Gaussian LHL for Modules over Number Fields

Joint work with Martin R. Albrecht, Joël Felderhoff, Russell W. F. Lai, and Ivy K. Y. Woo

Sasha Lapiha, Royal Holloway University of London

Classic Leftover Hash Lemma (LHL)

$$(A, A \cdot x \bmod q) \sim (A, \mathcal{U}(\mathcal{R}_q^n))$$

where

$$A \leftarrow \mathcal{U}(\mathcal{R}_q^{n \times m}), \quad x \leftarrow \chi$$

and χ is usually a short distribution over $\mathcal{R}^m$ or $\mathcal{R}_q^m$

Gaussian LHL

$$(X, X \cdot v) \sim (X, \mathcal{D}_{\mathcal{R}^r, \sigma})$$

where

$$X \leftarrow \left(\mathcal{D}_{\mathcal{R}^r, \mathbf{S}_x}\right)^m, \quad v \leftarrow \mathcal{D}_{\mathcal{R}^m, \mathbf{S}_v}$$

Notations

- Number field $\mathscr{K}$ of degree d.
- Field discriminant $\Delta_{\mathscr{K}}$.
- The ring of integers $\mathscr{R} = \mathscr{O}_{\mathscr{K}}$.
- We assume the canonical embedding of $\mathscr{R}$ has a basis $||\mathbf{B}_{\mathscr{R}}||_{\infty} \leq \delta_{\mathscr{K}}$.
- We assume $\mathscr{K}$ contains $\mathbb{Q}(\zeta_f)$ for some $f \geq 2$.

Gaussian Linear Transform

$$(X, X \cdot v) \sim \left(X, \mathscr{D}_{\sqrt{\mathbf{X} \cdot \mathbf{S}_v \cdot \mathbf{S}_v^T \cdot \mathbf{X}^T}}\right)$$

where

$$X \leftarrow \left(\mathscr{D}_{\mathbf{S}_x}\right)^m, \qquad v \leftarrow \mathscr{D}_{\mathbf{S}_v}$$

Discrete Gaussian version

$$(\mathbf{X}, \mathbf{X} \cdot \mathbf{v}) \sim (\mathbf{X}, \mathcal{D}_{\mathbf{X} \cdot \mathcal{R}^m, \sqrt{\mathbf{X} \cdot \mathbf{S}_v \cdot \mathbf{S}_v^T \cdot \mathbf{X}^T}})$$

for $\quad \mathbf{X} \leftarrow \left(\mathcal{D}_{\mathcal{R}^r, \mathbf{S}_x}\right)^m, \quad \mathbf{v} \leftarrow \mathcal{D}_{\mathcal{R}^m, \mathbf{S}_v}$

as long as $\quad \mathbf{S}_v \geq \eta_\varepsilon(\Lambda^\perp(\mathbf{X}))$

Discrete Gaussian version

$$(\mathbf{X}, \mathbf{X} \cdot \mathbf{v}) \sim (\mathbf{X}, \mathcal{D}_{\mathbf{X} \cdot \mathcal{R}^m, \sqrt{\mathbf{X} \cdot \mathbf{S}_v \cdot \mathbf{S}_v^T \cdot \mathbf{X}^T}})$$

for $\mathbf{X} \leftarrow \left(\mathcal{D}_{\mathcal{R}^r, \mathbf{S}_x}\right)^m, \quad \mathbf{v} \leftarrow \mathcal{D}_{\mathcal{R}^m, \mathbf{S}_v}$

as long as $\mathbf{S}_v \geq \eta_\varepsilon(\Lambda^\perp(\mathbf{X}))$

we also consider $\mathbf{X} \cdot \mathcal{R}^m = \mathcal{R}^r$, and $\sqrt{\mathbf{X} \cdot \mathbf{S}_v \cdot \mathbf{S}_v^T \cdot \mathbf{X}^T} \approx \sigma \cdot I$

Surjective Gaussian Matrices

Extending [NP20] to the ring setting

Surjective Gaussian Matrices

- In fields Surjective = Full Rank = Non-Sigular Submatrix $\implies$ "Easy" to argue via entropy.

Surjective Gaussian Matrices

- In fields Surjective = Full Rank = Non-Sigular Submatrix $\implies$ "Easy" to argue via entropy.
- For $\mathbf{X} \in \mathscr{R}^{r \times m}$ take a submatrix $\mathbf{X}_0 \in \mathscr{R}^{r \times r}$.
- We reduce mod every prime ideal $\boldsymbol{p}$ and prove non-zero determinant w.h.p.

Surjective Gaussian Matrices

- In fields Surjective = Full Rank = Non-Sigular Submatrix $\Longrightarrow$ "Easy" to argue via entropy.
- For $\mathbf{X} \in \mathscr{R}^{r \times m}$ take a submatrix $\mathbf{X}_0 \in \mathscr{R}^{r \times r}$.
- We reduce mod every prime ideal p and prove non-zero determinant w.h.p.
- Number of prime ideals in $\mathcal{O}_{\mathscr{K}}$ = infinite.
- Only consider small prime ideals that could divide $\mathbf{det}(\mathbf{X}_0)$.

Surjective Gaussian Matrices

- In fields Surjective = Full Rank = Non-Sigular Submatrix $\Longrightarrow$ "Easy" to argue via entropy.
- For $\mathbf{X} \in \mathscr{R}^{r \times m}$ take a submatrix $\mathbf{X}_0 \in \mathscr{R}^{r \times r}$.
- We reduce mod every prime ideal p and prove non-zero determinant w.h.p.
- Number of prime ideals in $\mathcal{O}_{\mathscr{K}}$ = infinite.
- Only consider small prime ideals that could divide $\det(\mathbf{X}_0)$.
- Bound the number for $N(p) \leq B$ by $B/\log(B)$ (uses GRH).

The result

$$\Pr\left(\mathbf{X} \leftarrow (\mathcal{D}_{\mathcal{R}^r,\mathbf{s}_x})^m \text{ is surjective}\right) \geq 1 - 2^{-\lambda}$$

when $m \geq 2r + \dfrac{\lambda}{\log(N_{\mathcal{R}})}$, $N_{\mathcal{R}}$ - the norm of the smallest ideal

Short Kernel Basis

Lifting [AR16] to the ring setting

Short Kernel Basis

From the the kernel to the unit vector preimages

- Find short $\mathbf{U} \in \mathscr{R}^{m \times r}$ such that $\mathbf{X} \cdot \mathbf{U} = \mathbf{I}_r$
- Then for $\mathbf{I}_m - \mathbf{U} \cdot \mathbf{X}$ we have $\mathbf{X} \cdot (\mathbf{I}_m - \mathbf{U} \cdot \mathbf{X}) = \mathbf{X} - \mathbf{I}_r \cdot \mathbf{X} = \mathbf{0}$

Short Kernel Basis

From the the kernel to the unit vector preimages

- Find short $\mathbf{U} \in \mathscr{R}^{m \times r}$ such that $\mathbf{X} \cdot \mathbf{U} = \mathbf{I}_r$
- Then for $\mathbf{I}_m - \mathbf{U} \cdot \mathbf{X}$ we have $\mathbf{X} \cdot (\mathbf{I}_m - \mathbf{U} \cdot \mathbf{X}) = \mathbf{X} - \mathbf{I}_r \cdot \mathbf{X} = \mathbf{0}$
- Similarly if $\mathbf{X} \cdot \mathbf{U} = f \cdot \mathbf{I}_r$
- Then for $f \cdot \mathbf{I}_m - \mathbf{U} \cdot \mathbf{X}$ (still short) we have $\mathbf{X} \cdot (f \cdot \mathbf{I}_m - \mathbf{U} \cdot \mathbf{X}) = \mathbf{X} \cdot f - f \cdot \mathbf{I}_r \cdot \mathbf{X} = \mathbf{0}$

Short Kernel Basis

Integer case

For $\mathbf{X} = [\mathbf{x}_1, \ldots, \mathbf{x}_m]$ with $||\mathbf{x}_i||_\infty \leq B$ consider the set $S = \sum_{i=1}^{j} \{0,1\} \cdot \mathbf{x}_i$

Short Kernel Basis

Integer case

For $\mathbf{X} = [\mathbf{x}_1, \ldots, \mathbf{x}_m]$ with $||\mathbf{x}_i||_\infty \leq B$ consider the set $S = \sum_{i=1}^{j} \{0,1\} \cdot \mathbf{x}_i$

As j grows the norms in S grow slower than cardinality.

For $\mathbf{v} \in S$: $||\mathbf{v}||_\infty \leq j \cdot B$ this is a set of size $(2jB + 1)^r$ but $|S| = 2^j$.

When $2^j \geq (2jB + 1)^r$ (or $j \geq 2r\log(Br)$) we have a collision or $\sum_{i=1}^{j} \{0, \pm 1\} \cdot \mathbf{x}_i = 0$

Short Kernel Basis

Sets with a shift

Consider the set $S_j = \sum_{i=1}^{j} \{0, \pm 1\} \cdot \mathbf{x}_i$

We define random variables:

- $\text{Win}_j : S_j \cap S_j + \mathbf{e}_1 \neq \emptyset$
- $\text{Gain}_j : \mathbf{x}_{j+1} \notin S_j \wedge ||\mathbf{x}_{j+1}||_\infty \leq \sigma_x \sqrt{m} = B$

Short Kernel Basis

Sets with a shift

Consider the set $S_j = \sum_{i=1}^{j} \{0, \pm 1\} \cdot \mathbf{x}_i$

We define random variables:

- $\text{Win}_j : S_j \cap S_j + \mathbf{e}_1 \neq \emptyset$
- $\text{Gain}_j : \mathbf{x}_{j+1} \notin S_j \wedge ||\mathbf{x}_{j+1}||_\infty \leq \sigma_x \sqrt{m} = B$

If $\text{Gain}_j = 1$ for $j \in [1, 2r\log(Br)]$ then $\sum_{j=1}^{2r\log(Br)} \{0, \pm 1\} \cdot \mathbf{x}_j = 0$ and $\pm \mathbf{x}_{\text{last}} = \sum \{0, \pm 1\} \cdot \mathbf{x}_j$.

Short Kernel Basis

We Gain often enough

When $\neg\textsf{Win}$ so $S_j \cap S_j + \mathbf{e}_1 = \varnothing$ we have $\rho_{\sigma_x}(S_j) + \rho_{\sigma_x}(S_j + \mathbf{e}_1) \leq \rho_{\sigma_x}(\mathbb{Z}^m)$

And also $\rho_{\sigma_x}(S_j) \approx_\delta \rho_{\sigma_x}(S_j + \mathbf{e}_1)$

Hence $\Pr(S_j) \leq \frac{1}{2} + \delta$ and $\Pr(\neg S_j) \geq \frac{1}{2} - \delta$

Short Kernel Basis

Issues with integers

For $\mathbf{X} = [\mathbf{x}_1, \ldots, \mathbf{x}_m]$ with $||\mathbf{x}_i||_\infty \leq B$ consider the set $S = \sum_{i=1}^{j} \{0,1\} \cdot \mathbf{x}_i$

As j grows the norms in S grow slower than cardinality.

For $\mathbf{v} \in S$: $||\mathbf{v}||_\infty \leq j \cdot B$ this is a set of size $(2jB+1)^r$ but $|S| = 2^j$.

When $2^j \geq (2jB+1)^r$ (or $j \geq 2r\log(Br)$) we have a collision or $\sum_{i=1}^{j} \{0, \pm 1\} \cdot \mathbf{x}_i = 0$

Short Kernel Basis

We change the set

Consider the set $A = \mathbf{B}_{\mathscr{R}} \cdot \{0,1\}^d$ and $S_j = \{\sum_{i=1}^{j} a_i \cdot \mathbf{x}_i \mid a_i \in A\}$.

Now $|S_j| = 2^{dj}$ with norm $\mathbf{v} \in S_j : ||\mathbf{v}||_\infty \leq jB \cdot d \cdot \delta_{\mathscr{K}}$

Short Kernel Basis

We change the set

Consider the set $A = \mathbf{B}_{\mathscr{R}} \cdot \{0,1\}^d$ and $S_j = \{ \sum_{i=1}^{j} a_i \cdot \mathbf{x}_i \mid a_i \in A \}$.

Now $|S_j| = 2^{dj}$ with norm $\mathbf{v} \in S_j : ||\mathbf{v}||_\infty \leq jB \cdot d \cdot \delta_{\mathscr{K}}$

Pigeonhole gives $dr \cdot \log(2jB \cdot d\delta_{\mathscr{K}} + 1) \leq dj \cdot \log(2)$ so $m \approx r \log(rB \cdot d\delta_{\mathscr{K}})$

** we actually take $A = \mathbf{B}_{\mathscr{R}} \cdot \{0, \pm 1\}^d$

Short Kernel Basis

The proof doesn't work

Now for $S_j = \sum_{i=1}^{j} A \cdot \mathbf{x}_i$

We define random variables:

- $\text{Win}_j : S_j \cap S_j + \mathbf{e}_1 \neq \varnothing$
- $\text{Gain}_j : \mathbf{x}_{j+1} \notin S_i \wedge ||\mathbf{x}_{j+1}||_\infty \leq \sigma_x \sqrt{m} = B$

If $\text{Gain}_j = 1$ for $j \in [1, \approx r\log(Br \cdot d\delta_{\mathcal{K}})]$ then $\sum_{j=1}^{\approx r\log(Brd\delta_{\mathcal{K}})} a_j \cdot \mathbf{x}_j = 0$ and $a_{\text{last}} \cdot \mathbf{x}_{\text{last}} = \sum a_j \cdot \mathbf{x}_j$.

Short Kernel Basis

Change further

Consider two sets $S_j = \sum_{i=1}^{j} A \cdot \mathbf{x}_i$ and $\hat{S}_j = \{s/a \mid s \in S_j, a \in A \backslash \{0\}\}$

We define random variables:

- $\text{Win}_j : \hat{S}_j \cap \hat{S}_j + \mathbf{e}_1 \neq \emptyset$
- $\text{Gain}_j : \mathbf{x}_{j+1} \notin \hat{S}_j \wedge ||\mathbf{x}_{j+1}||_\infty \leq \sigma_x \sqrt{m} = B$ implies $\mathbf{x}_{j+1} \notin S_j \subset \hat{S}_j$

If $\text{Gain}_j = 1$ for $j \in [1, \approx r \log(Br \cdot d\delta_{\mathcal{K}})]$ then $\sum_{j=1}^{\approx r \log(Brd\delta_{\mathcal{K}})} a_j \cdot \mathbf{x}_j = 0$ and $a_{\text{last}} \cdot \mathbf{x}_{\text{last}} = \sum a_j \cdot \mathbf{x}_j$.

Short Kernel Basis

One more improvement

Consider two sets $S_j = \sum_{i=1}^{j} A \cdot \mathbf{x}_i$ and $\hat{S}_j = \{s/a \mid s \in S_j, a \in A \backslash \{0\}\}$

We define random variables:

- $\text{Win}_j : \hat{S}_j + \zeta^x \cdot \mathbf{e}_1 \cap \hat{S}_j + \zeta^y \cdot \mathbf{e}_1 \neq \emptyset$ now $\Pr(\neg \hat{S}_j) \geq 1/f - \delta$
- $\text{Gain}_j : \mathbf{x}_{j+1} \notin \hat{S}_j \wedge || \mathbf{x}_{j+1} ||_\infty \leq \sigma_x \sqrt{m} = B$ implies $\mathbf{x}_{j+1} \notin S_j \subset \hat{S}_j$

If $\text{Gain}_j = 1$ for $j \in [1, \approx r \log(Br \cdot d\delta_{\mathcal{K}})]$ then $\sum_{j=1}^{\approx r \log(Brd\delta_{\mathcal{K}})} a_j \cdot \mathbf{x}_j = 0$ and $a_{\text{last}} \cdot \mathbf{x}_{\text{last}} = \sum a_j \cdot \mathbf{x}_j$.

Short Kernel Basis

Win condition

$\hat{S}_j + \zeta^x \cdot \mathbf{e}_1 \cap \hat{S}_j + \zeta^y \cdot \mathbf{e}_1 \neq \varnothing$ implies

$$s_1/a_1 - s_2/a_2 = (\zeta^y - \zeta^x) \cdot \mathbf{e}_1 = \zeta^y \cdot (1 - \zeta^{x-y}) \cdot \mathbf{e}_1$$

Short Kernel Basis

Win condition

$\hat{S}_j + \zeta^x \cdot \mathbf{e}_1 \cap \hat{S}_j + \zeta^y \cdot \mathbf{e}_1 \neq \emptyset$ implies

$$s_1/a_1 - s_2/a_2 = (\zeta^y - \zeta^x) \cdot \mathbf{e}_1 = \zeta^y \cdot (1 - \zeta^{x-y}) \cdot \mathbf{e}_1$$

$$u \cdot (s_1 \cdot a_2 - s_2 \cdot a_1) = a_1 a_2 \cdot f \cdot \mathbf{e}_1$$

where $u = \zeta^{f-y} \cdot \dfrac{f}{1 - \zeta^{x-y}} \in \mathscr{R}$ is short

However for every $\mathbf{e}_i$ the value $a_1 a_2$ may be different.

Short Kernel Basis

We run it twice

Define $B = \{b \text{ s.t. } ||b||_\infty \leq R,$ coprime with $a_1 a_2\}$

We prove there exists $|B| \geq 2^d$ for $R = O(\Delta_{\mathcal{K}}^{1/d} \cdot d^{2.5} \cdot \delta_{\mathcal{K}}^3)$.

We get $u' \cdot (s_1' \cdot b_2 - s_2' \cdot b_1) = b_1 b_2 \cdot f \cdot \mathbf{e}_1$ using small Bezout identity $\alpha \cdot a_1 a_2 + \beta \cdot b_1 b_2 = 1$

We finally get $\alpha \cdot u \cdot (s_1 \cdot a_2 - s_2 \cdot a_1) + \beta \cdot u' \cdot (s_1' \cdot b_2 - s_2' \cdot b_1) = f \cdot \mathbf{e}_1$

Short Kernel Basis

The result and open problems

$$\Pr\left(\eta_\varepsilon(\Lambda^\perp(\mathbf{X})) \geq O(m^{3/2} \cdot d^{12} \cdot f^2 \cdot \delta_{\mathcal{K}}^{14} \cdot \Delta_{\mathcal{K}}^{4/d} \cdot s_{\min}(\mathbf{S}_x))\right) \geq 1 - 2^{-\lambda}$$

when $m \geq r \log(d \cdot r \cdot s_{\max}(\mathbf{S}_x))^{1+o(1)} + \dfrac{\lambda}{\log f}$.

Short Kernel Basis

The result and open problems

$$\Pr\left(\eta_\varepsilon(\Lambda^\perp(\mathbf{X})) \leq O(m^{3/2} \cdot d^{12} \cdot f^2 \cdot \delta_{\mathscr{K}}^{14} \cdot \Delta_{\mathscr{K}}^{4/d} \cdot s_{\min}(\mathbf{S}_x))\right) \geq 1 - 2^{-\lambda}$$

when $m \geq r \log(d \cdot r \cdot s_{\max}(\mathbf{S}_x))^{1+o(1)} + \dfrac{\lambda}{\log f}$.

- Find a different set A that contains:
  - Short unit elements, with short inverses.
- Find a set A where all elements have many coprime short values.

Spherical covariance

Spherical covariance

First approach

Set $\mathbf{S}_v$ as pseudo-inverse of $\mathbf{X}$ scaled by σ. Then $\sqrt{\mathbf{X} \cdot \mathbf{S}_v \cdot \mathbf{S}_v^T \cdot \mathbf{X}^T} = \sigma \cdot I$

And $$\frac{\sigma}{s_{\max}(\mathbf{X})} \leq s_{\min}(\mathbf{S}_v) \leq s_{\max}(\mathbf{S}_v) \leq \frac{\sigma}{s_{\min}(\mathbf{X})}$$

Spherical covariance

Second approach

- [AGHS13] conjectured that singular values of $\sqrt{\mathbf{X} \cdot \mathbf{X}^T}$ are close for a large enough m
- We refine their bound and apply it to rings

Spherical covariance

Rotating a Real Gaussian Matrix [Sil85]

Assume $\mathbf{Z} \leftarrow (\mathscr{D}_{\sigma=1})^{r\times m}$ then there exist orthogonal $\mathbf{O}_i$ s.t.

$$\mathbf{Z} = \begin{bmatrix} — & \mathbf{z}_1^{\mathrm{T}} & — \\ — & \mathbf{z}_2^{\mathrm{T}} & — \\ & \cdots & \end{bmatrix}$$

$$\mathbf{Z}\cdot\mathbf{O}_0 = \begin{bmatrix} X_m & 0 \dots 0 \\ & \tilde{\mathbf{Z}}_0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 \dots 0 \\ 0 & \\ \vdots & \tilde{\mathbf{O}}_1 \\ 0 & \end{bmatrix} \cdot \mathbf{Z}\cdot\mathbf{O}_0 = \begin{bmatrix} X_m & 0 \dots 0 \\ Y_{r-1} & \\ \vdots & \tilde{\mathbf{Z}}_1 \\ 0 & \end{bmatrix}$$

where X_m, Y_{r-1} are Chi random variables of corresponding dimension.

Spherical covariance

Gershgorin circle theorem

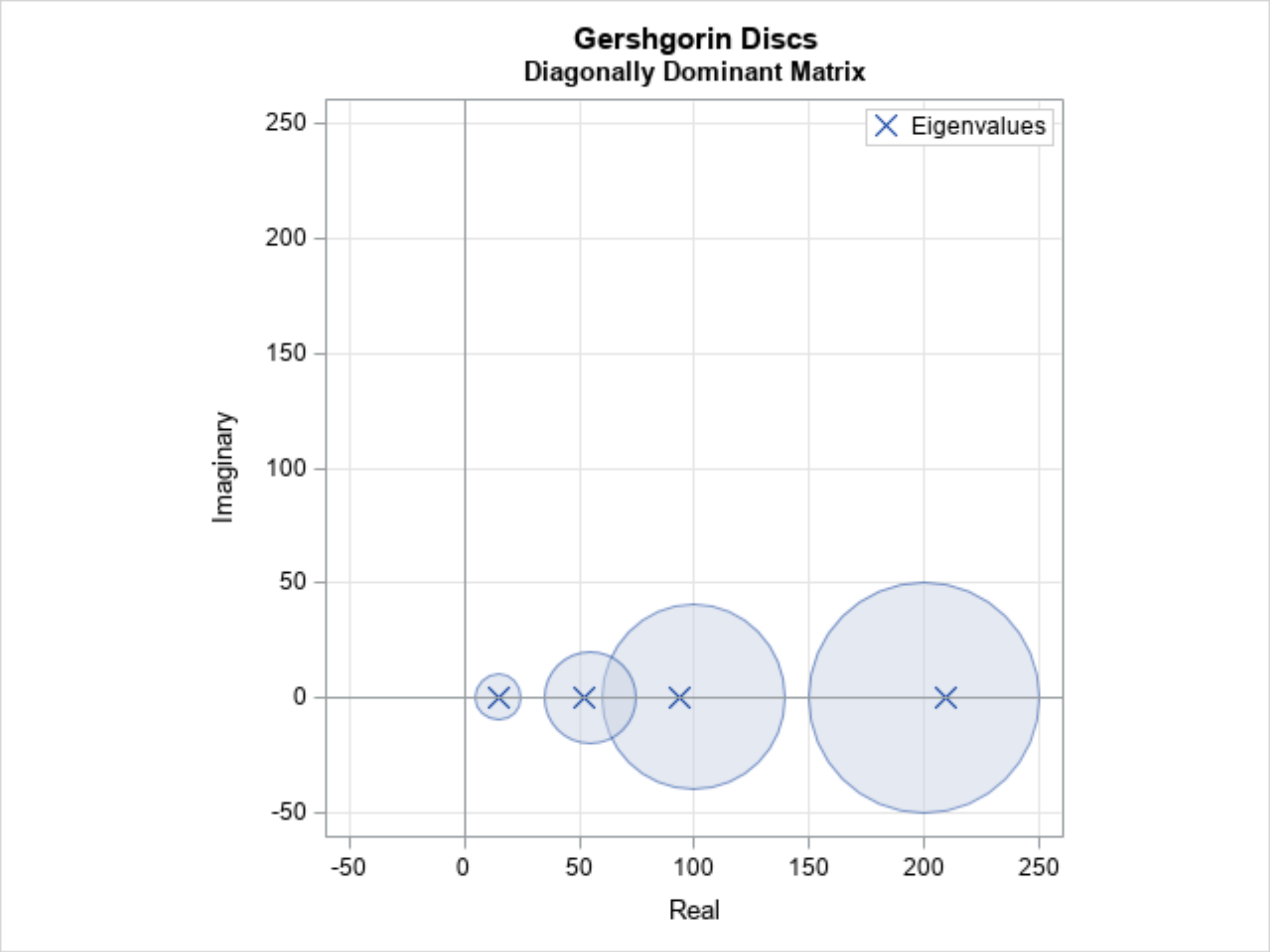
$$\mathbf{O} \cdot \mathbf{Z} \cdot \mathbf{Z}^{\mathrm{T}} \cdot \mathbf{O}^{\mathrm{T}} =$$

$$\begin{bmatrix} X_m^2 & X_m Y_{r-1} & 0 & & & 0 \\ X_m Y_{r-1} & X_{m-1}^2 + Y_{r-1}^2 & X_{m-1} Y_{r-2} & 0 & & 0 \\ & & \cdots & \cdots & & \\ 0 & & & 0 & X_{m-r+2} Y_1 & X_{m-r+1}^2 + Y_1^2 \end{bmatrix}$$

Then [Sil85] applies the Gershgorin circle theorem and Chi tail bounds

Spherical covariance

Gershgorin circle theorem



Then [Sil85] applies the Gershgorin circle theorem and Chi tail bounds

Spherical covariance

Moving to Discreet Gaussians

$$\Pr\left(1 - \frac{1}{rd} \leq \lambda_{\min}/m \leq \lambda_{\max}/m \leq 1 + \frac{1}{rd}\right) \geq 1 - 4r \cdot \exp(-\lambda) \quad \text{for} \quad m \geq 49 \max(r, \lambda) \cdot (rd)^2$$

- We add continuos noise to embedding of $\mathbf{X}$ such that $\mathbf{Z} = \mathbf{X} + \mathbf{Y}$ is close to continuos
- Apply [Sil85] result
- We prove RD between this distribution and spherical Gaussian is a constant

Application to k-SIS

Gaussian matrix with a trapdoor from [LPSS14].

$\mathsf{HintTG}_{m,k}(\varsigma_1, \varsigma_2) \to (\mathbf{X} \in \mathcal{O}_{\mathcal{K}}^{k\times(m+k)}, \mathbf{U} \in \mathcal{O}_{\mathcal{K}}^{(m+k)\times(m+k)})$

1 : $\mathbf{X}_1 \leftarrow \mathcal{D}^m_{\mathcal{O}^k_{\mathcal{K}}, \varsigma_1}$

2 : $\mathbf{\Sigma} \coloneqq \sqrt{\mathbf{S}\cdot\mathbf{S}^\mathsf{T}}$ s.t. $\varsigma_2^2 \cdot \mathbf{I}_{dr} = \tilde{\Phi}(\mathbf{X}_1)\cdot\mathbf{S}\cdot\mathbf{S}^\mathsf{T}\cdot\tilde{\Phi}(\mathbf{X}_1)^\mathsf{T}$

3 : $\forall : i \in [k] : \mathbf{r}_i \leftarrow \mathcal{D}_{\mathcal{O}^m_{\mathcal{K}}, \sqrt{\mathbf{\Sigma}}}$. Let $\mathbf{R} \coloneqq (\mathbf{r}_1, \ldots, \mathbf{r}_k)$

4 : $\mathbf{X}_2 \coloneqq \mathbf{X}_1 \cdot \mathbf{R} + \mathbf{I}_k \in \mathcal{O}_{\mathcal{K}}^{k\times k}$

5 : $\mathbf{U} \coloneqq \begin{bmatrix} -\mathbf{R} & -\mathbf{I}_m - \mathbf{R}\mathbf{X}_1 \\ \mathbf{I}_k & \mathbf{X}_1 \end{bmatrix} \in \mathcal{O}_{\mathcal{K}}^{(m+k)\times(m+k)}$

6 : **return** $((\mathbf{X}_1, \mathbf{X}_2), \mathbf{U})$

Thank you!

Sasha Lapiha, Royal Holloway University of London

References

- [AGHS13] - Shweta Agrawal, Craig Gentry, Shai Halevi, and Amit Sahai. Discrete Gaussian leftover hash lemma over infinite domains.

- [AR16] - Divesh Aggarwal and Oded Regev. A note on discrete gaussian combinations of lattice vectors

- [LPSS14] - San Ling, Duong Hieu Phan, Damien Stehle, and Ron Steinfeld. Hardness of k-LWE and applications in traitor tracing.

- [NP20] - Hoi H. Nguyen and Elliot Paquette. Surjectivity of near-square random matrices.

- [Sil85] - Jack W. Silverstein. The smallest eigenvalue of a large dimensional wishart matrix.