SMOOTHING BOUNDS FOR CODES AND LATTICES: SYSTEMATIC STUDY AND NEW BOUNDS

Thomas Debris-Alazard
Inria

Léo Ducas
CWI, Leiden University

Nicolas Resch
CWI→University of Amsterdam

Jean-Pierre Tillich
Inria

SMOOTHING

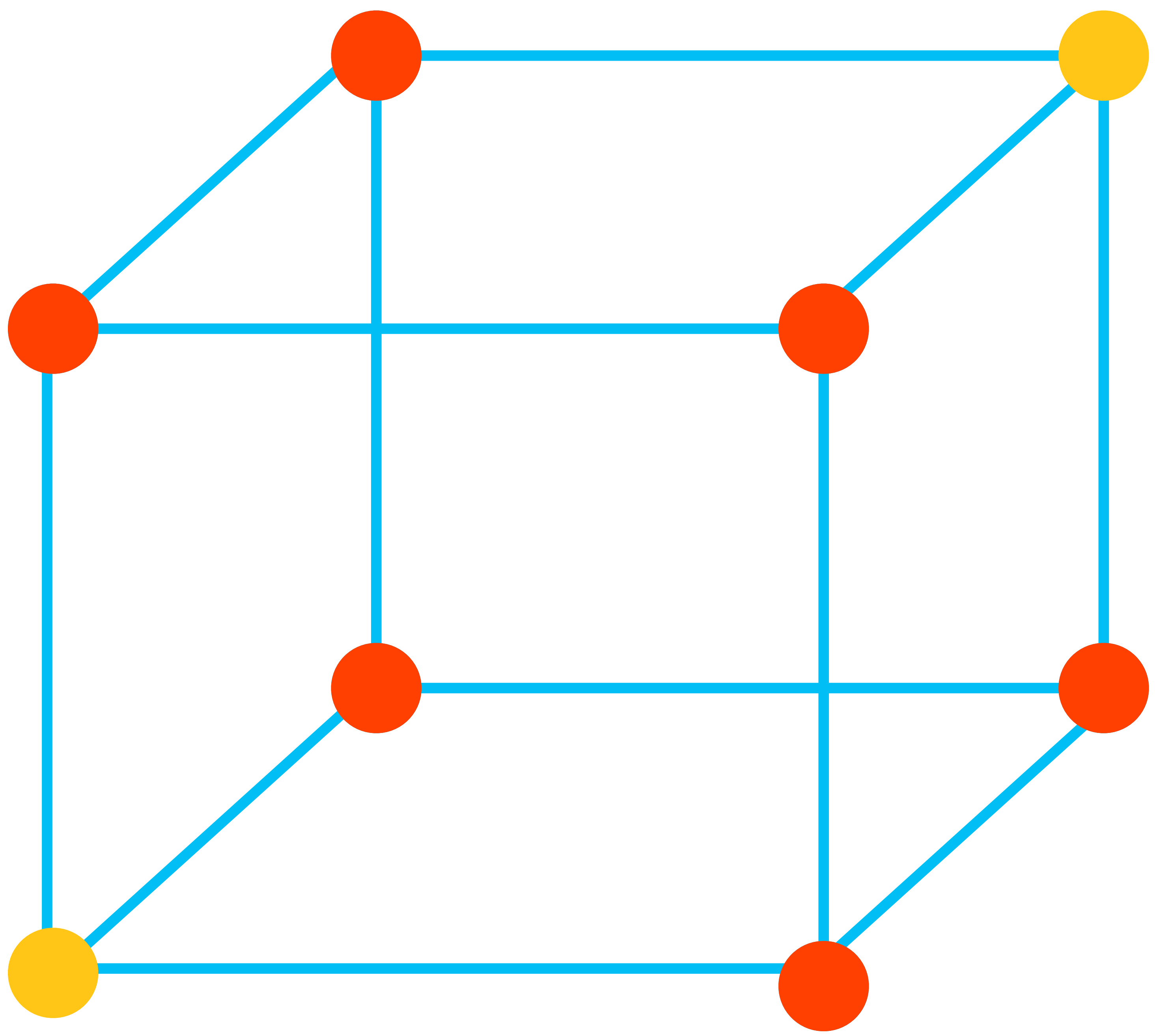
SMOOTHING

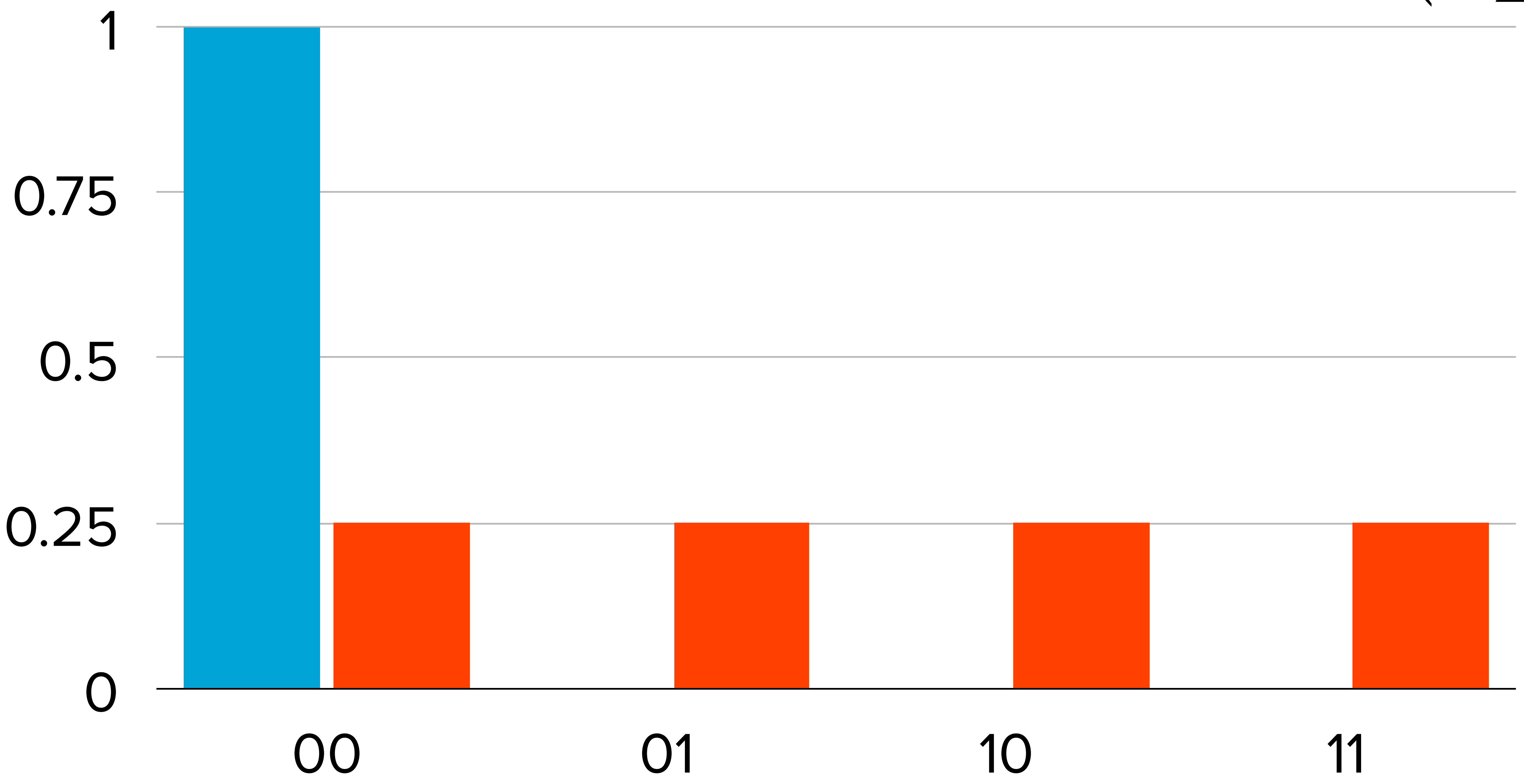
$\mathscr{C} = \{000, 111\}$ $\qquad$ $\mathbf{e} = \text{unif. wt. } 0{,}1$ $\qquad$ $\mathbf{c} + \mathbf{e} \sim \text{Unif}\left(\mathbb{F}_2^3\right)$

$\mathbf{c} \sim \text{Unif}(\mathscr{C})$

$$\Updownarrow$$

$\mathbf{e} \mod \mathscr{C} \sim \text{Unif}\left(\mathbb{F}_2^3/\mathscr{C}\right)$





SMOOTHING BOUNDS

- Given $\mathscr{C} \leq \mathbb{F}_2^n$ of dim. k, quantify closeness between $\mathbf{u} \sim \text{Unif}\left(\mathbb{F}_2^n/\mathscr{C}\right)$ and $\mathbf{e} \mod \mathscr{C}$
- Use statistical / ℓ_1-distance:

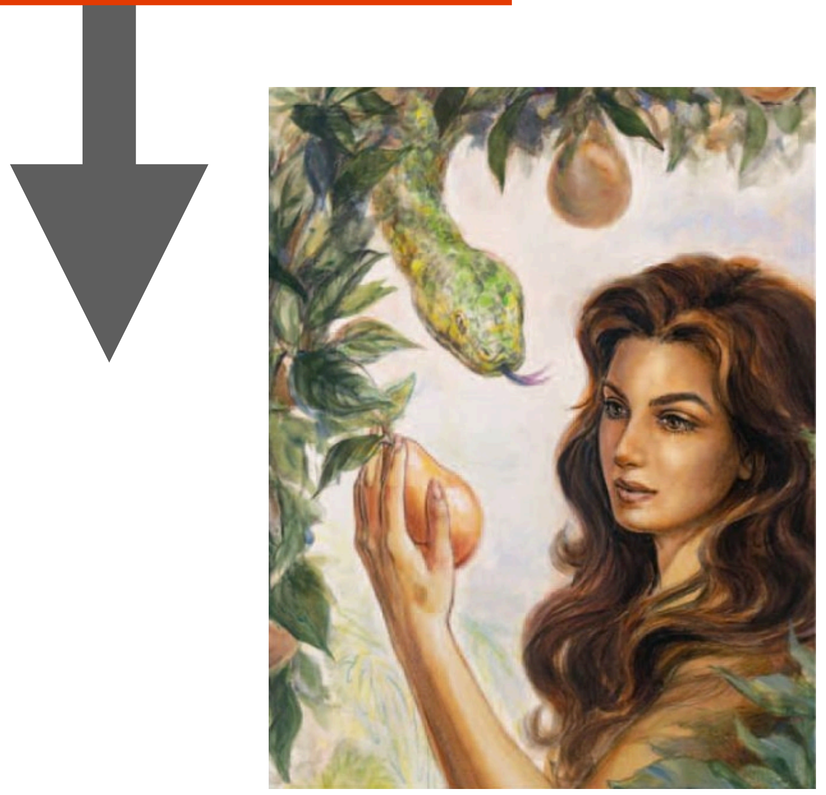
$$\Delta(\mathbf{u}, \mathbf{e} \mod \mathscr{C}) = \max_{S \subseteq \mathbb{F}_2^n/\mathscr{C}} \left(\Pr[\mathbf{u} \in S] - \Pr[\mathbf{e} \mod \mathscr{C} \in S]\right)$$
$$= \frac{1}{2} \sum_{\mathbf{x} \in \mathbb{F}_2^n/\mathscr{C}} \left|\Pr[\mathbf{u} = \mathbf{x}] - \Pr[\mathbf{e} \mod \mathscr{C} = \mathbf{x}]\right|$$

Question: How "large" must the noise $\mathbf{e}$ be to have

$$\Delta(\mathbf{u}, \mathbf{e} \mod \mathscr{C}) \leq \text{negl}(n)\,?$$

- Measure "largeness" as $t = \mathbb{E}[\,|\mathbf{e}|\,]$ where $|\mathbf{x}| = |\{i \in [n] : x_i = 1\}|$

MOTIVATIONS



- Wiretap channel
  - [Mirghsemi-Belfiore'14] (Gaussian noise)
- Lattice trapdoors
  - [Gentry-Peikert-Vaikuntanathan'08]
- Mixing on Markov chains

- Reductions to average-case problems
  - we'll discuss this later…

TRANSLATING STRATEGY

[MR07, GPV08]

LATTICES	CODES
– Use *Gaussian* noise	– Use *Bernoulli* noise
– Poisson summation formula: sum over lattice becomes sum of Fourier transform over dual lattice	– Poisson summation formula applies to codes too! Get summation over $\mathscr{C}^* = \{\mathbf{c}^* : \langle \mathbf{c}^*, \mathbf{c} \rangle = \mathbf{0} \ \forall \mathbf{c} \in \mathscr{C}\}$
– Tail bounds for Gaussians (Banaszczyk 93)	– Code version quite weak…
– More recently [ADRS15]: LP bounds [L79]	– Code LP bounds quite effective! [MRRW77]

Lattice strategy translates flawlessly!

Result fairly weak… Can we improve it?

OUR STRATEGY

PERIODIZATION

f made uniform on cosets of $\mathscr{C}$: $f^{\mathscr{C}}(\mathbf{x}) = f^{\mathscr{C}}(\mathbf{x}+\mathbf{c})$ $\forall \mathbf{x} \in \mathbb{F}_2^n, \mathbf{c} \in \mathscr{C}$

- For function f on $\mathbb{F}_2^n$, $f^{\mathscr{C}}$ denotes its periodization w.r.t. $\mathscr{C}$

$$f^{\mathscr{C}}(\mathbf{x}) = \sum_{\mathbf{c}\in\mathscr{C}} f(\mathbf{c}+\mathbf{x})$$

- Naturally view as function on $\mathbb{F}_2^n/\mathscr{C}$
- Given distribution ν of noise $\mathbf{e} \sim \mathbb{F}_2^n$, distribution of $\mathbf{e} \mod \mathscr{C}$ is $\nu^{\mathscr{C}}$

$$\Pr[\mathbf{e} \mod \mathscr{C} = \mathbf{x}] = \sum_{\substack{\mathbf{y} \in \mathbb{F}_2^n \\ \mathbf{y} \mod \mathscr{C} = \mathbf{x}}} \Pr[\mathbf{e} = \mathbf{y}]$$

$$= \sum_{\mathbf{c}\in\mathscr{C}} \Pr[\mathbf{e} = \mathbf{x}+\mathbf{c}] = \sum_{\mathbf{c}\in\mathscr{C}} \nu(\mathbf{x}+\mathbf{c}) = \nu^{\mathscr{C}}(\mathbf{x})$$

SETUP

- Let $\mu(\mathbf{x}) = 2^{-(n-k)}$ for all $\mathbf{x} \in \mathbb{F}_2^n/\mathscr{C}$ (uniform distribution)
- ν distribution of noise $\mathbf{e}$ (assume radial)

$\nu(\mathbf{x})$ only function of $|\mathbf{x}|$

- Define $f = 2^{n-k}\nu$ and $g = 2^{n-k}\mu$

relative density functions

$$2 \cdot \Delta(\mu, \nu^{\mathscr{C}}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n/\mathscr{C}} \left|\mu(\mathbf{x}) - \nu^{\mathscr{C}}(\mathbf{x})\right|$$

$$= \frac{1}{2^{n-k}} \sum_{\mathbf{x}\in\mathbb{F}_2^n/\mathscr{C}} \left|g(\mathbf{x}) - f^{\mathscr{C}}(\mathbf{x})\right| = \|g - f^{\mathscr{C}}\|_{L_1}$$

STEP 1: CAUCHY-SCHWARZ

For $f : U \to \mathbb{C}, p \geq 1$:

$$\|f\|_{\ell_p} := \left(\sum_{x \in U} |f(x)|^p \right)^{1/p}$$

$$\|f\|_{L_p} := \left(\frac{1}{|U|} \sum_{x \in U} |f(x)|^p \right)^{1/p}$$

- We can upper bound

$$\|g - f^{\mathscr{C}}\|_{L_1} \leq \|g - f^{\mathscr{C}}\|_{L_2}$$

- The L_2-norm interacts well with the Fourier Transform…

FOURIER FOR COSET FUNCTIONS

- Let $f, g : \mathbb{F}_2^n/\mathscr{C} \to \mathbb{C}$ be functions (e.g., densities)
- Scalar product: $\langle f, g \rangle = \frac{1}{2^{n-k}} \sum_{\mathbf{x} \in \mathbb{F}_2^n/\mathscr{C}} f(\mathbf{x})\overline{g(\mathbf{x})}$; norm $\|f\|_{L_2} = \sqrt{\frac{1}{2^{n-k}} \sum_{\mathbf{x} \in \mathbb{F}_2^n/\mathscr{C}} |f(\mathbf{x})|^2}$
- Orthonormal basis of characters: $\chi_{\mathbf{c}^*}$ for $\mathbf{c}^* \in \mathscr{C}^*$ defined as $\chi_{\mathbf{c}^*}(\mathbf{x}) = (-1)^{\mathbf{c}^* \cdot \mathbf{x}}$
- Fourier transform: $\hat{f} : \mathscr{C}^* \to \mathbb{C}$ defined by $\hat{f}(\mathbf{c}^*) = \langle f, \chi_{\mathbf{c}^*} \rangle$
- Yields Fourier decomposition: $f(\mathbf{x}) = \sum_{\mathbf{c}^* \in \mathscr{C}^*} \hat{f}(\mathbf{c}^*)\chi_{\mathbf{c}^*}(\mathbf{x})$
- **Parseval's Identity**: $\|f\|_{L_2} = \|\hat{f}\|_{\ell_2} = \sqrt{\sum_{\mathbf{c}^* \in \mathscr{C}^*} |\hat{f}(\mathbf{c}^*)|^2}$

STEP 2: PARSEVAL'S IDENTITY

$$\left\| g - f^{\mathscr{C}} \right\|_{L_2} = \left\| \widehat{g - f^{\mathscr{C}}} \right\|_{\ell_2} = \left\| \hat{g} - \widehat{f^{\mathscr{C}}} \right\|_{\ell_2} = \sqrt{\sum_{\mathbf{c}^* \in \mathscr{C}^*} \left(\hat{g}(\mathbf{c}^*) - \widehat{f^{\mathscr{C}}}(\mathbf{c}^*) \right)^2}$$

- Need to compute fourier transform of periodization of a function

STEP 3: POISSON SUMMATION

$$\begin{tikzcd}[column sep=huge, row sep=huge]
f \arrow[r, "\text{Fourier}"] \arrow[d, "\text{Periodization}"'] & \hat{f} \arrow[d, "\substack{\text{Restriction}\\ \text{(renormalized)}}"'] \\
f^{\mathscr{C}} \arrow[r, "\text{Fourier}"'] & \widehat{f^{\mathscr{C}}} = 2^k \hat{f}|_{\mathscr{C}^*}
\end{tikzcd}$$

PUTTING IT TOGETHER

- Therefore:

$$\widehat{f^{\mathscr{C}}}(\mathbf{0}) = 2^k \hat{f}(\mathbf{0}) = \frac{2^k}{2^n} \sum_{\mathbf{x} \in \mathbb{F}_2^n} f(\mathbf{x})(-1)^{\langle \mathbf{x}, \mathbf{0} \rangle} = \frac{2^k}{2^n} \sum_{\mathbf{x} \in \mathbb{F}_2^n} 2^{n-k} \cdot \nu(\mathbf{x}) = 1$$

$$\hat{g}(\mathbf{c}^*) = \frac{1}{2^{n-k}} \sum_{\mathbf{x} \in \mathbb{F}_2^n / \mathscr{C}} 2^{n-k} \mu(\mathbf{x}) \cdot (-1)^{\langle \mathbf{x}, \mathbf{c}^* \rangle} = \begin{cases} 1 & \mathbf{c}^* = \mathbf{0} \\ 0 & \text{otherwise} \end{cases}$$

- Thus:

$$\sqrt{\sum_{\mathbf{c}^* \in \mathscr{C}^*} \left(\hat{g}(\mathbf{c}^*) - \widehat{f^{\mathscr{C}}}(\mathbf{c}^*) \right)^2} = 2^k \sqrt{\sum_{\mathbf{c}^* \in \mathscr{C} \setminus \{\mathbf{0}\}} \hat{f}(\mathbf{c}^*)^2} = 2^n \sqrt{\sum_{\mathbf{c}^* \in \mathscr{C} \setminus \{\mathbf{0}\}} \hat{\nu}(\mathbf{c}^*)^2}$$

COMPARISON TO PREVIOUS APPROACH

- Essentially, we replaced triangle inequality by Cauchy-Schwarz
- [MR07,GPV08] approach would get following bound:

$$2\Delta(\mu^{\mathscr{C}}, \nu^{\mathscr{C}}) \leq 2^n \sum_{\mathbf{c}^* \in \mathscr{C} \setminus \{\mathbf{0}\}} |\hat{\nu}(\mathbf{c}^*)|$$

Our bound $2^n \sqrt{\sum_{\mathbf{c}^* \in \mathscr{C} \setminus \{\mathbf{0}\}} |\hat{\nu}(\mathbf{c}^*)|^2}$ is smaller

$$a^2 + b^2 \leq (a+b)^2$$

REMAINING CHALLENGE:

How to bound

$$2^n \sqrt{\sum_{\mathbf{c}^* \in \mathscr{C} \setminus \{\mathbf{0}\}} \hat{\nu}(\mathbf{c}^*)^2} = 2^n \sqrt{\sum_{\ell \geq d_{\min}(\mathscr{C}^*)} N_\ell(\mathscr{C}^*) \hat{\nu}(\ell)^2} \ ?$$

- Above:

$$N_\ell(\mathscr{C}^*) = |\{\mathbf{c}^* \in \mathscr{C}^* : |\mathbf{c}^*| = \ell\}|$$

$$d_{\min}(\mathscr{C}^*) = \min\{|\mathbf{c}^*| : \mathbf{c}^* \in \mathscr{C}^* \setminus \{\mathbf{0}\}\}$$

TWO CASES

RANDOM CODES/ LATTICES

- Easier computations
- Guide choice of smoothing distribution

ARBITRARY CODES/ LATTICES

- Case of interest
- Approach guided by random case

RANDOM CODES

RANDOM CODES

- For random dimension k $\mathscr{C} \leq \mathbb{F}_2^n$:

$$\mathbb{E}\left[N_\ell(\mathscr{C}^*)\right] = 2^{-k}\binom{n}{\ell}$$

$$\mathbb{E}\left[2\Delta(\mu, \nu^{\mathscr{C}})\right] \leq \mathbb{E}\left[2^n \sqrt{\sum_{\ell>0} N_\ell(\mathscr{C}^*)\hat{\nu}(\ell)^2}\right]$$

Jensen's Inequality

$$\leq 2^n \sqrt{\sum_{\ell>0} \mathbb{E}\left[N_\ell(\mathscr{C}^*)\right]\hat{\nu}(\ell)^2}$$

$$= 2^n \sqrt{\sum_{\ell>0} 2^{-k}\binom{n}{\ell}\hat{\nu}(\ell)^2}$$

Easy to estimate!

BERNOULLI NOISE

- Let $\varphi_p(\mathbf{x}) = p^{|\mathbf{x}|}(1-p)^{n-|\mathbf{x}|}$ be distribution of Bernoulli noise

$$\hat{\varphi}_p(\mathbf{x}) = \frac{1}{2^n}(1-2p)^{|\mathbf{x}|}$$

$$\mathbb{E}\left[2\Delta(\mu, \varphi_p^{\mathscr{C}})\right] \leq 2^n \sqrt{\sum_{\ell>0} 2^{-k} \binom{n}{\ell} \hat{\varphi}_p(\ell)^2}$$

$$\leq 2^n \sqrt{\sum_{\ell=0}^{n} 2^{-k} \binom{n}{\ell} \left(2^{-n}(1-2p)^{\ell}\right)^2}$$

Binomial Theorem

$$= \sqrt{2^{-k}\left(1+(1-2p)^2\right)^n}$$

COMPARISON WITH TRADITIONAL APPROACH

- To have $\sqrt{2^{-k}\left(1+(1-2p)^2\right)^n} = \mathrm{negl}(n)$, suffices for

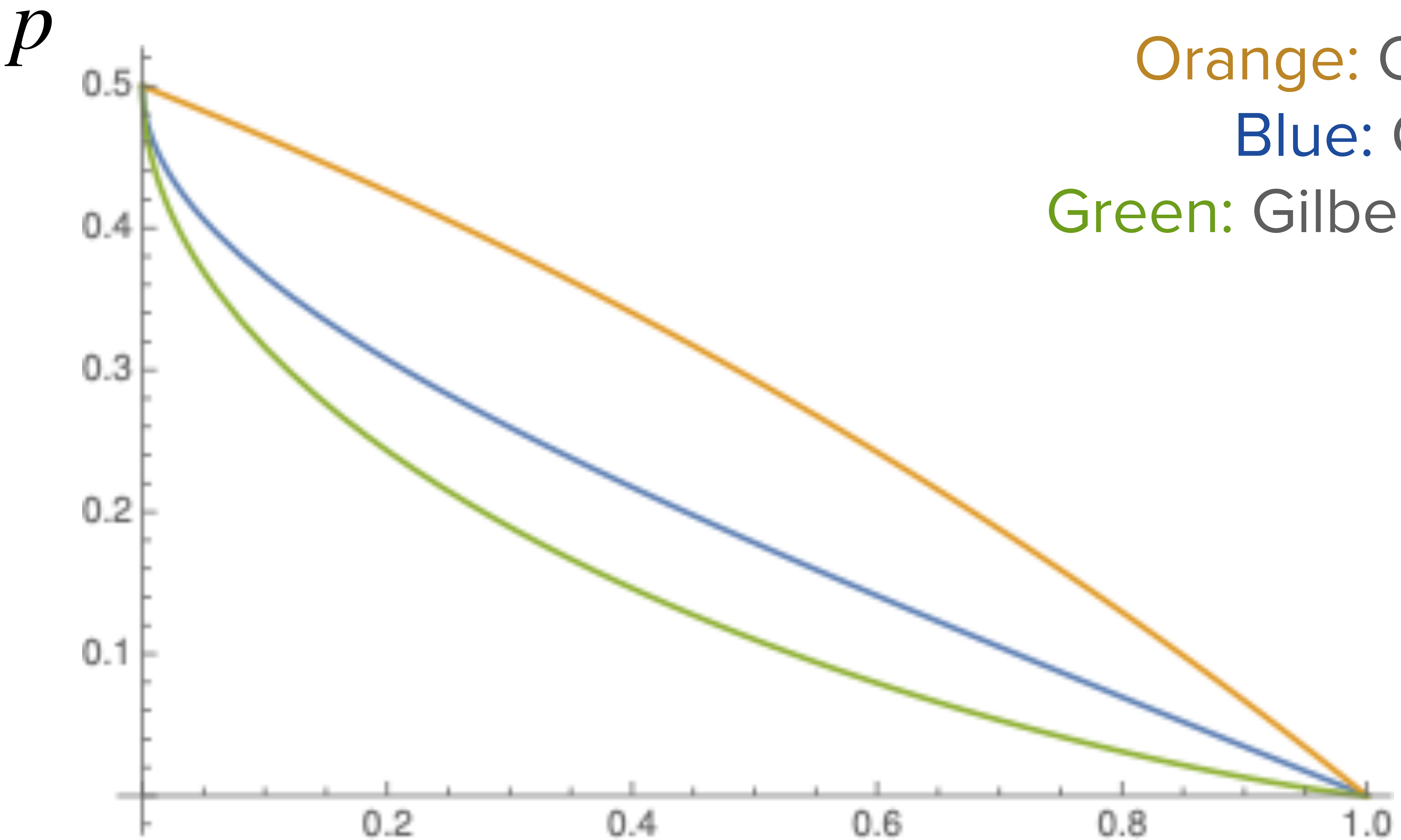
$$p \geq \frac{1}{2}\left(1-\sqrt{2^R-1}\right) \text{ where } R = k/n$$

- Following traditional lattice approach: get upper bound

$$\mathbb{E}\left[2\Delta(\mu, \varphi_p^{\mathscr{C}})\right] \leq 2^{n-k}(1-p)^n$$

  - To make $\mathrm{negl}(n)$, need $p \geq 1 - 2^{-(1-R)}$

BETTER! BUT...



$R = k/n$

Orange: Original approach
Blue: Our approach
Green: Gilbert-Varshamov Bound

GILBERT-VARSHAMOV BOUND

- Define $w_{GV} = w_{GV}(n, k)$ so that

$$\binom{n}{w_{GV}} \approx 2^{n-k} = |\mathbb{F}_2^n / \mathscr{C}|$$

- If $w = \mathbb{E}(|\mathbf{e}|) \geq w_{GV}$, could hope to have $\Delta(\mu, \nu^{\mathscr{C}}) \leq \mathrm{negl}(n)$
- Can we achieve this with our approach?

Yes! But for different noise distribution…

NOISE FROM THE SPHERE

UNIFORM SPHERE NOISE

- Let $\mathbf{e}$ be a uniformly random vector of weight w. Has distribution function

$$\psi_w(\mathbf{x}) = \frac{1_{\mathbb{S}_w}(\mathbf{x})}{\binom{n}{w}} = \begin{cases} \frac{1}{\binom{n}{w}} & |\mathbf{x}| = w \\ 0 & \text{otherwise} \end{cases} \implies \hat{\psi}_w(\mathbf{x}) = 2^{-n} \cdot \frac{K_w(|\mathbf{x}|)}{\binom{n}{w}}$$

- Above, $K_w(\cdot)$ is a Krauwtchouk polynomial; give orthonormal basis for *radial* functions

UNIFORM SPHERE NOISE

- Identity: $$\sum_{\ell=0}^{n} \frac{\binom{n}{\ell}}{2^n} \frac{K_w(\ell)^2}{\binom{n}{w}} = 1$$

$$\mathbb{E}\left[2\Delta(\mu, \psi_w^{\mathscr{C}})\right] \leq \sqrt{\frac{2^n}{\binom{n}{w} 2^k}} \sqrt{\sum_{\ell>0} \frac{\binom{n}{\ell}}{2^n} \frac{K_w(\ell)^2}{\binom{n}{w}}} \leq \sqrt{\frac{2^{n-k}}{\binom{n}{w}}}$$

$w \approx w_{GV}$ **suffices!**

WHAT ABOUT BERNOULLI?

- Bernoulli distribution φ_p is very concentrated: $|\mathbf{e}| = (1 \pm \varepsilon)pn$ with high probability

- Intuitively: φ_p and ψ_{pn} should smooth just about the same… and this is true!

$$\Delta(\mu, \varphi_p^{\mathscr{C}}) \leq \sum_{w=(1-\varepsilon)pn}^{(1+\varepsilon)pn} \Delta(\mu, \psi_w^{\mathscr{C}}) + 2^{-\Omega(n)}$$

$p \approx w_{GV}/n$ suffices!

ARBITRARY CODES

LP BOUNDS

- Given arbitrary $[n, k, d]$ code $\mathscr{C}$, need to bound $N_\ell(\mathscr{C}^*)$'s
- Use LP bounds [MRRW77, ABL01]

Thm: [ABL01] Let $\delta^* = d_{\min}(\mathscr{C}^*)/n$ and $\delta^{*\perp} = \frac{1}{2} - \sqrt{\delta^*(1-\delta^*)}$.

Then

$$N_\ell(\mathscr{C}^*) \le \begin{cases} \frac{\binom{n}{\delta^{*\perp}n}}{2^n}\binom{n}{\ell} & \ell/n \in (\delta^*, 1-\delta^*) \\ 2^{n\alpha(\ell/n,\delta^*)} & \text{otherwise} \end{cases} \approx 2^{-c(\delta^*)\cdot n}\binom{n}{\ell}$$

where $\alpha(\cdot,\cdot) < 1$ is a function related to Krawtchouk polynomials.

PROBLEM WITH UNIFORM SPHERE NOISE

Suppose $\mathbf{1} = (1,\ldots,1) \in \mathscr{C}^*$

$$\implies \forall \mathbf{c} \in \mathscr{C}, \ |\mathbf{c}| \equiv 0 \pmod 2$$

$$\implies \forall \mathbf{c} \in \mathscr{C}, \mathbf{e} \in \mathbb{S}_w, \ |\mathbf{c} + \mathbf{e}| \equiv w \pmod 2$$

Can't have $\mathbf{c} + \mathbf{e} \approx$ uniform; doesn't even touch half the vectors!

In general: $\mathscr{C}^*$ has large weight vectors

$$\implies 2^n \sum_{\ell \geq d_{\min}(\mathscr{C}^*)} N_\ell(\mathscr{C}^*) \hat{\psi}_w(\ell)^2 \text{ large}$$

$$\hat{\psi}_w(\mathbf{x}) = 2^{-n} \cdot \frac{K_w(|\mathbf{x}|)}{\binom{n}{w}}$$

TRUNCATED BERNOULLI

Not so bad: $\sum_{\ell > (n - d_{\min}(\mathscr{C}^*))/2} N_\ell(\mathscr{C}^*) \leq 1$

Bernoulli noise does not have this "parity" problem

$$\hat{\varphi}_p(\mathbf{x}) = 2^{-n}(1-2p)^{|\mathbf{x}|}$$

Our solution: Truncated Bernoulli

Sample $\mathbf{e} \sim \mathrm{Ber}(p)^n$ conditioned on $|\mathbf{e}| \in (p \pm \varepsilon)n$

BACK TO LATTICES

- In case of lattice Λ, if
  - μ is uniform distribution over $\mathbb{R}^n/\Lambda$;
  - ν radial distribution over $\mathbb{R}^n$:

$$\Delta(\mu, \nu^{\Lambda}) \leq \frac{1}{2}\sqrt{\sum_{\mathbf{x}\in\Lambda^*\setminus\{\mathbf{0}\}} |\hat{\nu}(\mathbf{x})|^2}$$

Choices for ν

Gaussian noise:

$$D_s(\mathbf{x}) = \frac{1}{s^n}\exp\Big((-\pi|\mathbf{x}|_2/s)^2\Big)$$

Uniform ball noise:

$$\beta_w(\mathbf{x}) = \frac{1_{\mathscr{B}_w}(\mathbf{x})}{V_n(w)} = \frac{\mathbf{1}\{|\mathbf{x}|_2 \leq w\}}{V_n(w)}$$

RANDOM LATTICES

Used to analyse lattice dual attack: [DP23]

$$M = \mathrm{Vol}(\mathbb{R}^n/\Lambda) = |\det(\Lambda)|$$

- Covolume M Haar random lattices satisfy that, for any *nice* function g,

$$\mathop{\mathbb{E}}_{\Lambda}\left(\sum_{\vec{x}\in\Lambda\setminus\{\mathbf{0}\}} g(\mathbf{x})\right) = \frac{1}{M}\int_{\mathbb{R}^n} g(\mathbf{x})\,d\mathbf{x}$$

(argue as with codes) $\implies \mathop{\mathbb{E}}_{\Lambda}\left(2\Delta(\mu, \beta_w^{\Lambda})\right) \leq \sqrt{\frac{M}{V_n(w)}}$

In particular, if $w > \sqrt{n/2\pi e}M^{1/n}$: $< 2^{-\Omega(n)}$

Gaussian heuristic!

Natively worse for Gaussian...

Can analogously argue Gaussian "close" to uniform ball noise!

ARBITRARY LATTICES

Extra ingredients:

LP bound
[Kabatiansky-Levenshtein'78]

Summing over annuli
[Cohn-Elkies'03]

$$2\Delta(\mu, \beta_w^\Lambda) \leq \sqrt{\frac{1}{V_n(w)} \sum_{j=0}^{\infty} N_j \cdot \varphi_j}$$

bound with LP

bound with asymptotics of Bessel functions

where

- $t_0 = \lambda_1(\Lambda^*)$, $t_{j+1} := (1 + 1/n)t_j$
- $N_j = \#\{\mathbf{x}^* : t_j \leq |\mathbf{x}^*|_2 < t_{j+1}\}$
- $\varphi_j = V_n(w)^{-1} \max \left\{ \widehat{1_{\mathscr{B}_w}}(\mathbf{x})^2 : t_j \leq |\mathbf{x}|_2 < t_{j+1} \right\}$

COMPARISON

$$\min F > 0 \text{ s.t.}$$
$$\Delta(\nu^{\Lambda}, \mu) \leq 2^{-\Omega(n)}$$
$$\text{when } \mathop{\mathbb{E}}_{\mathbf{e}\sim\nu}(\|\mathbf{e}\|_2) = \frac{F n}{\lambda_1^*(\Lambda)}$$

$C_{\mathrm{KL}} \approx 2^{0.401}$
from LP bound

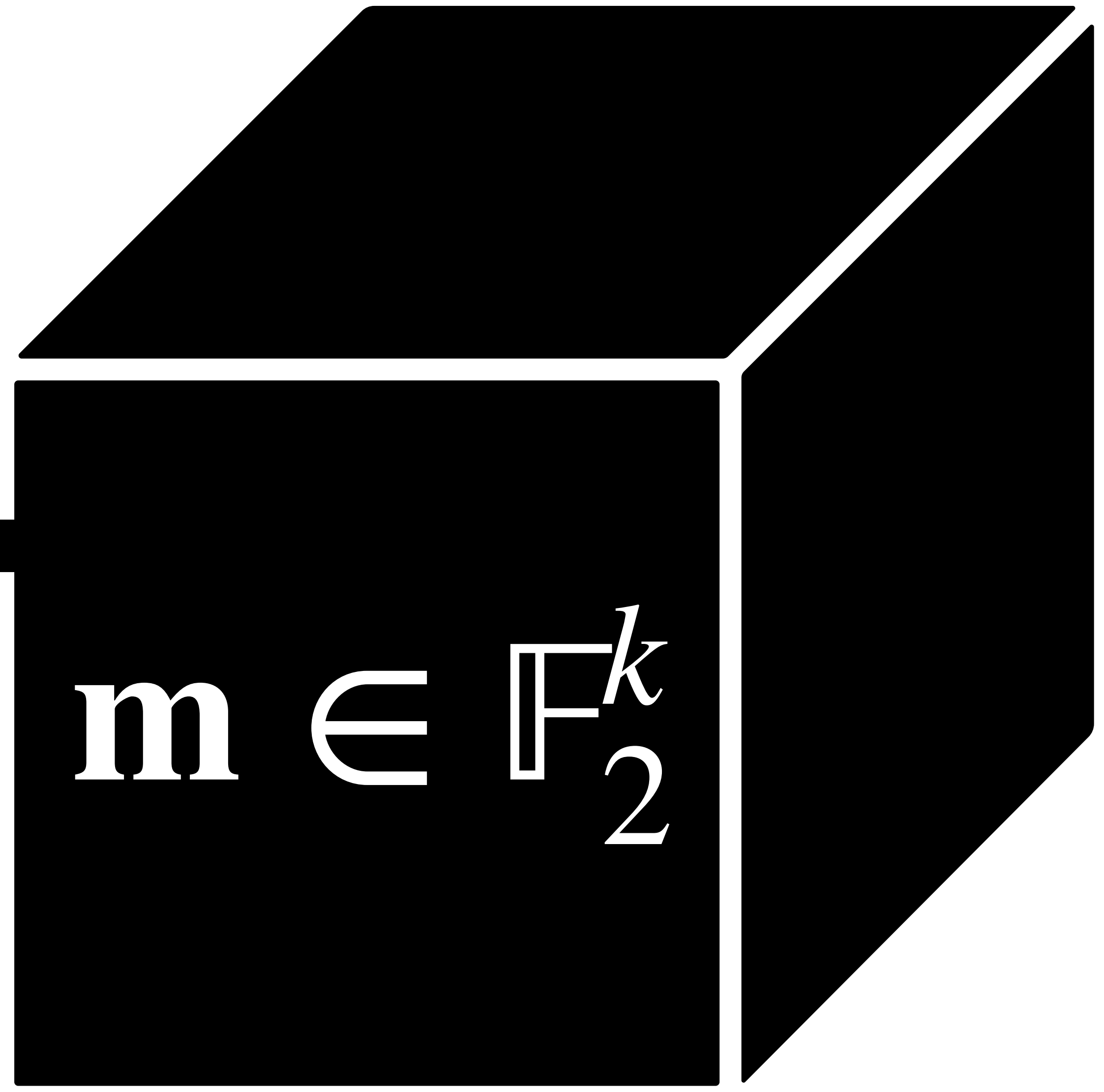
Distribution	Proof strategy	Smooth. factor	Source
Gaussian	PSF+TI+BT	$1/(2\pi) \approx 0.159$	[MR07]
Gaussian	PSF+TI+LP	$C_{\mathrm{KL}}/(2\pi\sqrt{e}) \approx 0.127$	[ADRS15]
Gaussian	PI+CS+LP	$C_{\mathrm{KL}}/(2\pi\sqrt{2e}) \approx 0.090$	Our work
Unif. Ball	PI+CS+LP	$C_{\mathrm{KL}}/(2\pi e) \approx 0.077$	Our work
Gaussian	Unif. + Trunc.	$C_{\mathrm{KL}}/(2\pi e) \approx 0.077$	Our work

For random q-ary lattices: [LLB'22] get same (optimal) bound as us

WORST-CASE TO AVERAGE-CASE REDUCTIONS FOR CODES

LEARNING PARITY WITH NOISE

$$(\mathbf{a}, \langle \mathbf{a}, \mathbf{m} \rangle + b)$$



Can request samples

$$\mathbf{a} \xleftarrow{\$} \mathbb{F}_2^k$$

$$b \xleftarrow{\$} \mathrm{Ber}(p)$$

$$p < \frac{1}{2}$$

Goal: recover $\mathbf{m}$

Notation: $\mathrm{LPN}(k, p)$

DECODING PROBLEM

- Parameters: $t, k, n \in \mathbb{N}$, $t, k \leq n$: $\mathrm{DP}(n, k, t)$
- Given:
  - matrix $\mathbf{G} \in \mathbb{F}_2^{k \times n}$, and
  - vector $\mathbf{y} = \mathbf{m}\mathbf{G} + \mathbf{v}$ where $\mathbf{m} \in \mathbb{F}_2^k$ and $\mathbf{v} \in \mathbb{F}_2^n$, $|\mathbf{v}| = t$
- Goal: find $\mathbf{m}$

$$\boxed{\mathbf{G}}\,, \quad \boxed{\mathbf{m}}\,\boxed{\mathbf{G}} + \boxed{\mathbf{v}} = \boxed{\mathbf{y}}$$

REDUCTION

Goal: create algorithm $\mathscr{B}$ solving $\mathrm{DP}(n, k, t)$

On input $\mathbf{G}$, $\mathbf{y}$:

Simulate $\mathscr{A}$

Algorithm $\mathscr{A}$ solving $\mathrm{LPN}(k, p)$

When $\mathscr{A}$ requests a new sample:

- Sample $\mathbf{e} \sim \mathbb{F}_2^n$ from smoothing distribution
- Reply with $(\mathbf{e}\mathbf{G}^\top, \langle \mathbf{e}, \mathbf{y} \rangle)$

$\mathbf{e}\mathbf{G}^\top \approx \mathbf{a} \iff \mathbf{e}$ smooths code checked by $\mathbf{G}$

$\langle \mathbf{e}, \mathbf{y} \rangle = \langle \mathbf{e}\mathbf{G}^\top, \mathbf{s} \rangle + \langle \mathbf{e}, \mathbf{v} \rangle$
$\approx \langle \mathbf{a}, \mathbf{s} \rangle + b$

Minor issue: $\mathbf{e}\mathbf{G}^\top$ and $\langle \mathbf{e}, \mathbf{v} \rangle$ not independent

Bigger issue: $b = \langle \mathbf{e}, \mathbf{v} \rangle \sim \mathrm{Ber}\left(\frac{1}{2} - \varepsilon\right)$ for very small ε...

"BEST" RESULTS...

- [BLVW19, YZ21, D**R**22]: all obtain the same qualitative result:

$\boxed{\mathrm{LPN}\left(k, \frac{1}{2} - \frac{1}{n^4}\right) \text{ hard}}$ $\Longrightarrow$ $\boxed{\mathrm{DP}\left(k^{O(1)}, k, O(\log^2 k)\right) \text{ hard}}$

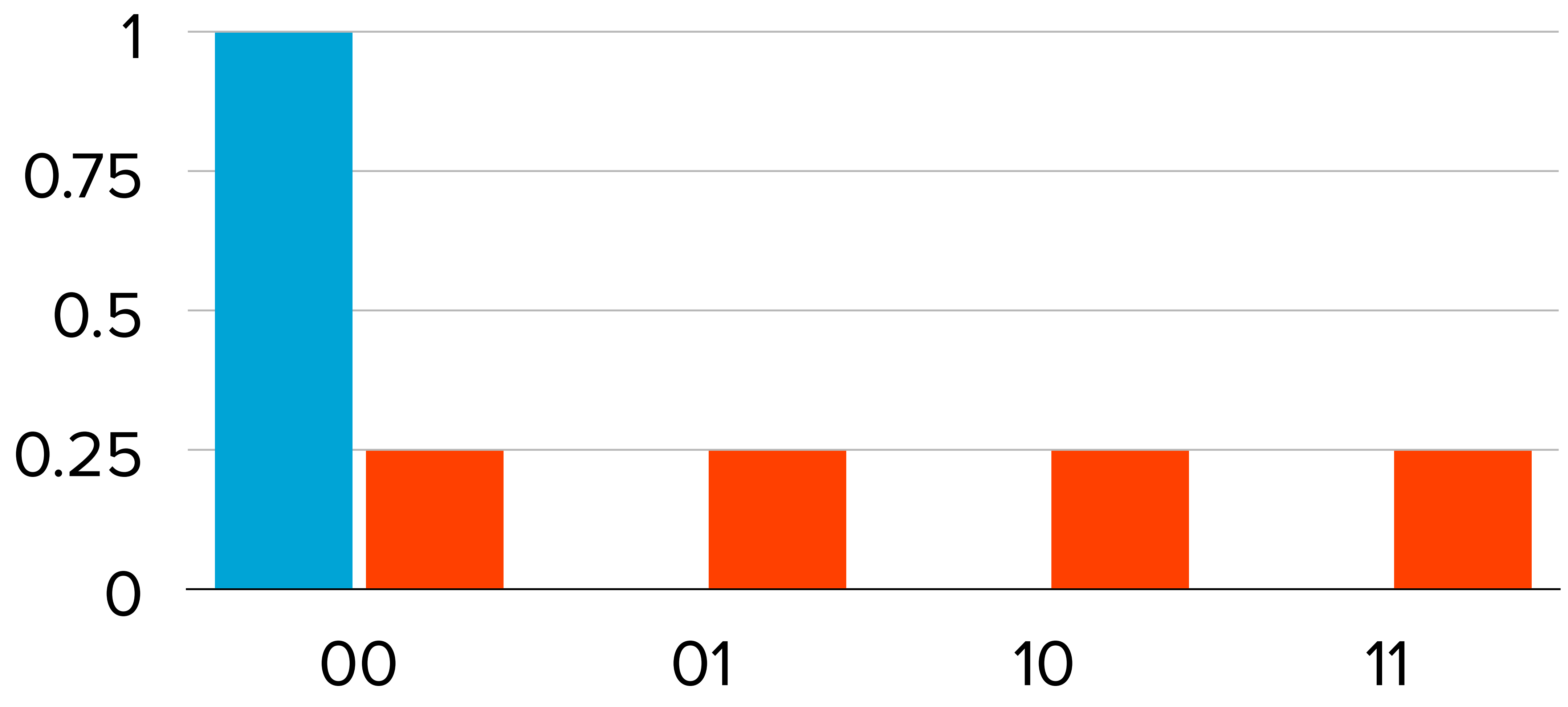
- Also require "balanced" assumption

Conclusion: there must be a better result possible... right?

- There (should be) some information-theoretic barriers...
- [BCD'23]: search-to-decision reduction for codes via oracle comparison method; uses [D**R**22] smoothing bound for Bernoulli

SUMMARY

SMOOTHING BOUNDS



Proofs that $\Delta(\mathbf{u}, \mathbf{e} \mod \mathscr{C})$ or $\Delta(\mathbf{y}, \mathbf{e} \mod \Lambda) \leq$ negl(n)

3 step recipe:

1: Cauchy-Schwarz ($L_1 \to L_2$)

2: Plancherel ($L_2 \to \ell_2$ in Fourier)

3: Poisson Sum (Fourier of period.)

$$\Delta\left(\mu, \nu^{\mathscr{C}}\right) \leq 2^n \sqrt{\sum_{\mathbf{c}^* \neq \mathbf{0}} \hat{\nu}(\mathbf{c}^*)^2}$$

RANDOM CODES	RANDOM LATTICES
	$\mathbb{E}_{\mathbf{v}\sim D_s}(\lvert\mathbf{v}\rvert) = s\sqrt{n/(2\pi)}$
$\mathrm{Ber}(p)^n$: $p \geq \frac{1}{2}\left(1 - \sqrt{2^R - 1}\right)$ $\mathrm{Sph}(w)$: $w \geq w_{GV}$	$\mathrm{Gau}(s)$: $s \geq M^{1/n}/\sqrt{2}$ $\mathrm{Ball}(w)$: $w \geq \sqrt{n/2\pi e}M^{1/n} =: w_{GH}$
Truncation, concentration, convex combination: $\implies p \geq w_{GV}/n$ suffices for $\mathrm{Ber}(p)$	Truncation, concentration, convex combination: $\implies s \geq w_{GH}\sqrt{2\pi/n}$ suffices for $\mathrm{Gau}(s)$

ARBITRARY CODES

ARBITRARY LATTICES

ARBITRARY CODES	ARBITRARY LATTICES
Bound $N_\ell(\mathscr{C}^*)$'s w/ LP [AKL01]	Bound $N_\ell(\Lambda^*)$'s w/ LP [L79]
Use truncated Bernoulli	Can use uniform ball (or Gaussian)
Deal with ≤ 1 high weight $\mathbf{c}^*$	Sum over annuli [CE03]

OPEN QUESTIONS

- Can we improve worst-case to average-case reductions?
  - Or are there barriers?
- Maybe different notions of "closeness" are useful?

- Reductions for structured codes?
  - noise distributions for, e.g., quasi-cyclic codes are quite hard to interpret...

Thank you! Questions?