Its Inverse: given $f : \{0, \ldots, n\} \to \mathbb{C}$

$$\widehat{f}(x) \stackrel{\text{def}}{=} \sum_{y=0}^{n} f(y)p_y(x) \quad \text{and} \quad \widetilde{f}(x) \stackrel{\text{def}}{=} \sum_{y=0}^{n} f(y)q_y(x)$$

Do they really define Fourier transforms?

- When $X = \mathbb{F}_2^n$: it corresponds to Fourier transform of radial functions!
- When $X = \mathcal{S}_t$: Fourier theory is not defined, $\mathcal{S}_t$ not a group

THE CASE OF THE SPHERE

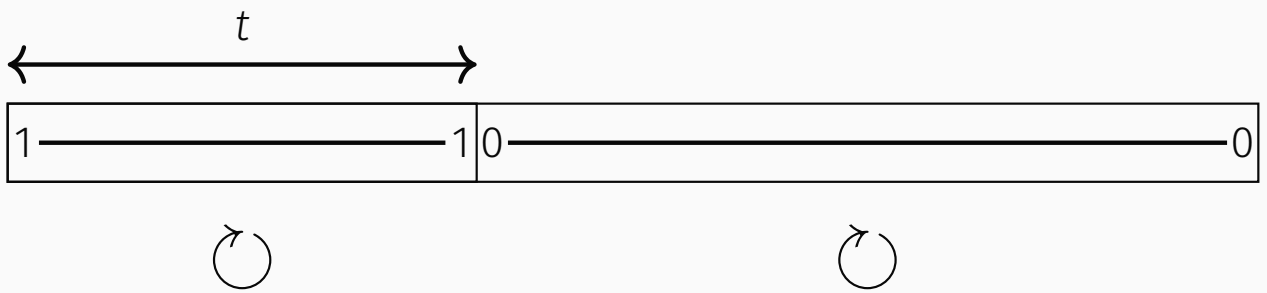
The Hamming sphere $\mathcal{S}_t$ is not a group: no Fourier theory

But. . .

Sphere as a Quotient:

The Hamming sphere $\mathcal{S}_t \subseteq \mathbb{F}_2^n$ can be identified as a quotient of the symmetric group:

$$\mathcal{S}_t \cong \mathfrak{S}_n / \Big(\mathfrak{S}_t \times \mathfrak{S}_{n-t} \Big)$$



$\longrightarrow$ Fourier theory over $\mathcal{S}_t$ derives from Fourier theory over $\mathfrak{S}_n$

$\Big($non-commutative group$\Big)$

Fourier transform:

Given a group G and $f : G \to \mathbb{C}$. Its Fourier transform at the representation ρ is

$$\widehat{f}(\rho) = \sum_{g \in G} f(g)\rho(g)$$

$\longrightarrow$ When G is commutative representations are one dimensional objects

GELFAND PAIRS

- Homogenous Space: G be a group acting transitively on finite set X
- Isotropy subgroup: given $x_0 \in X$, $N = \{s \in G : \ s \cdot x_0 = x_0\}$

$\longrightarrow$ The group G acts on the coset space G/N and there is an isomorphisim between X and G/N respecting the action of G

Space $L(X)$:

$$L(X) = \{f : X \to \mathbb{C}\} \text{ with the } G \text{ action: } \forall g \in G,\ g \cdot f : y \mapsto f(g^{-1} \cdot y)$$

Gelfand Pair:

For all function $f : X = G/N \to \mathbb{C}$ which is also N-left invariant and any irreducible representation (V, ρ) it exists a basis of V such that,

$$\widehat{f}(\rho) = \begin{pmatrix} \star & 0 \\ 0 & 0 \end{pmatrix}$$

- It mimics the Abelian case for bi-invariant functions
- The basis in which the Fourier transforms are one-dimensional corresponds to the basis $\mathbf{E}_i$ of association schemes (also called spherical functions)

SPHERE PACKING IN R^n?

An equivalent of association schemes and Gelfand pairs also exists for lattices:

2-point-homogenous spaces, zonal functions

The "same" theory than for codes $\left(\text{linear program}\right)$ leads to the best known asymptotic packing bound $\left(\text{Kabatiasnky\&Levenshtein}\right)$

CONCLUSION

FOURIER ANALYSIS: A POWERFUL COMMON TOOL

Fourier duality:

Powerful tool to identify source of hardness in code- and lattice-based cryptography

$\longrightarrow$ Both codes and lattices behave in the same way via Fourier!

WHAT ABOUT STRUCTURED CODES VERSUS STRUCTURED LATTICES?

Structured versions of LWE are often considered: MLWE with the number field framework

$\longrightarrow$ Still a code-based analogy: function-fields

Number fields	Function fields
$\mathbb{Q}$	$\mathbb{F}_q(T)$
$\mathbb{Z}$	$\mathbb{F}_q[T]$
Prime numbers $q \in \mathbb{Z}$	Irreducible polynomials $Q \in \mathbb{F}_q[T]$
$K = \mathbb{Q}[X]/(f(X))$	$K = \mathbb{F}_q(T)[X]/(f(T,X))$
$\mathcal{O}_K =$ Integral closure of $\mathbb{Z}$	$\mathcal{O}_K =$ Integral closure of $\mathbb{F}_q[T]$
Dedekind domain	*Dedekind* domain
characteristic 0	**characteristic > 0**

ONE FUNDAMENTAL DIFFERENCE: BASIS REDUCTION

A powerful tool for lattice-based cryptography:

Basis reduction!

$\longrightarrow$ It can be adapted to codes (LLL, BKZ, . . .)

But the code-based analogue does not give competitive attacks versus ISD/Dual-attacks

- The Hamming metric is coarse: the profile a basis is quickly trivial
- LLL for codes proves the Griesmer bound for codes as LLL for lattices proves Hermitte bound