Gram Root Decomposition over the Polynomial Ring: Application to Sphericalization of Discrete Gaussian

Hiroki Okada[1,2][a] and Tsuyoshi Takagi[2]

[1] *KDDI Research, Inc., Saitama, 356-8502 Japan*

[2] *The University of Tokyo, Tokyo, 113-8654 Japan*

Keywords: Lattice-Based Cryptography, Polynomial Ring, Discrete Gaussian, Gram Root Decomposition.

Abstract: Efficient construction of lattice-based cryptography is often based on the polynomial ring. Furthermore, many advanced lattice-based cryptosystems require the analysis of the discrete Gaussian under convolutions and linear transformations. In this paper, we present an efficient *Gram root decomposition* algorithm of the polynomial ring and an application to sphericalization of the discrete Gaussian. Let r be a polynomial of spherical discrete Gaussian coefficients and e be a fixed polynomial. Then, the coefficient vector of $r \cdot e$ is (statistically close to) non-spherical discrete Gaussian whose (scaled) covariance matrix is $\mathbf{G}_e := \mathbf{E}\mathbf{E}^\intercal$, where $\mathbf{E}$ is composed of rotations of the coefficient vector of e. Given $\mathbf{G}_e$, our algorithm outputs polynomials $\zeta_1, \dots, \zeta_l$ s.t. $\sum_{i=1}^{l} \mathbf{G}_{\zeta_i} + \mathbf{G}_e$ is a scalar matrix. The objective of this algorithm is similar to the (ring version of) integral Gram root decomposition proposed by Ducas *et al.* (Eurocrypt 2020). Notably, our algorithm ensures the bounds of the norm of ζ_i and the minimum eigenvalue of $\mathbf{G}_{\zeta_i}$, whereas Ducas *et al.*'s algorithm does not ensure such bounds. Owing to the bounds, we can obtain a polynomial $(r_0 e + \sum_{i=1}^{l} r_i \zeta_i)$ whose coefficients are spherical discrete Gaussians, where r_i are polynomials with discrete Gaussian coefficients; i.e., we can "cancel out" the dependence between the coefficients.

1 INTRODUCTION

Lattice-based cryptosystems (Kiltz et al., 2018; Bos et al., 2018; Fouque et al., 2020) have been selected as NIST post-quantum cryptography (PQC) standards (Alagic et al., 2022). Lattice-based schemes, including the PQC standards, are often based on polynomial rings i.e., NTRU (Hoffstein et al., 1998; Fouque et al., 2020), Ring-LWE (Stehlé et al., 2009; Lyubashevsky et al., 2010) and Module-LWE (Brakerski et al., 2011; Langlois and Stehlé, 2015), to achieve better efficiency.

The discrete Gaussian probability distribution (Definition 2.2) is an important object in lattice cryptography, and more generally the mathematical aspects of lattices. For example, the analysis of the computational hardness of lattice problems (Regev, 2005; Micciancio and Regev, 2007; Gentry et al., 2008; Peikert, 2009; Brakerski et al., 2013) relies on the useful properties of discrete Gaussians.

In addition, many advanced lattice-based cryptosystems such as identity-based encryption (Gentry et al., 2008; Agrawal et al., 2010) and functional encryption (Agrawal et al., 2011) require algorithms to sample discrete Gaussian that are efficient and secure against side-channel attacks, e.g., (Gentry et al., 2008; Peikert, 2010; Micciancio and Peikert, 2012; Micciancio and Walter, 2017; Genise and Micciancio, 2018; Ducas et al., 2020). While most works rely on floating-point arithmetic (FPA), Ducas *et al.* (Ducas et al., 2020) presented an algorithm without FPA, which is efficient and amenable to side-channel countermeasures. The core technique of (Ducas et al., 2020) is the integral matrix Gram root decomposition, which is an algorithm to obtain an integer matrix $\mathbf{A}$ s.t. $\mathbf{G} = \mathbf{A}\mathbf{A}^\intercal$ for the target covariance matrix $\mathbf{G}$.

Many studies have analyzed the properties (e.g., correlation, convolutions, linear transformation) of discrete Gaussians: (Peikert, 2010; Agrawal et al., 2013; Aggarwal and Regev, 2016; Genise et al., 2020; Okada et al., 2023). The discrete Gaussian distribution is called *spherical* if its covariance matrix is a scalar matrix, and *ellipsoidal* otherwise. Although lattice-based cryptography usually uses the spherical discrete Gaussian, some applications rely on the ellipsoidal discrete Gaussian because of some artifacts of the proof techniques (Agrawal et al., 2013). As dis-

[a] https://orcid.org/0000-0002-5687-620X

Okada, H. and Takagi, T.
Gram Root Decomposition over the Polynomial Ring: Application to Sphericalization of Discrete Gaussian.
DOI: 10.5220/0013139700003899
Paper published under CC license (CC BY-NC-ND 4.0)
In *Proceedings of the 11th International Conference on Information Systems Security and Privacy (ICISSP 2025) - Volume 2*, pages 306-317
ISBN: 978-989-758-735-1; ISSN: 2184-4356

cussed in (Lyubashevsky et al., 2010), an ellipsoidal discrete Gaussian makes certain applications and their proofs are more cumbersome than the case with the spherical discrete Gaussian.

Our Contributions. In this paper, we advance the research on the properties of ring polynomials whose coefficients are distributed accordingly to the discrete Gaussian distribution. Our contributions are 1) an algorithm for Gram root decomposition over the ring and 2) its application to the sphericalization of a discrete Gaussian over the ring.

Root Decomposition over the Ring First, we present an efficient *Gram root decomposition* algorithm of polynomials.

Let r be a polynomial over the ring $\mathfrak{R}$ (defined in Eq. (1)) whose coefficient vector (Definition 3.7) is a multivariate spherical discrete Gaussian, and let e be a fixed polynomial over $\mathfrak{R}$. Then, the coefficient vector of $r \cdot e$ is (statistically close to) nonspherical discrete Gaussian whose (scaled) covariance matrix is $\mathbf{G}_e := \mathbf{E}\mathbf{E}^{\intercal}$, where $\mathbf{E}$ is composed of rotations of the coefficient vector of e. That is, $\mathbf{E}$ is the coefficient matrix of e, and $\mathbf{G}_e$ is the coefficient Gram matrix of e, as defined in Definition 3.7.

Given e (and $\mathbf{G}_e$), our Gram root decomposition algorithm outputs polynomials $\zeta_1, \ldots, \zeta_l$ s.t. $\sum_{i=1}^{l} \mathbf{G}_{\zeta_i} + \mathbf{G}_e$ [1] become a scalar matrix $\beta\mathbf{I}$ for some $\beta > 0$, where $\mathbf{G}_{\zeta_i}$ is the coefficient Gram matrix of ζ_i. In other words, the Gram root decomposition algorithm outputs polynomials whose sums of coefficients Gram matrices can "diagonalize" the given matrix $\mathbf{G}_e$.

Notably, this algorithm also ensures an upper bound of the norm of ζ_i and a lower bound of the minimum eigenvalue of $\mathbf{G}_{\zeta_i}$. These bounds are crucial for our second convolution described below. The objective of our Gram root decomposition algorithm is similar to that of the integral Gram root decomposition proposed by Ducas *et al*. (Ducas et al., 2020). However, their method does not ensure the bounds on the outputs as does our algorithm; thus, it is not sufficient for the application that we will explain later.

Application: Sphericalizing the Discrete Gaussian over the Ring. As an application of our root Gram root decomposition algorithm, we show how to "sphericalize" ring polynomials with (ellipsoidal) discrete Gaussian coefficients. Let $r_0, \ldots, r_l$ be polynomials with a spherical discrete Gaussian coefficient vector. Given a fixed $e \in \mathfrak{R}$ and $\mathbf{G}_e$, output polynomials $\zeta_1, \ldots, \zeta_l$ s.t. $\sum_{i=1}^{l} \mathbf{G}_{\zeta_i} + \mathbf{G}_e = \beta\mathbf{I}$ by using our Gram root decomposition algorithm. Then, we show that the coefficient vector of the polynomial $(r_0 e + \sum_{i=1}^{l} r_i \zeta_i) \in \mathfrak{R}$ follows discrete Gaussian distribution whose covariance is a scalar matrix $\beta\mathbf{I}$, i.e., a spherical discrete Gaussian.

Notably, the above convolution theorem requires a lower-bound of the minimum eigenvalue of $\mathbf{G}_{\zeta_i}$. It is not trivial to obtain a nonnegligibly large lower bound of the minimum eigenvalue of random matrices, as analyzed in, e.g., (Tao, 2012; Nguyen and Vu, 2016). Owing to the bounds ensured by our algorithm, we can prove the convolution theorem.

Organization. The remainder of this paper is organized as follows. In Section 2, we provide necessary definitions and lemmas. We analyze the basic properties of the polynomial ring of concern (defined in Eq. (1)) in Section 3, which are building blocks of this paper and may be of independent interest. We propose our Gram root decomposition algorithm in Section 4. Then, as an application, we show how to sphericalize discrete Gaussians in Section 5. Finally, we summarize this paper and discuss future work in Section 6.

2 PRELIMINARIES

In Section 2.1, we provide the notations used in this paper. Then, we provide necessary the definitions and lemmas of lattices in Section 2.2 and the Gaussian distribution in Section 2.3.

2.1 Notations

The base 2 logarithm is denoted by log. For $N \in \mathbb{N}$, define $[N] := \{1, \ldots, N\}$. The size of set S is denoted by $|S|$.

We use bold lower-case for vectors and bold upper-case for matrices. We write the transpose of $\mathbf{x}$ as $\mathbf{x}^{\intercal}$. The l_2-norm and l_∞-norm of $\mathbf{x}$ is denoted by $\|\mathbf{x}\|$ and $\|\mathbf{x}\|_\infty$, respectively. We denote the identity matrix by $\mathbf{I}_n \in \mathbb{Z}^{n \times n}$. We write $\mathbf{G} \succ 0$ if $\mathbf{G}$ is positive definite. A square root of $\mathbf{G} \succ 0$ is a nonsingular matrix $\mathbf{S}$ such that $\mathbf{S}\mathbf{S}^{\intercal} = \mathbf{G}$, which is written as $\mathbf{S} = \sqrt{\mathbf{G}}$. Note that $(\sqrt{\mathbf{G}})^{-1} = \mathbf{S}^{-1} = (\mathbf{S}^{-\intercal})^{\intercal} = (\sqrt{\mathbf{G}^{-1}})^{\intercal}$ holds. The largest and smallest singular values of a matrix $\mathbf{S}$ are denoted by $\sigma_{\max}(\mathbf{S})$ and $\sigma_{\min}(\mathbf{S})$, respectively. We denote by $\|\mathbf{S}\|$ the matrix norm of $\mathbf{S}$ induced by the l_2-norm. Note that we have $\sigma_{\max}(\mathbf{S}) = \|\mathbf{S}\|$, and if $\sigma_{\min}(\mathbf{S}) \neq 0$, i.e., $\mathbf{S}$ is nonsingular, then $\sigma_{\min}(\mathbf{S})^{-1} = \|\mathbf{S}^{-1}\|$ holds. The Frobenius norm of $\mathbf{S}$ is $\|\mathbf{S}\|_F = \sqrt{\mathrm{tr}(\mathbf{S}^{\intercal}\mathbf{S})}$. Let $\|\mathbf{S}\|_{\mathrm{len}} = \max_{i \in [n]} \|\mathbf{s}_i\|$, where $\mathbf{s}_i$ is the i-th column vector of $\mathbf{S}$, then we have:

[1] More generally, given $e_1, \ldots, e_m$, our algorithm outputs $\zeta_1, \ldots, \zeta_l$ s.t. $\sum_{i=1}^{l} \mathbf{G}_{\zeta_i} + \sum_{i=1}^{m} \mathbf{G}_{e_i}$. We set $m = 1$ in the abstract and Section 1 for simplicity.

Fact 2.1. *For any matrix* $\mathbf{S}$*, we have* $\|\mathbf{S}\|_{\text{len}} \le \|\mathbf{S}\| \le \|\mathbf{S}\|_F$*,* $\|\mathbf{S}_1\mathbf{S}_2\|_{\text{len}} \le \|\mathbf{S}_1\|\|\mathbf{S}_2\|_{\text{len}} \le \|\mathbf{S}_1\|\|\mathbf{S}_2\|$*.*

2.2 Lattices

A lattice $\mathcal{L}$ is the set of all integer linear combinations of linearly independent vectors $\mathbf{b}_1, \cdots, \mathbf{b}_n \in \mathbb{R}^m$, i.e., $\mathcal{L} = \{\sum_{i=1}^n z_i \mathbf{b}_i \mid \mathbf{z} \in \mathbb{Z}^n\}$. If we arrange the vectors $\mathbf{b}_i$ as the columns of a matrix $\mathbf{B} \in \mathbb{R}^{m\times n}$, then we have

$$\mathcal{L} := \mathcal{L}(\mathbf{B}) = \{\mathbf{B}\mathbf{z} \mid \mathbf{z} \in \mathbb{Z}^n\} = \mathbf{B}\mathbb{Z}^n.$$

The rank of this lattice is n and its dimension is m. If $n = m$, then the lattice is called full rank. For arbitrary $\mathbf{c} \in \mathbb{R}^m$, a coset of lattice $\mathcal{L}$ is defined as $\mathcal{L} + \mathbf{c} := \{\mathbf{v} + \mathbf{c} \mid \mathbf{v} \in \mathcal{L}\}$. The dual of a lattice $\mathcal{L}$ is $\widehat{\mathcal{L}} := \{\mathbf{x} \mid \forall \mathbf{y} \in \mathcal{L}, \langle \mathbf{x}, \mathbf{y}\rangle \in \mathbb{Z}\}$. We denote the volume of the fundamental parallelepiped of $\mathcal{L}$ as $\det(\mathcal{L})$. We have $\det(\widehat{\mathcal{L}}) = 1/\det(\mathcal{L})$. For a full-rank lattice $\mathcal{L}(\mathbf{B})$, we have $\det(\mathcal{L}(\mathbf{B})) = |\det(\mathbf{B})|$. For n-rank lattice $\mathcal{L}$ and $i = 1, \ldots, n$, the successive minimum $\lambda_i(\mathcal{L})$ is defined as the radius of the smallest ball that contains i linearly independent vectors in $\mathcal{L}$. The integer lattice $\mathcal{L} := \mathbb{Z}^n$ is the primary focus of this paper.

2.3 Gaussians

The continuous Gaussian distribution with a mean of 0 and a standard deviation $\sigma > 0$ is denoted as $\mathcal{N}_\sigma$.

For a rank-n matrix $\mathbf{S} \in \mathbb{R}^{n\times m}$, the (centered) ellipsoidal Gaussian function on $\mathbb{R}^n$ with the (scaled) covariance matrix $\mathbf{G} = \mathbf{S}\mathbf{S}^\mathsf{T} \in \mathbb{R}^{n\times n}$ is defined as:

$$\rho_{\mathbf{S}}(\mathbf{x}) := \exp(-\pi \mathbf{x}^\mathsf{T}(\mathbf{S}\mathbf{S}^\mathsf{T})^{-1}\mathbf{x}).$$

Since the function $\rho_{\mathbf{S}}(\mathbf{x})$ is determined exactly by $\mathbf{G}$, we have $\rho_{\mathbf{S}} = \rho_{\sqrt{\mathbf{G}}}$. When $\mathbf{S} = s\mathbf{I}_n$, we write $\rho_{\mathbf{S}}$ as ρ_s. For any set $A \subseteq \mathbb{R}^n$, we define $\rho_{\mathbf{S}}(A) := \sum_{\mathbf{x}\in A} \rho_{\mathbf{S}}(\mathbf{x})$.

We define the discrete Gaussian distribution over the lattice $\mathcal{L}$ as follows:

Definition 2.2 (Discrete Gaussian). *For a full column-rank matrix* $\mathbf{S}$*, the (centered) discrete Gaussian distribution over a lattice* $\mathcal{L}$ *is defined as*

$$\forall \mathbf{x} \in \mathcal{L}, D_{\mathcal{L},\mathbf{S}}(\mathbf{x}) = \rho_{\mathbf{S}}(\mathbf{x})/\rho_{\mathbf{S}}(\mathcal{L}).$$

In particular, when $\mathbf{S}\mathbf{S}^\mathsf{T} = s^2\mathbf{I}_n$ *for some* $s > 0$*, we abbreviate* $D_{\mathcal{L},\mathbf{S}}$ *as* $D_{\mathcal{L},s}$ *and call it the spherical discrete Gaussian distribution.*

The *smoothing parameter* of lattice $\mathcal{L}$ is defined as $\eta_\varepsilon(\mathcal{L}) = \min\{s \mid \rho_{1/s}(\widehat{\mathcal{L}}) \le 1 + \varepsilon\}$ for $\varepsilon > 0$. Unless otherwise specified, we set ε to be negligibly small; $\varepsilon = \text{negl}(\lambda)$. An upper-bound of $\eta_\varepsilon(\mathcal{L})$ is obtained by the successive minimum[2] $\lambda_n(\mathcal{L})$:

Lemma 2.3 ((Micciancio and Regev, 2007, Lemma 3.3)). *Define* $\eta^+_\varepsilon(\mathbb{Z}^n) := \sqrt{\ln(2n(1+1/\varepsilon))/\pi}$*. For any rank-n lattice* $\mathcal{L}$ *and any* $\varepsilon > 0$*, we have* $\eta_\varepsilon(\mathcal{L}) \le \lambda_n(\mathcal{L})\eta^+_\varepsilon(\mathbb{Z}^n)$*. In particular,* $\eta_\varepsilon(\mathbb{Z}^n) \le \eta^+_\varepsilon(\mathbb{Z}^n)$ *holds.*

For simplicity of notation, we also define $\tilde{\eta}_\varepsilon(\cdot) := \sqrt{2}\eta_\varepsilon(\cdot)$ and $\tilde{\eta}^+_\varepsilon(\mathbb{Z}^n) := \sqrt{2}\eta^+_\varepsilon(\mathbb{Z}^n)$. Note that we have $\tilde{\eta}^+_\varepsilon(\mathbb{Z}) > \eta^+_\varepsilon(\mathbb{Z}^2)$. The smoothing parameter is extended to matrices as follows:

Definition 2.4 ((Peikert, 2010, Definition 2.3)). *Let* $\mathbf{G} \succ 0$ *be any positive definite matrix. For any lattice* $\mathcal{L}$*, we say that* $\sqrt{\mathbf{G}} \ge \eta_\varepsilon(\mathcal{L})$ *if* $\eta_\varepsilon(\sqrt{\mathbf{G}}^{-1}\mathcal{L}) \le 1$*.*

For a full-rank lattice, we obtain a sufficient condition as follows:

Fact 2.5. *For any full-rank lattice* $\mathcal{L}(\mathbf{B})$ *and* $\mathbf{G} \succ 0$*,* $\sqrt{\mathbf{G}} \ge \eta_\varepsilon(\mathcal{L})$ *holds if* $1 \ge \|\sqrt{\mathbf{G}}^{-1}\|\|\mathbf{B}\|_{\text{len}}\eta^+_\varepsilon(\mathbb{Z}^n)$*, i.e.,* $\sigma_{\min}(\sqrt{\mathbf{G}}) \ge \|\mathbf{B}\|_{\text{len}}\eta^+_\varepsilon(\mathbb{Z}^n)$*.*

Proof. By Fact 2.1 and Lemma 2.3, we have $\eta_\varepsilon(\sqrt{\mathbf{G}}^{-1}\mathcal{L}) \le \lambda_n(\sqrt{\mathbf{G}}^{-1}\mathcal{L})\eta^+_\varepsilon(\mathbb{Z}^n) \le \|\sqrt{\mathbf{G}}^{-1}\mathbf{B}\|_{\text{len}} \eta^+_\varepsilon(\mathbb{Z}^n) \le \|\sqrt{\mathbf{G}}^{-1}\|\|\mathbf{B}\|_{\text{len}}\eta^+_\varepsilon(\mathbb{Z}^n) \le 1$. □

The linear transformation of a discrete Gaussian is as follows:

Lemma 2.6 (Special case of (Genise et al., 2020, Lemma 1)). *For any nonsingular matrices* $\mathbf{S}, \mathbf{T} \in \mathbb{Z}^{n\times n}$*, we have* $\mathbf{T} \cdot D_{\mathbb{Z}^n,\mathbf{S}} = D_{\mathbf{T}\cdot\mathbb{Z}^n,\mathbf{T}\mathbf{S}}$*.*

The sum of two ellipsoidal discrete Gaussians is statistically close to an ellipsoidal discrete Gaussian:

Lemma 2.7 (Special case of (Peikert, 2010, Thm. 3.1)). *Let* $\mathbf{G}_1, \mathbf{G}_2 \succ 0$ *be positive definite matrices and define* $\mathbf{G}_3 := (\mathbf{G}_1^{-1} + \mathbf{G}_2^{-1})^{-1}$*. Let* $\mathcal{L}_1$*,* $\mathcal{L}_2$ *be full-rank lattices such that* $\sqrt{\mathbf{G}_2} \ge \eta_\varepsilon(\mathcal{L}_2)$ *and* $\sqrt{\mathbf{G}_3} \ge \eta_\varepsilon(\mathcal{L}_1)$*, and let*

$$X := \{(\mathbf{x}_1, \mathbf{x}_2) | \mathbf{x}_1 \leftarrow D_{\mathcal{L}_1,\sqrt{\mathbf{G}_1}}, \mathbf{x}_2 \leftarrow \mathbf{x}_1 + D_{\mathcal{L}_2-\mathbf{x}_1,\sqrt{\mathbf{G}_2}}\}.$$

Then, the marginal distribution of $\mathbf{x}_2$ *in* X *is statistically close to* $D_{\mathcal{L}_2,\sqrt{\mathbf{G}_1+\mathbf{G}_2}}$*.*

In particular, when $\mathcal{L}_1 \subseteq \mathcal{L}_2$, we can simplify Lemma 2.7 because the coset $\mathcal{L}_2 - \mathbf{x}_1$ is equal to $\mathcal{L}_2$ itself for any $\mathbf{x}_1 \in \mathcal{L}_1$:

Corollary 2.8. *Let* $\mathbf{G}_1, \mathbf{G}_2 \succ 0$ *be positive definite matrices and define* $\mathbf{G}_3 := (\mathbf{G}_1^{-1} + \mathbf{G}_2^{-1})^{-1}$*. Let* $\mathcal{L}_1$*,* $\mathcal{L}_2$ *be full-rank lattices such that* $\mathcal{L}_1 \subseteq \mathcal{L}_2$*,* $\sqrt{\mathbf{G}_2} \ge \eta_\varepsilon(\mathcal{L}_2)$ *and* $\sqrt{\mathbf{G}_3} \ge \eta_\varepsilon(\mathcal{L}_1)$*. Then, we have*

$$D_{\mathcal{L}_1,\sqrt{\mathbf{G}_1}} + D_{\mathcal{L}_2,\sqrt{\mathbf{G}_2}} \approx_{\text{s}} D_{\mathcal{L}_2,\sqrt{\mathbf{G}_1+\mathbf{G}_2}}.$$

[2] Although (Gentry et al., 2008, Lemma 3.1) provides a sharper bound, we rely on Lemma 2.3 for simplicity.

3 PROPERTIES OF THE POLYNOMIAL RING

In this section, we analyze the basic properties of the polynomial ring defined in Eq. (1). The properties derived in this section are the building blocks for the construction of our algorithm presented in Section 5.

3.1 Definition

Let $\mathbb{Z}[X]$ be a set of polynomials with integer coefficients. In this paper, we consider a polynomial ring

$$\mathfrak{R} = \mathbb{Z}[X]/(X^n + 1) \text{ for } n \text{ a power of 2,} \quad (1)$$

which is often used in lattice-based cryptography, e.g., (Lyubashevsky et al., 2010; Kiltz et al., 2018; Bos et al., 2018).

We define a signed permutation matrix that is useful for analyzing the properties of $\mathfrak{R}$.

Definition 3.1. *The signed permutation matrix is defined as*

$$\mathbf{P} = \left(\begin{array}{c|c} \mathbf{0} & -1 \\ \hline \mathbf{I}_{n-1} & \mathbf{0} \end{array}\right) \in \mathbb{Z}^{n\times n}. \quad (2)$$

The following facts hold for $\mathbf{P}$:

Fact 3.2 (Properties of P). *For* $\mathbf{P}$ *defined in Eq.* (2)*, we have:*

$$\mathbf{P}^i = \left(\begin{array}{c|c} \mathbf{O} & -\mathbf{I}_i \\ \hline \mathbf{I}_{n-i} & \mathbf{O} \end{array}\right)$$

$$\mathbf{P}^{n/2} = \left(\begin{array}{c|c} \mathbf{O} & -\mathbf{I}_{n/2} \\ \hline \mathbf{I}_{n/2} & \mathbf{O} \end{array}\right) \textit{for n even} \quad (3)$$

$$\mathbf{P}^{-i} = \left(\begin{array}{c|c} \mathbf{O} & \mathbf{I}_{n-i} \\ \hline -\mathbf{I}_i & \mathbf{O} \end{array}\right) = (\mathbf{P}^i)^\intercal \quad (4)$$

$$\mathbf{P}^{n-i} = \mathbf{P}^n\mathbf{P}^{-i} = -\mathbf{P}^{-i} = -(\mathbf{P}^i)^\intercal \quad (5)$$

We also define a reverse permutation matrix:

Definition 3.3. *The reverse permutation matrix is define as*

$$\mathbf{R} := \begin{pmatrix} 0 & \dots & 1 \\ \vdots & 1 & \vdots \\ 1 & \dots & 0 \end{pmatrix} \in \mathbb{Z}^{n\times n}.$$

The following facts hold for $\mathbf{R}$ (and $\mathbf{P}$):

Fact 3.4. $\mathbf{RR} = \mathbf{I}, \quad \mathbf{R}^\intercal = \mathbf{R}$

Fact 3.5. $\mathbf{P}^i\mathbf{R} = \mathbf{RP}^{-i} \quad (\mathbf{RP}^i = \mathbf{P}^{-i}\mathbf{R})$

We define an outer-product-like operation $\otimes$:

Definition 3.6 ($\otimes$)**.** *For any* $m, n \in \mathbb{N}$, $\mathbf{A}_1, \dots, \mathbf{A}_m \in \mathbb{Z}^{n\times n}$ *and* $\mathbf{b} \in \mathbb{Z}^n$*, we define:*

$$(\mathbf{A}_1 \cdots \mathbf{A}_m) \otimes \mathbf{b} := (\mathbf{A}_1\mathbf{b} \cdots \mathbf{A}_m\mathbf{b}) \in \mathbb{Z}^{n\times m}$$

$$\mathbf{b}^\intercal \otimes \begin{pmatrix} \mathbf{A}_1 \\ \vdots \\ \mathbf{A}_m \end{pmatrix} := \begin{pmatrix} \mathbf{b}^\intercal\mathbf{A}_1 \\ \vdots \\ \mathbf{b}^\intercal\mathbf{A}_m \end{pmatrix} \in \mathbb{Z}^{m\times n}$$

Finally, using the $\mathbf{P}$ defined in Definition 3.1 and the operation $\otimes$, we define the *coefficient vector*, *coefficient matrix* and *coefficient Gram matrix* for any polynomial $a \in \mathfrak{R}$ as follows:

Definition 3.7 (Coefficient vector / matrix / Gram matrix). *Let* $a = \sum_{i=0}^{n-1} a_i X^i \in \mathfrak{R}$ *be a polynomial. For a, we define the coefficient vector, the coefficient matrix and the coefficient Gram matrix as follows:*

$$\mathbf{a} := \mathsf{vec}(a) := (a_0, a_1, \dots, a_{n-1})^\intercal \in \mathbb{Z}^n$$
$$\mathbf{A} := \mathsf{mat}(a) := \begin{pmatrix} \mathbf{I} & \mathbf{P} & \cdots & \mathbf{P}^{n-1} \end{pmatrix} \otimes \mathbf{a} \in \mathbb{Z}^{n\times n}$$
$$\mathbf{G}_a := \mathsf{Gram}(a) := \mathbf{AA}^\intercal \in \mathbb{Z}^{n\times n}.$$

We denote the distribution over $\mathfrak{R}$ as follows:

Definition 3.8. *For the distribution* χ *over* $\mathbb{Z}^n$*, define*

$$\mathfrak{R}(\chi) := \{a \in \mathfrak{R} \mid \mathsf{vec}(a) \sim \chi\}.$$

3.2 Properties of the Coefficient Matrix

In this subsection, we present some basic properties of the coefficient matrix ($\mathsf{mat}(a)$). By Definitions 3.1, 3.6 and 3.7, for any $a \in \mathfrak{R}$ s.t. $\mathsf{vec}(a) := (a_0, a_1, \dots, a_{n-1})^\intercal \in \mathbb{Z}^n$, we have:

$$\begin{aligned} \mathsf{mat}(a) &:= \begin{pmatrix} \mathbf{I} & \mathbf{P} & \dots & \mathbf{P}^{n-1} \end{pmatrix} \otimes \mathsf{vec}(a) \\ &:= \begin{pmatrix} \mathbf{a} & \mathbf{Pa} & \dots & \mathbf{P}^{n-1}\mathbf{a} \end{pmatrix} \\ &= \begin{pmatrix} a_0 & -a_{n-1} & \dots & -a_1 \\ a_1 & a_0 & \dots & -a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & \dots & a_0 \end{pmatrix} \end{aligned} \quad (6)$$

We can see that $\mathsf{mat}(a)$ is a matrix composed of permutations (by $\mathbf{P}^i$) of the first column vector $\mathbf{a} = \mathsf{vec}(a)$. The coefficient matrix $\mathsf{mat}(a)$ can also be seen a matrix composed of permutations of the *last row vector* $(a_{n-1}, a_{n-2}, a_{n-3}, \dots, a_0) = \mathbf{a}^\intercal\mathbf{R}$:

Fact 3.9 (Dual representation of $\mathsf{mat}(a)$**).** *For any* $a \in \mathfrak{R}$*, we have:*

$$\mathsf{mat}(a) = \mathbf{a}^\intercal\mathbf{R} \otimes \begin{pmatrix} \mathbf{P}^{n-1} \\ \vdots \\ \mathbf{P} \\ \mathbf{I} \end{pmatrix}$$

3.3 Properties of the Coefficient Gram Matrix

In this subsection, we present some basic properties of the coefficient Gram matrix ($\mathsf{mat}(a)$). We can explicitly write the coefficient Gram matrix as follows:

Fact 3.10. *Let $a \in \mathfrak{R}$ and $\mathbf{a} := \mathsf{vec}(a)$. Then, we have:*

$$
\begin{aligned}
&\mathsf{Gram}(a)\\
&= \begin{pmatrix}
\|\mathbf{a}\|^2 & \mathbf{a}^\intercal\mathbf{P}\mathbf{a} & \cdots & \mathbf{a}^\intercal\mathbf{P}^{n-1}\mathbf{a}\\
\mathbf{a}^\intercal\mathbf{P}^{-1}\mathbf{a} & \|\mathbf{a}\|^2 & \cdots & \mathbf{a}^\intercal\mathbf{P}^{n-2}\mathbf{a}\\
\vdots & & \ddots & \vdots\\
\mathbf{a}^\intercal\mathbf{P}^{-(n-1)}\mathbf{a} & \mathbf{a}^\intercal\mathbf{P}^{-(n-2)}\mathbf{a} & \cdots & \|\mathbf{a}\|^2
\end{pmatrix}
\end{aligned}
$$

Proof. By Definition 3.7, Fact 3.4, Fact 3.5 and Fact 3.9, we have:

$$
\begin{aligned}
&\mathsf{Gram}(a)\\
&:= \mathsf{mat}(a)(\mathsf{mat}(a))^\intercal\\
&= \mathbf{a}^\intercal\mathbf{R} \otimes \begin{pmatrix}\mathbf{P}^{n-1}\\ \cdots\\ \mathbf{P}\\ \mathbf{I}\end{pmatrix} \cdot \begin{pmatrix}\mathbf{P}^{-(n-1)} & \ldots & \mathbf{I}\end{pmatrix} \otimes \mathbf{R}\mathbf{a}\\
&= \mathbf{a}^\intercal\mathbf{R} \otimes \begin{pmatrix}
\mathbf{I} & \mathbf{P} & \cdots & \mathbf{P}^{n-1}\\
\mathbf{P}^{-1} & \mathbf{I} & \cdots & \mathbf{P}^{n-2}\\
\vdots & & \ddots & \vdots\\
\mathbf{P}^{-(n-1)} & \mathbf{P}^{-(n-2)} & \cdots & \mathbf{I}
\end{pmatrix} \otimes \mathbf{R}\mathbf{a}\\
&= \begin{pmatrix}
\|\mathbf{a}\|^2 & \mathbf{a}^\intercal\mathbf{P}^{-1}\mathbf{a} & \cdots & \mathbf{a}^\intercal\mathbf{P}^{-(n-1)}\mathbf{a}\\
\mathbf{a}^\intercal\mathbf{P}\mathbf{a} & \|\mathbf{a}\|^2 & \cdots & \mathbf{a}^\intercal\mathbf{P}^{-(n-2)}\mathbf{a}\\
\vdots & \vdots & \ddots & \vdots\\
\mathbf{a}^\intercal\mathbf{P}^{n-1}\mathbf{a} & \mathbf{a}^\intercal\mathbf{P}^{n-2}\mathbf{a} & \cdots & \|\mathbf{a}\|^2
\end{pmatrix}
\end{aligned}
$$

Thus, the claim follows by subsequent Fact 3.11. □

Fact 3.11. $\mathbf{a}^\intercal\mathbf{P}^i\mathbf{a} = \mathbf{a}^\intercal(\mathbf{P}^i)^\intercal\mathbf{a} = \mathbf{a}^\intercal\mathbf{P}^{-i}\mathbf{a}$

Proof. Follows from Fact 3.2: $(\mathbf{P}^i)^\intercal = \mathbf{P}^{-i}$. □

Furthermore, owing to the properties of $\mathbf{P}$ (shown in Fact 3.2), we show that coefficient Gram matrices have symmetricity in their elements. To begin with, we define the inverse function of $\mathsf{mat}(\cdot)$ for simplicity of notation.

Definition 3.12 (mat^{-1}). *For any $a \in \mathfrak{R}$ and $\mathbf{A} := \mathsf{mat}(a)$, we define $\mathsf{mat}^{-1}(\mathbf{A}) := \mathbf{a} = \mathsf{vec}(a)$ (the first column vector of $\mathbf{A}$).*

Then, we show the symmetricity of the elements of the coefficient Gram matrices. Note that the coefficient Gram matrix of $a \in \mathfrak{R}$ is a coefficient matrix of some $b (= \overline{a}a) \in \mathfrak{R}$, as we will show later in Lemma 3.21.

Lemma 3.13 (Symmetricity of $\mathsf{Gram}(a)$). *Let $a \in \mathfrak{R}$, $\mathbf{a} := \mathsf{vec}(a)$, $\mathbf{G}_a := \mathsf{Gram}(a)$ and $(\sigma_0, \ldots, \sigma_{n-1}) := \mathsf{mat}^{-1}(\mathbf{G}_a)$. Then, we have:*

$$
\begin{aligned}
\sigma_0 &= \|\mathbf{a}\|^2 \\
\sigma_i &= -\sigma_{n-i} \quad \left(1 \le i \le \tfrac{n}{2} - 1\right) && (7)\\
\sigma_{\frac{n}{2}} &= 0 && (8)
\end{aligned}
$$

(Note: Here, n is assumed to be even. This is satisfied by the definition of Eq. (1)*.)*

Proof. By Fact 3.10, we have:

$$
\begin{cases}
\sigma_0 &= \|\mathbf{a}\|^2\\
\sigma_i &= \mathbf{a}^\intercal\mathbf{P}^{-i}\mathbf{a} \quad (i = 1, \ldots, n-1)
\end{cases}.
$$

Then, for $(i = 1, \ldots, n-1)$, we have:

$$
\begin{aligned}
-\sigma_{n-i} &= -\mathbf{a}^\intercal\mathbf{P}^{-(n-i)}\mathbf{a} = -\mathbf{a}^\intercal(\mathbf{P}^{n-i})^\intercal\mathbf{a} \quad (\because \text{Eq. } (4))\\
&= -\mathbf{a}^\intercal\mathbf{P}^{n-i}\mathbf{a} = \mathbf{a}^\intercal\mathbf{P}^{i}\mathbf{a} = \sigma_i \quad (\because \text{Eq. } (5))
\end{aligned}
$$

Thus, Eq. (7) holds. We have Eq. (8) since $\mathbf{a}^\intercal\mathbf{P}^{\frac{n}{2}}\mathbf{a} = 0$ holds any $\mathbf{a} \in \mathbb{Z}^n$ by Eq. (3) in Fact 3.2. □

Owing to this symmetricity, $\mathbf{G}_a := \mathsf{Gram}(a)$ is determined only by $\sigma_0, \ldots, \sigma_{\frac{n}{2}-1}$ (since $\mathbf{A} := \mathsf{mat}(a)$ is determined only by $\mathbf{a} := \mathsf{vec}(a)$).

3.4 Rotation

For any $a \in \mathfrak{R}$, multiplication by X^i can be regarded as "rotation" of the coefficient vector/matrix by the permutation matrix $\mathbf{P}^i$. The coefficient Gram Matrix is invariant with respect to multiplication by X^i:

Fact 3.14 (Rotation). *For any $a \in \mathfrak{R}$ and $i \in \mathbb{Z}$,*

$$
\begin{aligned}
\mathsf{vec}(aX^i) &= \mathbf{P}^i\mathbf{a},\\
\mathsf{mat}(aX^i) &= \mathbf{P}^i\mathbf{A},\\
\mathsf{Gram}(aX^i) &= \mathsf{Gram}(a).
\end{aligned}
$$

Proof. Let $a = \sum_{i=0}^{n-1} a_i X^i$. Then, we have:

$$
\begin{aligned}
aX &= -a_{n-1} + a_0X + \cdots + a_{n-2}X^{n-1}\\
\mathsf{vec}(aX^i) &= \mathbf{P}^i\mathbf{a}\\
\mathsf{mat}(aX^i) &= \begin{pmatrix}\mathbf{I} & \mathbf{P} & \ldots & \mathbf{P}^{n-1}\end{pmatrix} \otimes \mathsf{vec}(aX^i)\\
&= \begin{pmatrix}\mathbf{I} & \mathbf{P} & \ldots & \mathbf{P}^{n-1}\end{pmatrix} \otimes \mathbf{P}^i\mathbf{a}\\
&= \mathbf{P}^i\begin{pmatrix}\mathbf{I} & \mathbf{P} & \ldots & \mathbf{P}^{n-1}\end{pmatrix} \otimes \mathbf{a}\\
&= \mathbf{P}^i\mathbf{A}\\
\mathsf{Gram}(aX^i) &= \mathbf{A}\mathbf{P}^i(\mathbf{A}\mathbf{P}^i)^\intercal = \mathbf{A}\mathbf{A}^\intercal \quad (\because \text{Eq. } (4))
\end{aligned}
$$
□

3.5 Commutativity

We show an important lemma to analyze the coefficient vector of the product of polynomials over $\mathfrak{R}$: This result is why we define the coefficient matrix as in Definition 3.7.

Lemma 3.15 (Multiplication over $\mathfrak{R}$). *For $a, b \in \mathfrak{R}$,*

$$
\mathsf{vec}(ab) = \mathbf{A}\mathbf{b} = \mathbf{B}\mathbf{a},
$$

where $\mathbf{A} := \mathsf{mat}(a)$, $\mathbf{a} := \mathsf{vec}(a)$, $\mathbf{B} := \mathsf{mat}(b)$, and $\mathbf{b} := \mathsf{vec}(b)$.

Proof. Note that $X^{n+i} = (X^n + 1)X^i - X^i \equiv -X^i$ holds. We have

$$a = a_0 + a_1 X + \cdots + a_{n-1}X^{n-1} = \mathbf{x}^\intercal \mathbf{a} \text{ and}$$
$$b = b_0 + b_1 X + \cdots + b_{n-1}X^{n-1} = \mathbf{x}^\intercal \mathbf{b},$$

where $\mathbf{a} := (a_0, a_1, \dots, a_{n-1})^\intercal$ and $\mathbf{b} := (b_0, b_1, \dots, b_{n-1})^\intercal$ are the coefficient vectors of a and b, and $\mathbf{x} := (1, X, X^2, \dots, X^{n-1})^\intercal$. Then, we have

$$\begin{aligned} ab =& (a_0b_0 - a_1b_{n-1} - a_2b_{n-2} \cdots - a_{n-1}b_1) \\ &+ (a_0b_1 + a_1b_0 - a_2b_{n-1} \cdots - a_{n-1}b_2)X \\ &+ (a_0b_2 + a_1b_1 + a_2b_0 \cdots - a_{n-1}b_3)X^2 + \dots \\ =& \mathbf{x}^\intercal \begin{pmatrix} b_0 & -b_{n-1} & \dots & -b_1 \\ b_1 & b_0 & \dots & -b_2 \\ \vdots & \vdots & \ddots & \vdots \\ b_{n-1} & b_{n-2} & \dots & b_0 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} \\ =& \mathbf{x}^\intercal \mathbf{B}\mathbf{a} \end{aligned}$$

Thus, we have $\mathsf{vec}(ab) = \mathbf{B}\mathbf{a}$. We obtain $\mathsf{vec}(ab) = \mathbf{A}\mathbf{b}$ in a similar manner. □

It is known that the ring $\mathfrak{R}$ defined in Eq. (1) is commutative: for any $a, b \in \mathfrak{R}$, we have $ab = ba$. This can also be confirmed by Lemma 3.15: we obtain $\mathsf{vec}(ab) = \mathbf{A}\mathbf{b} = \mathbf{B}\mathbf{a} = \mathsf{vec}(ba)$ by Lemma 3.15, and $\mathsf{vec}(\cdot)$ is isomorphic from $\mathfrak{R}$ to $\mathbb{Z}^n$.

Importantly, the coefficient matrix also has commutativity:

Theorem 3.16 (Commutativity of the coefficient matrices). *For any* $\mathbf{A} := \mathsf{mat}(a)$, $\mathbf{B} := \mathsf{mat}(b)$,

$$\mathsf{mat}(ab) = \mathbf{AB} = \mathbf{BA}$$

Proof. Let $\mathbf{a} := \mathsf{vec}(a)$ and $\mathbf{b} := \mathsf{vec}(b)$. We have:

$$\begin{aligned} &\mathsf{mat}(ab) \\ &= \begin{pmatrix} \mathbf{I} & \mathbf{P} & \dots & \mathbf{P}^{n-1} \end{pmatrix} \otimes \mathsf{vec}(ab) \\ &= \begin{pmatrix} \mathbf{I} & \mathbf{P} & \dots & \mathbf{P}^{n-1} \end{pmatrix} \otimes \mathbf{Ab} \quad (\because \text{Lemma 3.15}) \\ &= \begin{pmatrix} \mathbf{A} & \mathbf{PA} & \dots & \mathbf{P}^{n-1}\mathbf{A} \end{pmatrix} \otimes \mathbf{b} \\ &= \begin{pmatrix} \mathbf{A} & \mathbf{AP} & \dots & \mathbf{AP}^{n-1} \end{pmatrix} \otimes \mathbf{b} \ (\because \text{ Lemma 3.17}) \\ &= (\mathbf{A} \otimes \begin{pmatrix} \mathbf{I} & \mathbf{P} & \dots & \mathbf{P}^{n-1} \end{pmatrix}) \otimes \mathbf{b} \\ &= \mathbf{AB} \end{aligned}$$

By Lemma 3.15, $\mathsf{vec}(ab) = \mathbf{Ab} = \mathbf{Ba}$. Thus, similarly, we also have $\mathsf{mat}(ab) = \mathbf{BA}$. □

We complete the above proof by presenting the deferred Lemma 3.17:

Lemma 3.17. *For any* $a \in \mathfrak{R}$, $\mathbf{A} := \mathsf{mat}(a)$ *and* $i \in \mathbb{Z}$, *we have* $\mathbf{P}^i\mathbf{A} = \mathbf{AP}^i$

Proof. Let $\mathbf{a} := \mathsf{vec}(a)$. Then, we have

$$\begin{aligned} \mathbf{P}^i\mathbf{A} &= \mathbf{P}^i \cdot \begin{pmatrix} \mathbf{I} & \mathbf{P} & \dots & \mathbf{P}^{n-1} \end{pmatrix} \otimes \mathbf{a} \\ &= \begin{pmatrix} \mathbf{I} & \mathbf{P} & \dots & \mathbf{P}^{n-1} \end{pmatrix} \otimes \mathbf{P}^i\mathbf{a} = \mathsf{mat}(\mathbf{P}^i\mathbf{a}), \text{ and} \\ \mathbf{AP}^i &= \mathbf{a}^\intercal\mathbf{R} \otimes \begin{pmatrix} \mathbf{P}^{n-1} \\ \mathbf{P}^{n-2} \\ \vdots \\ \mathbf{P} \\ \mathbf{I} \end{pmatrix} \cdot \mathbf{P}^i = \mathbf{a}^\intercal\mathbf{R}\mathbf{P}^i \otimes \begin{pmatrix} \mathbf{P}^{n-1} \\ \mathbf{P}^{n-2} \\ \vdots \\ \mathbf{P} \\ \mathbf{I} \end{pmatrix} \\ &= (\mathbf{P}^i\mathbf{a})^\intercal\mathbf{R} \otimes \begin{pmatrix} \mathbf{P}^{n-1} \\ \mathbf{P}^{n-2} \\ \vdots \\ \mathbf{P} \\ \mathbf{I} \end{pmatrix} \quad (\because \text{Fact 3.5}) \\ &= \mathsf{mat}(\mathbf{P}^i\mathbf{a}), \end{aligned}$$

where we use the fact that $\mathbf{a}^\intercal\mathbf{R}\mathbf{P}^i = \mathbf{a}^\intercal\mathbf{P}^{-i}\mathbf{R} = (\mathbf{P}^i\mathbf{a})^\intercal\mathbf{R}$ holds. □

As a corollary of Lemma 3.15, we obtain the following fact:

Corollary 3.18. *For* $a, b \in \mathfrak{R}$, $ab = 0$ *holds if and only if* $a = 0$ *or* $b = 0$. *Thus,* $\mathbf{A} := \mathsf{mat}(a)$ *is nonsingular for any* $a \neq 0$.

3.6 Transpose

We first define the *transpose* of polynomials in $\mathfrak{R}$:

Definition 3.19 (*Transpose* in the ring). *For* $a := a(X) := \sum_{i=0}^{n-1} a_iX^i \in \mathfrak{R}$, *we define its transpose as* $\overline{a} := a(X^{-1}) \in \mathfrak{R}$.

Then, we can derive the coefficient vector, coefficient matrix and coefficient Gram matrix of the transpose polynomials as follows:

Fact 3.20. *For any* $a := \sum_{i=0}^{n-1} a_iX^i \in \mathfrak{R}$, *we have:*

$$\mathsf{vec}(\overline{a}) = (a_0, -a_{n-1}, -a_{n-2}, \dots, -a_1)^\intercal \tag{9}$$
$$\mathsf{mat}(\overline{a}) = (\mathsf{mat}(a))^\intercal (= \mathbf{A}^\intercal) \tag{10}$$
$$\mathsf{Gram}(\overline{a}) = (\mathsf{mat}(a))^\intercal \mathsf{mat}(a) (= \mathbf{A}^\intercal\mathbf{A}) \tag{11}$$

Proof. Note that $X^n + 1 \equiv 0 \Leftrightarrow -1 \equiv X^n \Leftrightarrow X^{-i} \equiv -X^{n-i}$ holds. Hence, we have

$$\begin{aligned} \overline{a} := a(X^{-1}) &:= \sum_{i=0}^{n-1} a_iX^{-i} = \sum_{i=0}^{n-1} (-a_i)X^{n-i} \\ &= a_0 + \sum_{i=1}^{n-1} (-a_{n-i})X^i. \end{aligned}$$

Thus, we obtain Eq. (9). We can derive Eq. (10) since

$$\begin{aligned} \mathsf{mat}(\overline{a}) &= \begin{pmatrix} \mathbf{I} & \mathbf{P} & \dots & \mathbf{P}^{n-1} \end{pmatrix} \otimes \mathsf{vec}(\overline{a}) \\ &= (\mathsf{mat}(a))^\intercal \end{aligned}$$

via Eq. (6). We obtain Eq. (11) by definition. □

Next, we show an important lemma to analyze the coefficient Gram matrix: for any $a \in \mathfrak{R}$, the coefficient Gram matrix of a is the coefficient matrix (not coefficient "Gram" matrix) of the product of $\overline{a}$ and a:

Lemma 3.21. *For any $a \in \mathfrak{R}$, $\mathsf{Gram}(a) = \mathsf{mat}(\overline{a}a)$.*

Proof. Let $\mathbf{A} := \mathsf{mat}(a)$ and $\mathbf{a} := \mathsf{vec}(a)$. Then, we have

$$\begin{aligned} &\mathsf{Gram}(a) \\ &= \mathbf{A}\mathbf{A}^\intercal = \mathbf{A}^\intercal\mathbf{A} \quad (\because \text{Theorem 3.16}) \\ &= \mathbf{A}^\intercal \begin{pmatrix} \mathbf{I} & \mathbf{P} & \dots & \mathbf{P}^{n-1} \end{pmatrix} \otimes \mathbf{a} \\ &= \begin{pmatrix} \mathbf{I} & \mathbf{P} & \dots & \mathbf{P}^{n-1} \end{pmatrix} \otimes \mathbf{A}^\intercal\mathbf{a} \quad (\because \text{Lemma 3.17}) \\ &= \begin{pmatrix} \mathbf{I} & \mathbf{P} & \dots & \mathbf{P}^{n-1} \end{pmatrix} \otimes \mathsf{vec}(\overline{a}a), \end{aligned}$$

where we use the fact $\mathsf{mat}(\overline{a}) = \mathbf{A}^\intercal$ (by Fact 3.20) and Lemma 3.15. □

The above lemma implies that each column of $\mathsf{Gram}(a)$ is a rotation (by P^i) of its first column vector $\mathsf{vec}(\overline{a}a)$:

Corollary 3.22. *For any $a \in \mathfrak{R}$, we have $\mathsf{mat}^{-1}(\mathsf{Gram}(a)) = \mathsf{mat}^{-1}(\mathsf{mat}(\overline{a}a)) = \mathsf{vec}(\overline{a}a)$.*

4 OUR ALGORITHM FOR GRAM ROOT DECOMPOSITION OVER THE RING

In this section, we present an algorithm for Gram root decomposition over the ring $\mathfrak{R}$.

We present our algorithm for Gram root decomposition over the ring $\mathfrak{R}$ in Algorithm 1. The inputs of the algorithm are "short" polynomials $e_1, \dots, e_m \in \mathfrak{R}$ s.t. $\|e_i\| \leq B \in \mathbb{N}$ for all $i \in [m]$. (Note that we explained our algorithm with $m = 1$ in the abstract and introduction section of this paper for simplicity.) Then, the algorithm outputs $\zeta = (\zeta_1, \dots, \zeta_l)^\intercal \in \mathfrak{R}^l$ s.t. $\sum_{i=1}^{l} \mathbf{G}_{\zeta_i} + \sum_{i=1}^{m} \mathbf{G}_{e_i} = mnB^2\mathbf{I}$, where $\mathbf{G}_{\zeta_i} := \mathsf{Gram}(\zeta_i)$ and $\mathbf{G}_{e_i} := \mathsf{Gram}(e_i)$. In other words, the goal of the algorithm is to "diagonalize" the sum of the coefficient Gram matrices $\sum_{i=1}^{m} \mathbf{G}_{e_i}$. Furthermore, the output polynomials $\zeta_1, \dots, \zeta_l$ are short ($\|\zeta_i\| \leq \sqrt{2mB}$), and the lower-bound of the minimum eigenvalue of $\mathbf{G}_{\zeta_i}$ is given ($\sigma_{\min}(\mathbf{Z}_i) \geq \frac{2}{n}$). These conditions on the output are necessary for the application we present in Section 5.

We prove the correctness of Algorithm 1 in Section 4.1. We then show that the outputs of Algorithm 1 satisfies the bounds ($\|\zeta_i\| \leq \sqrt{2mB}$ and $\sigma_{\min}(\mathsf{mat}(\zeta_i)) \geq \frac{2}{n}$) in Section 4.2.

4.1 Correctness

We show that Algorithm 1 works correctly:

Theorem 4.1. *The output $\zeta_1, \dots, \zeta_l \in \mathfrak{R}$ of Algorithm 1 satisfies $\sum_{i=1}^{l} \mathbf{G}_{\zeta_i} = \mathbf{G}$ and $l < \frac{5}{2}n$.*

Proof. The first part (Algorithms 1 to 1) of the algorithm decomposes the non-diagonal elements of

$$\mathbf{G} := mnB^2\mathbf{I} - \textstyle\sum_{i=1}^{m} \mathbf{G}_{e_i},$$

i.e., $\overline{\mathbf{G}} := \sum_{i=1}^{m} \mathbf{G}_{e_i}$. Define $\overline{\sigma} := (\overline{\sigma_0}, \dots, \overline{\sigma_{n-1}})^\intercal := \mathsf{mat}^{-1}(\overline{\mathbf{G}})$; Then we have $\overline{\sigma} = \sum_{i=1}^{m} \mathsf{mat}^{-1}(\mathbf{G}_{e_i}) = \sum_{i=1}^{m} \mathsf{vec}(\overline{e_i}e_i)$ via Corollary 3.22. On Algorithm 1, we first decompose $|\overline{\sigma_i}|$ by four non-negative integer squares $c_1^2, \dots, c_4^2$. Such integer squares exist for any natural numbers according to Lagrange's four-square theorem, and we efficiently calculate them via the Rabin–Shallit (RS) algorithm in Theorem 4.2. For $z^{(j)} := (c_j - \mathrm{sgn}(\overline{\sigma_i})c_j \cdot X^i) \cdot X^r \in \mathfrak{R}$ on Algorithm 1, let $\tau^{(j)} := (\tau_0^{(j)}, \dots, \tau_{n-1}^{(j)}) := \mathsf{mat}^{-1}(\mathsf{Gram}(z^{(j)}))$. Then, by Lemma 4.4, we have:

$$\begin{cases} \tau_0^{(j)} & = 2c_j^2 \\ \tau_i^{(j)} & = -\mathrm{sgn}(\overline{\sigma_i})c_j^2 \\ \tau_{n-i}^{(j)} & = \mathrm{sgn}(\overline{\sigma_i})c_j^2 \\ \tau_k^{(j)} & = 0 \quad (i \notin \{0, i, n-i\}) \end{cases}$$

Hence, we have:

$$\begin{cases} \sum_{j=1}^{4} \tau_0^{(j)} & = 2\sum_{j=1}^{4} c_j^2 = 2|\overline{\sigma_i}| \\ \sum_{j=1}^{4} \tau_i^{(j)} & = -\mathrm{sgn}(\overline{\sigma_i}) \sum_{j=1}^{4} c_j^2 = -\overline{\sigma_i} \\ \sum_{j=1}^{4} \tau_{n-i}^{(j)} & = \mathrm{sgn}(\overline{\sigma_i}) \sum_{j=1}^{4} c_j^2 = \overline{\sigma_i} \end{cases}$$

Therefore, at Algorithm 1, $\mathsf{mat}^{-1}(\sum_{\zeta \in \mathcal{S}_1} \mathsf{Gram}(\zeta)) = (\sum_{i=1}^{\frac{n}{2}-1} 2|\overline{\sigma_i}|, -\overline{\sigma_1}, \dots, -\overline{\sigma_{n-1}})$; thus, we have

$$\begin{aligned} \mathbf{G} - \textstyle\sum_{\zeta \in \mathcal{S}_1} \mathsf{Gram}(\zeta) &= mnB^2\mathbf{I} - (\overline{\mathbf{G}} + \textstyle\sum_{\zeta \in \mathcal{S}_1} \mathsf{Gram}(\zeta)) \\ &= mnB^2\mathbf{I} - \gamma\mathbf{I} = \beta\mathbf{I}, \end{aligned}$$

where $\gamma := \overline{\sigma_0} + \sum_{i=1}^{\frac{n}{2}-1} 2|\overline{\sigma_i}|$ as defined on Algorithm 1. Note that $|\overline{\sigma_i}| \leq \overline{\sigma_0} = \sum_{i=1}^{m} \|e_i\|^2 \leq mB^2$ holds by Lemma 4.3; thus, $\gamma \leq (n-1)\overline{\sigma_0} \leq m(n-1)B^2$. Hence, we have $mB^2 \leq \beta$.

The second part (Algorithms 1 to 1) of the algorithm decomposes $\beta\mathbf{I}$. The purpose of Algorithms 1 to 1 is to decompose $\beta\mathbf{I}$ with "short" polynomials: This is needed only to satisfy $\|\zeta_i\| \leq \sqrt{2mB}$. For the monomial $z := \sqrt{2mB} \cdot X^r$ on Algorithm 1, $\mathsf{Gram}(z) = 2mB^2\mathbf{I}$ holds by Lemma 4.4. Thus, at Algorithm 1, we have $\sum_{\zeta \in \mathcal{S}_1} \mathsf{Gram}(\zeta) = l' \cdot 2mB^2\mathbf{I}$. The rest of the algorithm is to decompose $(\beta - l' \cdot 2mB^2)\mathbf{I} = \delta\mathbf{I}$. For the monomial $z^{(j)} := c_j \cdot X^r$ on Algorithm 1, Algorithm 1: Gram root decomposition over the ring.

```
Input  : $e_1,\dots,e_m \in \mathfrak{R}$ s.t. $\|e_i\| \le B$ for all $i \in [m]$
Output : $\zeta_1,\dots,\zeta_l \in \mathfrak{R}$ s.t. $\sum_{i=1}^{l} \mathbf{G}_{\zeta_i} = \mathbf{G} := mnB^2\mathbf{I} - \sum_{i=1}^{m} \mathbf{G}_{e_i} \in \mathbb{Z}^{n\times n}$, $\|\zeta_i\| \le \sqrt{2m}B$ and
         $\sigma_{\min}(\mathbf{Z}_i) \ge \frac{2}{n}$, where $\mathbf{Z}_i := \mathsf{mat}(\zeta_i)$ $\mathbf{G}_{\zeta_i} := \mathsf{Gram}(\zeta_i)$ and $\mathbf{G}_{e_i} := \mathsf{Gram}(e_i)$ for any $i$.
$\mathcal{S}_1 := \emptyset$, $\mathcal{S}_2 := \emptyset$  // Sets to store $\zeta_1,\dots,\zeta_l$
Decompose non-diagonal elements of $\mathbf{G}$:
Define $\overline{\mathbf{G}} := \sum_{i=1}^{m} \mathbf{G}_{e_i}$ and $\overline{\sigma} := (\overline{\sigma_0},\dots,\overline{\sigma_{n-1}})^\intercal := \mathsf{mat}^{-1}(\overline{\mathbf{G}})$. (c.f., Definition 3.12)
  // $|\overline{\sigma_i}| \le \overline{\sigma_0} = \sum_{i=1}^{m}\|e_i\|^2 \le mB^2$ by Lemma 4.3. $\overline{\sigma_i} = -\overline{\sigma_{n-i}}$ for $i \in [1,\frac{n}{2}-1]$, $\overline{\sigma_{\frac{n}{2}+1}} = 0$ by Lemma 3.13
for $i = 1$ to $\frac{n}{2}-1$ do
    Find $c_1,\dots,c_4 \in \mathbb{N}$ s.t. $\sum_{j=1}^{4} c_j^2 = |\overline{\sigma_i}|$ with RS algorithm (Theorem 4.2)
    for $j = 1$ to 4 do
        $z^{(j)} := (c_j - \mathrm{sgn}(\overline{\sigma_i})c_j \cdot X^i)\cdot X^r \in \mathfrak{R}$ for $r \xleftarrow{\$} \mathbb{Z}_n$,     // $\|z^{(j)}\| = \sqrt{2c_j^2} \le \sqrt{2|\overline{\sigma_i}|} \le \sqrt{2m}B$
        Update $\mathcal{S}_1 := \mathcal{S}_1 \cup \{z^{(j)}\}$     // $\sigma_{\min}(\mathsf{mat}(z^{(j)})) \ge \frac{2c_j}{n} \ge \frac{2}{n}$ by Lemma 4.8
    end
     // $\mathsf{mat}^{-1}(\sum_{j=1}^{4}\mathsf{Gram}(z^{(j)})) = (2|\overline{\sigma}_i|,0,\dots,0,-\overline{\sigma}_i,\dots)^\intercal$ by Lemma 4.4
end
$\gamma := \overline{\sigma_0} + \sum_{i=1}^{\frac{n}{2}-1} 2|\overline{\sigma_i}|$     // $\le (n-1)\overline{\sigma_0} \le (n-1)mB^2$ by Lemma 4.3
Decompose diagonal elements of $\mathbf{G}$:
$\beta := mnB^2 - \gamma \in [mB^2, mnB^2)$     // $\mathbf{G} - \sum_{\zeta\in\mathcal{S}_1}\mathsf{Gram}(\zeta) = mnB^2\mathbf{I} - (\overline{\mathbf{G}} + \sum_{\zeta\in\mathcal{S}_1}\mathsf{Gram}(\zeta)) = mnB^2\mathbf{I} - \gamma\mathbf{I} = \beta\mathbf{I}$
$l' := \lfloor \beta/2mB^2 \rfloor$   $(< \frac{n}{2})$
for $i = 1$ to $l'$ do
    $z := \sqrt{2m}B \cdot X^r \in \mathfrak{R}$ for $r \xleftarrow{\$} \mathbb{Z}_n$     // $\mathsf{Gram}(z) = 2mB^2\mathbf{I}$ by Lemma 4.4
    Update $\mathcal{S}_2 := \mathcal{S}_2 \cup \{z\}$     // $\sigma_{\min}(\mathsf{mat}(z)) = \sqrt{\lambda_{\min}(\mathbf{G}_z)} = \sqrt{2m}B > 1 > \frac{2}{n}$, $\|z\| = \sqrt{2m}B$
end
$\delta := \beta - l' \cdot 2mB^2 \in [0, 2mB^2)$
Find $c_1,\dots,c_4 \in \mathbb{N}$ s.t. $\sum_{j=1}^{4} c_j^2 = \delta$ with RS algorithm (Theorem 4.2)
for $j = 1$ to 4 do
    $z^{(j)} := c_j \cdot X^r \in \mathfrak{R}$ for $r \xleftarrow{\$} \mathbb{Z}_n$     // $\|z^{(j)}\| = c_j \le \sqrt{\delta} < \sqrt{2m}B$
    Update $\mathcal{S}_2 := \mathcal{S}_2 \cup \{z^{(j)}\}$
end
return $\mathcal{S} := \mathcal{S}_1 \cup \mathcal{S}_2$     // $\sum_{\zeta\in\mathcal{S}_2}\mathsf{Gram}(\zeta) = \beta\mathbf{I}$, $\mathbf{G} = \sum_{\zeta\in\mathcal{S}}\mathsf{Gram}(\zeta)$, $l := |\mathcal{S}| = 4(\frac{n}{2}-1) + l' + 4 < \frac{5}{2}n$
```

$\mathsf{Gram}(z^{(j)}) = c_j^2\mathbf{I}$ holds by Lemma 4.4. Thus we have $\sum_{j=1}^{4}\mathsf{Gram}(z^{(j)}) = \sum_{j=1}^{4} c_j^2\mathbf{I} = \delta\mathbf{I}$. Hence, we obtain

$$\sum_{\zeta\in\mathcal{S}_2}\mathsf{Gram}(\zeta) = \beta\mathbf{I}$$

at Algorithm 1. Therefore, the output $\mathcal{S}$ of the algorithm satisfies $\sum_{\zeta\in\mathcal{S}}\mathsf{Gram}(\zeta) = \mathbf{G}$. We also have $l := |\mathcal{S}| = 4(\frac{n}{2}-1) + l' + 4 < \frac{5}{2}n$. □

We complete the above proof by describing the deferred facts; Theorem 4.2, Lemma 4.3, and Lemma 4.4:

Theorem 4.2 (Rabin–Shallit (RS) algorithm (Rabin and Shallit, 1986)). *For any $N \in \mathbb{N}$, there is a randomized algorithm for finding*

$$a,b,c,d \in \mathbb{N} \text{ s.t. } a^2+b^2+c^2+d^2 = N$$

within $O(\log^2 N \log\log N)$ operations on average.

Lemma 4.3 (Bound on $|\sigma_i|$). *Let $a \in \mathfrak{R}$, $\mathbf{a} := \mathsf{vec}(a)$, $\mathbf{G}_a := \mathsf{Gram}(a)$ and $(\sigma_0,\dots,\sigma_{n-1}) := \mathsf{mat}^{-1}(\mathbf{G}_a)$. Then, $|\sigma_i| \le \sigma_0 = \|\mathbf{a}\|^2$ holds for any i.*

Proof. By Fact 3.10, we have $\sigma_i = \mathbf{a}^\intercal\mathbf{P}^{-i}\mathbf{a}$ for any $i \ne 0$. Then, by the Cauchy–Schwarz inequality, $|\sigma_i| = |\mathbf{a}^\intercal\mathbf{P}^{-i}\mathbf{a}| \le \|\mathbf{a}\|\|\mathbf{P}^{-i}\mathbf{a}\| = \|\mathbf{a}\|^2$ holds. □

Lemma 4.4 (Coefficient Gram matrices of binomials and monomials). *Let $a \in \mathfrak{R}$ be a binomial: $a = X^r \cdot (a_0 + a_i X^i)$ for $i \in \mathbb{N}$ and $r \in \mathbb{Z}$. Let $\mathbf{a} := \mathsf{vec}(a)$, $\mathbf{G}_a := \mathsf{Gram}(a)$ and*

$$(\sigma_0,\dots,\sigma_{n-1}) := \mathsf{mat}^{-1}(\mathbf{G}_a).$$

Then, we have:

$$\begin{cases} \sigma_0 &= \|\mathbf{a}\|^2 = a_0^2 + a_i^2 \\ \sigma_i &= a_0 a_i, \quad \sigma_{n-i} = -a_0 a_i \\ \sigma_k &= 0 \quad (k \notin \{0, i, n-i\}) \end{cases}$$

In particular, for monomial $a := a_0 X^r \in \mathfrak{R}$ for $r \in \mathbb{Z}$, we have $\mathbf{G}_a = a_0^2 \mathbf{I}$, i.e.,

$$\begin{cases} \sigma_0 &= a_0^2 \\ \sigma_i &= 0 \quad (i \neq 0) \end{cases}$$

Proof. Follows from Fact 3.2 and Fact 3.10. □

4.2 Bounds on the Outputs

We first prove that the outputs of the algorithm are short polynomials:

Theorem 4.5. *The output $\zeta = (\zeta_1, \ldots, \zeta_l)^\intercal \in \mathfrak{R}^l$ of Algorithm 1 satisfies $\|\zeta_i\| \leq \sqrt{2m}B$ for any $i \in [l]$.*

Proof. The binomial $z^{(j)} := (c_j - \mathrm{sgn}(\overline{\sigma_i}) c_j \cdot X^i) \cdot X^r$ on Algorithm 1 satisfies

$$\|z^{(j)}\| = \sqrt{2c_j^2} \leq \sqrt{2|\overline{\sigma_i}|} \leq \sqrt{2m}B$$

by Lemma 3.13 and Lemma 4.3. The monomial $z := \sqrt{2m}B \cdot X^r \in \mathfrak{R}$ on Algorithm 1 satisfies $\|z\| = \sqrt{2m}B$. Finally, $z^{(j)} := c_j \cdot X^r \in \mathfrak{R}$ on Algorithm 1 also satisfies $\|z^{(j)}\| = c_j \leq \sqrt{\delta} < \sqrt{2m}B$. □

Finally, we show that the minimum singular value of the coefficient matrices of the outputs are lower-bounded by $\frac{2}{n}$:

Theorem 4.6. *The output $\zeta = (\zeta_1, \ldots, \zeta_l)^\intercal \in \mathfrak{R}^l$ of Algorithm 1 satisfies $\sigma_{\min}(\mathsf{mat}(\zeta_i)) \geq \frac{2}{n}$ for any i.*

Proof. The binomial $z^{(j)} := (c_j - \mathrm{sgn}(\overline{\sigma_i}) c_j \cdot X^i) \cdot X^r$ on Algorithm 1 satisfies $\sigma_{\min}(\mathsf{mat}(z^{(j)})) \geq \frac{2c_j}{n} \geq \frac{2}{n}$ by Lemma 4.8.

On Algorithm 1, the monomial $z := \sqrt{2m}B \cdot X^r$ satisfies $\sigma_{\min}(\mathsf{mat}(z)) = \sqrt{\lambda_{\min}(\mathbf{G}_z)} = \sqrt{2m}B > 1 > \frac{2}{n}$. Furthermore, $z^{(j)} := c_j \cdot X^r$ on Algorithm 1 also satisfies $\sigma_{\min}(\mathsf{mat}(z^{(j)})) \geq c_j \geq 1 \geq \frac{2}{n}$. □

We complete the above proof by presenting a deferred core lemma: Lemma 4.8. We first show that the coefficient matrix of the "inverse" polynomial is the inverse of the coefficient matrix:

Fact 4.7 (Inverse of coefficient matrix). *For any $a \in \mathfrak{R}$, there exists $b \in \mathbb{R}[X]/(X^n+1)$ such that $a \cdot b = 1$. Furthermore, for $\mathbf{A} := \mathsf{mat}(a)$, we have $\mathbf{A}^{-1} = \mathbf{B} = \mathsf{mat}(b)$. (Thus, such b is sufficient to derive $\mathbf{A}^{-1}$).*

Proof. Let $\mathbf{A} := \mathsf{mat}(A)$ and define

$$\mathbf{b} := \mathsf{vec}(b) := \mathbf{A}^{-1}(1, 0, \ldots, 0)^\intercal.$$

Then, by Lemma 3.15, we have

$$\mathsf{vec}(a \cdot b) = \mathbf{Ab} = (1, 0, \ldots, 0)^\intercal,$$

thus, we have $a \cdot b = 1$. Furthermore,we have $\mathsf{mat}(a \cdot b) = \mathbf{AB} = \mathbf{I}$ via Theorem 3.16; thus, $\mathbf{B} = \mathbf{A}^{-1}$. □

Then, we derive a lower bound of the singular value of the coefficient matrix of binomials:

Lemma 4.8 (Inverse of binomials). *Let $z = c \pm cX^k \in \mathfrak{R}$ for $c \in \mathbb{N}$, and let $g = \sum_{i=0}^{n-1} g_i X^i \in \mathbb{R}[X]/(X^n+1)$ be such that $z \cdot g = 1$ (i.e., the "inverse" of z). Then, we have $\|g\|_\infty = \frac{1}{2c}$. Furthermore, we have $\sigma_{\min}(\mathbf{Z}) \geq \frac{2c}{n}$, where $\mathbf{Z} := \mathsf{mat}(z)$.*

Proof. We let $z = c + cX^k$ since the proof for $z = c - cX^k$ is obtained similarly. By Fact 4.7 there exists g s.t. $z \cdot g = 1$. Let $\mathbf{z} := \mathsf{vec}(z)$ and $\mathbf{G} := \mathsf{mat}(g)$. Then, by Fact 4.7 and Lemma 3.15, we have

$$\begin{aligned} &\mathsf{vec}(z \cdot g) = \mathbf{Gz} \\ &= \begin{pmatrix} g_0 & -g_{n-1} & \cdots & -g_1 \\ g_1 & g_0 & \cdots & -g_2 \\ & \vdots & \ddots & \vdots \\ g_{n-1} & g_{n-2} & \cdots & g_0 \end{pmatrix} \begin{pmatrix} c \\ \vdots \\ c \\ \vdots \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \\ &\Leftrightarrow \begin{pmatrix} g_0 & -g_{n-k} \\ & \vdots \\ g_{k-1} & -g_{n-1} \\ g_k & g_0 \\ & \vdots \\ g_{n-1} & g_{n-k-1} \end{pmatrix} \begin{pmatrix} c \\ c \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \end{aligned}$$

Therefore, we have:

$$\begin{cases} g_0 = g_{n-k} + \frac{1}{c} \\ |g_j| = \cdots = |g_{x \cdot k + j \bmod n}| \\ \qquad \text{for } x \in \mathbb{N}, 0 \leq j \leq k-1 \end{cases}$$

We can analyze the absolute value of g_i's as follows:

- When $\gcd(k, n) = d > 1$, we have
  $$|g_{x \cdot d \bmod n}| = \frac{1}{2c} \text{ for } x \in \mathbb{N}, \text{ and}$$
  $$g_{x \cdot d + j \bmod n} = 0 \text{ for } x \in \mathbb{N}, j \in \{1, \ldots, d-1\}.$$
- When $\gcd(k, n) = 1$, we have
  $$|g_i| = \frac{1}{2c} \text{ for any } i \in \{0, n-1\}.$$

Thus, in any case, we have $\|g\|_\infty = \frac{1}{2c}$. Furthermore, we have

$$\begin{aligned} \sigma_{\min}(\mathbf{Z}) &= 1/\|\mathbf{Z}^{-1}\| = 1/\|\mathbf{G}\| \\ &\geq 1/\|\mathbf{G}\|_F = 1/(\sqrt{n}\|\mathbf{g}\|) \\ &\geq 1/(\sqrt{n}\sqrt{n(\tfrac{1}{2c})^2}) \geq 2c/n. \end{aligned}$$ □

5 APPLICATION: SPHERICALIZING THE DISCRETE GAUSSIAN OVER THE RING

We apply our Gram root decomposition algorithm (Algorithm 1) to sphericalize the discrete Gaussian over the ring: Let $r_0,\dots,r_{m+l} \overset{\text{iid}}{\sim} \mathfrak{R}(\mathcal{D}_{\mathbb{Z}^n,s})$ (Definition 3.8), i.e., polynomials with coefficients of the spherical discrete Gaussian. For given $e_1,\dots,e_m \in \mathfrak{R}$, we analyze the distribution of $(r_0+\sum_{i=1}^m r_i e_i)$ in Lemma 5.5. Furthermore, let $\zeta_1,\dots,\zeta_l$ be the outputs of Algorithm 1, then we show that the coefficients of $(r_0 e+\sum_{i=1}^m r_i e_i+\sum_{i=1}^l r_{m+i}\zeta_i)$ follow the spherical discrete Gaussian distribution in Theorem 5.6.

5.1 Building Blocks

The goal of this subsection is to present Lemma 5.4, which concerns the convolution of the discrete Gaussian. First, we describe the required basic facts about the singular values of the Gram matrices:

Fact 5.1. *For any $\mathbf{G} \succ 0$, $\sqrt{\mathbf{G}}^{-1} = (\sqrt{\mathbf{G}^{-1}})^\top$. Thus, we have:*

$$\sigma_{\max}(\sqrt{\mathbf{G}}^{-1}) = \sigma_{\max}(\sqrt{\mathbf{G}^{-1}})$$
$$\sigma_{\min}(\sqrt{\mathbf{G}}^{-1}) = \sigma_{\min}(\sqrt{\mathbf{G}^{-1}})$$

Proof. Let $\mathbf{S} := \sqrt{\mathbf{G}}$, then $\mathbf{G} = \mathbf{S}\mathbf{S}^\top$. Thus, $\mathbf{G}^{-1} = \mathbf{S}^{-\top}\mathbf{S}^{-1} = (\mathbf{S}^{-\top})(\mathbf{S}^{-\top})^\top$: we have $\mathbf{S}^{-\top} = \sqrt{\mathbf{G}^{-1}}$. Hence, we have

$$\sigma_{\max}(\sqrt{\mathbf{G}}^{-1}) = \|\sqrt{\mathbf{G}}^{-1}\| = \|\sqrt{\mathbf{G}^{-1}}\| = \sigma_{\max}(\sqrt{\mathbf{G}^{-1}}).$$

Thus, we also have

$$\sigma_{\min}(\sqrt{\mathbf{G}}^{-1}) = 1/\sigma_{\max}(\sqrt{\mathbf{G}}^{-1}) = 1/\sigma_{\max}(\sqrt{\mathbf{G}^{-1}}) = \sigma_{\min}(\sqrt{\mathbf{G}^{-1}}).$$ □

Lemma 5.2 ((Golub and Van Loan, 1996, Theorem 8.1.5)). *If $\mathbf{A},\mathbf{B} \in \mathbb{R}^{n\times n}$ are symmetric matrices, then for any $i \in [n]$,*

$$\lambda_i(\mathbf{A}) + \lambda_{\min}(\mathbf{B}) \le \lambda_i(\mathbf{A}+\mathbf{B}) \le \lambda_i(\mathbf{A}) + \lambda_{\max}(\mathbf{B})$$

Fact 5.3. *For any $\mathbf{G}_1,\mathbf{G}_2 \succ 0$, we have:*

$$\sigma_{\max}(\sqrt{\mathbf{G}_1+\mathbf{G}_2}) \le \sqrt{\sigma^2_{\max}(\sqrt{\mathbf{G}_1}) + \sigma^2_{\max}(\sqrt{\mathbf{G}_2})} \quad (12)$$

$$\sigma_{\min}(\sqrt{\mathbf{G}_1+\mathbf{G}_2}) \ge \sqrt{\sigma^2_{\min}(\sqrt{\mathbf{G}_1}) + \sigma^2_{\min}(\sqrt{\mathbf{G}_2})} \ge \sqrt{2}\min\{\sigma_{\min}(\sqrt{\mathbf{G}_1}),\sigma_{\min}(\sqrt{\mathbf{G}_2})\} \quad (13)$$

$$\sigma_{\min}(\sqrt{(\mathbf{G}_1^{-1}+\mathbf{G}_2^{-1})^{-1}}) \ge \sqrt{(\sigma^{-2}_{\min}(\sqrt{\mathbf{G}_1}) + \sigma^{-2}_{\min}(\sqrt{\mathbf{G}_2}))^{-1}} \ge \tfrac{1}{\sqrt{2}}\min\{\sigma_{\min}(\sqrt{\mathbf{G}_1}),\sigma_{\min}(\sqrt{\mathbf{G}_2})\} \quad (14)$$

Proof. By definition of singular value and Lemma 5.2, we have

$$\sigma_{\max}(\sqrt{\mathbf{G}_1+\mathbf{G}_2}) = \sqrt{\lambda_{\max}(\mathbf{G}_1+\mathbf{G}_2)} \le \sqrt{\lambda_{\max}(\mathbf{G}_1)+\lambda_{\max}(\mathbf{G}_2)}, \text{ and}$$
$$\sigma_{\min}(\sqrt{\mathbf{G}_1+\mathbf{G}_2}) = \sqrt{\lambda_{\min}(\mathbf{G}_1+\mathbf{G}_2)} \ge \sqrt{\lambda_{\min}(\mathbf{G}_1)+\lambda_{\min}(\mathbf{G}_2)}.$$

Thus, we obtain Eq. (12) and Eq. (13). By Fact 5.1 and Eq. (12), we obtain (14) as follows:

$$\begin{aligned}\sigma_{\min}(\sqrt{(\mathbf{G}_1^{-1}+\mathbf{G}_2^{-1})^{-1}}) &= (\sigma_{\max}(\sqrt{\mathbf{G}_1^{-1}+\mathbf{G}_2^{-1}}))^{-1}\\ &\ge (\sigma^2_{\max}(\sqrt{\mathbf{G}_1^{-1}}) + \sigma^2_{\max}(\sqrt{\mathbf{G}_2^{-1}}))^{-1/2}\\ &= (\sigma^{-2}_{\min}(\sqrt{\mathbf{G}_1}) + \sigma^{-2}_{\min}(\sqrt{\mathbf{G}_2}))^{1/2}\end{aligned}$$ □

Then, we prove Lemma 5.4, which is a generalization of Corollary 2.8:

Lemma 5.4 (Generalization of Corollary 2.8). *Let $\mathbf{G}_0,\dots,\mathbf{G}_m \in \mathbb{R}^{n\times n}$ be positive definite matrices. Let $\mathcal{L}_1(\mathbf{B}_1),\dots,\mathcal{L}_m(\mathbf{B}_m) \subseteq \mathbb{Z}^n$ be full-rank integer lattices with (nonsingular) basis $\mathbf{B}_1,\dots,\mathbf{B}_m$.*

Let $\sigma^*_{\min} := \min_{i\in\{0,\dots,m\}}\sigma_{\min}(\sqrt{\mathbf{G}_i})$ and $B^* := \max_{i\in\{1,\dots,m\}}\|\mathbf{B}_i\|_{\text{len}}$. Assume that $\sigma^*_{\min} \ge \sqrt{2}B^*\eta_\varepsilon(\mathbb{Z}^n)$. Then, we have

$$\textstyle\sum_{i=1}^m D_{\mathcal{L}_i,\sqrt{\mathbf{G}_i}} + D_{\mathbb{Z}^n,\sqrt{\mathbf{G}_0}} \approx_{\mathsf{s}} D_{\mathbb{Z}^n,\sqrt{\sum_{i=1}^m \mathbf{G}_i}}.$$

Proof. We first show

$$D_{\mathcal{L}_1,\sqrt{\mathbf{G}_1}} + D_{\mathbb{Z}^n,\sqrt{\mathbf{G}_0}} \approx_{\mathsf{s}} D_{\mathbb{Z}^n,\sqrt{\mathbf{G}_0+\mathbf{G}_1}} \quad (15)$$

by using Corollary 2.8. We have $\sqrt{\mathbf{G}_0} \ge \eta_\varepsilon(\mathbb{Z}^n)$ because $\sigma_{\min}(\sqrt{\mathbf{G}_0}) \ge \sigma^*_{\min} \ge \eta^+_\varepsilon(\mathbb{Z}^n)$ according to Fact 2.5 and the hypothesis. By Fact 5.3, we have $\sqrt{(\mathbf{G}_0^{-1}+\mathbf{G}_1^{-1})^{-1}} \ge \eta_\varepsilon(\mathcal{L}_1(\mathbf{B}_1))$ because we have

$$\begin{aligned}\sigma_{\min}(\sqrt{(\mathbf{G}_0^{-1}+\mathbf{G}_1^{-1})^{-1}}) &\ge \tfrac{1}{\sqrt{2}}\min\{\sigma_{\min}(\sqrt{\mathbf{G}_0}),\sigma_{\min}(\sqrt{\mathbf{G}_1})\}\\ &\ge \tfrac{1}{\sqrt{2}}\sigma^*_{\min} \ge \|\mathbf{B}_1\|_{\text{len}}\eta^+_\varepsilon(\mathbb{Z}^n)\end{aligned}$$

by the hypothesis ($\sqrt{2}\|\mathbf{B}_1\|_{\text{len}}\eta^+_\varepsilon(\mathbb{Z}^n) \le \sigma^*_{\min}$). Therefore, we obtain Eq. (15).

Next, we show

$$D_{\mathcal{L}_2,\sqrt{\mathbf{G}_2}} + D_{\mathbb{Z}^n,\sqrt{\mathbf{G}_0+\mathbf{G}_1}} \approx_{\mathsf{s}} D_{\mathbb{Z}^n,\sqrt{\mathbf{G}_0+\mathbf{G}_1+\mathbf{G}_2}}$$

via Corollary 2.8 again. By Fact 2.5 and Fact 5.3 and the hypothesis, we have $\sqrt{\mathbf{G}_0+\mathbf{G}_1} \geq \eta_\varepsilon(\mathbb{Z}^n)$ because

$$\begin{aligned}\sigma_{\min}(\sqrt{\mathbf{G}_0+\mathbf{G}_1}) &\geq \min\{\sigma_{\min}(\sqrt{\mathbf{G}_0}), \sigma_{\min}(\sqrt{\mathbf{G}_1})\} \\ &\geq \sigma^*_{\min} \geq \eta^+_\varepsilon(\mathbb{Z}^n)\end{aligned}$$

holds by the assumption $\eta^+_\varepsilon(\mathbb{Z}^n) \leq \sigma^*_{\min}$. Furthermore, we have

$$\sqrt{((\mathbf{G}_0+\mathbf{G}_1)^{-1}+\mathbf{G}_2^{-1})^{-1}} \geq \eta_\varepsilon(\mathcal{L}_1(\mathbf{B}_2))$$

because

$$\begin{aligned}&\sigma_{\min}(\sqrt{((\mathbf{G}_0+\mathbf{G}_1)^{-1}+\mathbf{G}_2^{-1})^{-1}}) \\ &\quad\geq \tfrac{1}{\sqrt{2}}\min\{\sigma_{\min}(\mathbf{G}_0+\mathbf{G}_1), \sigma_{\min}(\mathbf{G}_2)\} \\ &\quad\geq \tfrac{1}{\sqrt{2}}\min\{\sigma_{\min}(\mathbf{G}_0), \sigma_{\min}(\mathbf{G}_1), \sigma_{\min}(\mathbf{G}_2)\} \\ &\quad\geq \tfrac{1}{\sqrt{2}}\sigma^*_{\min} \geq \|\mathbf{B}_2\|_{\mathrm{len}}\eta^+_\varepsilon(\mathbb{Z}^n)\end{aligned}$$

holds by the assumption $\sqrt{2}\|\mathbf{B}_2\|_{\mathrm{len}}\eta^+_\varepsilon(\mathbb{Z}^n) \leq \sigma^*_{\min}$. Repeating the above, we obtain the claim. □

5.2 Main Theorem

We first apply Lemma 5.4 to the discrete Gaussian over the ring:

Lemma 5.5 (Applying Lemma 5.4 to the discrete Gaussian over the ring). *Let* $e_1,\ldots,e_m, \in \mathfrak{R}$ *and define* $\mathbf{E}_i := \mathsf{mat}(e_i)$ *and* $\mathbf{G}_{e_i} := \mathsf{Gram}(e_i)$. *Assume that* $\|e_i\| < B$ *and* $\sigma_{\min}(\mathbf{E}_i) \geq c$ *hold for some constant* $B, c > 0$. *Let* $r_0,\ldots,r_m \overset{\mathrm{iid}}{\sim} \mathfrak{R}(D_{\mathbb{Z}^n,s})$ *for* $s \geq \sqrt{2}c^{-1}B\eta^+_\varepsilon(\mathbb{Z}^n)$, *and define*

$$z := r_0 + \textstyle\sum_{i=1}^m r_i e_i. \tag{16}$$

Then, we have

$$\mathsf{vec}(z) \approx_{\mathsf{s}} D_{\mathbb{Z}^n,s\sqrt{\mathbf{I}_n+\sum_{i=1}^m \mathbf{G}_{e_i}}}.$$

Proof. By Lemma 3.15, we have $\mathsf{vec}(z) = \mathbf{r}_0 + \sum_{i=1}^m \mathbf{E}_i\mathbf{r}_i$, where $\mathbf{r}_i := \mathsf{vec}(r_i)$ for $i = 0,\ldots,m$. By Lemma 2.6, we obtain $\mathbf{E}_i\mathbf{r} \sim D_{\mathbf{E}_i\mathbb{Z}^n, s\mathbf{E}_i}$ for any i.

Let $\mathbf{G}_0 := s^2\mathbf{I}_n$, $\mathbf{G}_i := s^2\mathbf{G}_{e_i}$, $\mathbf{B}_i := \mathbf{Z}_i$ for all i. Then, $\mathbf{B}_i \in \mathbb{Z}^{n\times n}$ is nonsingular according to Corollary 3.18; thus $\mathcal{L}(\mathbf{B}_i) = \mathbf{B}_i\mathbb{Z}^n \subseteq \mathbb{Z}^n$ is a full-rank integer lattice for all i. Let $\sigma^*_{\min} := \min_i \sigma_{\min}(\sqrt{\mathbf{G}_i})$ and $B^* := \max_i \|\mathbf{B}_i\|_{\mathrm{len}}$, then we have

$$\sigma^*_{\min} = s \cdot \min\{1, \min_i \sigma_{\min}(\mathbf{E}_i)\} = c \cdot s,$$

$$B^* := \max_i \|\mathbf{E}_i\|_{\mathrm{len}} = \max_i \|\mathbf{e}_i\| < B.$$

Then, we obtain the claim by Lemma 5.4 since $\sigma^*_{\min} = cs \geq \sqrt{2}B^*\eta_\varepsilon(\mathbb{Z}^n)$ holds by hypothesis. □

Finally, we present the main theorem by adding $\sum_{i=1}^l r_{m+i}\zeta_i$ in Eq. (16), where $\zeta_1,\ldots\zeta_l$ are the outputs of Algorithm 1 for given $e_1,\ldots,e_m$. Then, a polynomial with *spherical* discrete Gaussian coefficients is obtained:

Theorem 5.6 (Sphericalize the discrete Gaussian over the ring). *Let* $e_1,\ldots,e_m \in \mathfrak{R}$ *and define* $\mathbf{E}_i := \mathsf{mat}(e_i)$ *and* $\mathbf{G}_{e_i} := \mathsf{Gram}(e_i)$. *Assume that* $\|e_i\| < B$ *and* $\sigma_{\min}(\mathbf{E}_i) \geq c$ *hold for some constant* $B, c > 0$.

Given $e_1,\ldots,e_m$ *as the inputs, let* $\zeta_1,\ldots,\zeta_l$ *be the outputs of Algorithm 1. Let* $r_0,\ldots,r_{m+l} \overset{\mathrm{iid}}{\sim} \mathfrak{R}(D_{\mathbb{Z}^n,s})$ *for* $s \geq 2\sqrt{m}B\max\{c^{-1}, \frac{n}{2}\}\eta^+_\varepsilon(\mathbb{Z}^n)$, *and define*

$$z := r_0 + \textstyle\sum_{i=1}^m r_i e_i + \sum_{i=1}^l r_{m+i}\zeta_i.$$

Then, we have

$$\mathsf{vec}(z) \approx_{\mathsf{s}} D_{\mathbb{Z}^n,s\sqrt{mnB^2+1}}.$$

Proof. The outputs $\zeta_1,\ldots,\zeta_l$ of Algorithm 1 satisfy $\|\zeta_i\| \leq \sqrt{2mB}$ and $\sigma_{\min}(\mathsf{mat}(\zeta_i)) \geq \frac{2}{n}$ for any $i \in [l]$ by Theorem 4.5 and Theorem 4.6, respectively. Hence, by Lemma 5.5, we have

$$\mathsf{vec}(z) \approx_{\mathsf{s}} D_{\mathbb{Z}^n,s\sqrt{\mathbf{I}_n+\sum_{i=1}^m \mathbf{G}_{e_i}+\sum_{i=1}^l \mathbf{G}_{\zeta_i}}}$$

since $s \geq 2\sqrt{m}B\max\{c^{-1}, \frac{n}{2}\}\eta^+_\varepsilon(\mathbb{Z}^n)$ by hypothesis.

Furthermore, the outputs $\zeta_1,\ldots,\zeta_l$ of Algorithm 1 satisfy $\sum_{i=1}^l \mathbf{G}_{\zeta_i} = mnB^2\mathbf{I} - \sum_{i=1}^m \mathbf{G}_{e_i}$ via Theorem 4.1. Thus, we obtain the claim. □

6 CONCLUSION AND FUTURE WORK

Many advanced lattice-based cryptosystems such as identity-based encryption and functional encryption require efficient and secure algorithms to sample discrete Gaussian. The integral Gram root decomposition of (Ducas et al., 2020) was developed in the context of the discrete Gaussian sampling algorithm.

In this work we proposed an algorithm for Gram root decomposition over the polynomial ring (Algorithm 1). While the objective of this algorithm is similar to the (ring version of) integral Gram root decomposition of (Ducas et al., 2020), our algorithm ensures the bounds of the norm of the output polynomial ζ_i (Theorem 4.5) and the minimum eigenvalue of the coefficient Gram matrix of ζ_i (Theorem 4.6). By utilizing the bounds, we showed how to sphericalize discrete Gaussian over the ring (Theorem 5.6).

Our further application would be an efficient and secure discrete Gaussian sampling algorithm for ring setting for advanced lattice-based cryptosystems, which we leave for future work.

REFERENCES

Aggarwal, D. and Regev, O. (2016). A note on discrete Gaussian combinations of lattice vectors. *Chicago Journal of Theoretical Computer Science*, (7).

Agrawal, S., Boneh, D., and Boyen, X. (2010). Efficient lattice (H)IBE in the standard model. In Gilbert, H., editor, *EUROCRYPT 2010*, pages 553–572. Springer.

Agrawal, S., Freeman, D. M., and Vaikuntanathan, V. (2011). Functional encryption for inner product predicates from learning with errors. In Lee, D. H. and Wang, X., editors, *ASIACRYPT 2011*, pages 21–40. Springer.

Agrawal, S., Gentry, C., Halevi, S., and Sahai, A. (2013). Discrete Gaussian leftover hash lemma over infinite domains. In Sako, K. and Sarkar, P., editors, *ASIACRYPT 2013*, pages 97–116. Springer.

Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., and Smith-Tone, D. (2022). NIST IR 8413-upd1: Status report on the third round of the NIST post-quantum cryptography standardization process.

Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., Seiler, G., and Stehlé, D. (2018). CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM. In *Euro S&P 2018*, pages 353–367.

Brakerski, Z., Gentry, C., and Vaikuntanathan, V. (2011). Fully homomorphic encryption without bootstrapping. ePrint 2011/277. https://eprint.iacr.org/2011/277.

Brakerski, Z., Langlois, A., Peikert, C., Regev, O., and Stehlé, D. (2013). Classical hardness of learning with errors. In *STOC '13*, page 575–584. ACM.

Ducas, L., Galbraith, S., Prest, T., and Yu, Y. (2020). Integral matrix Gram root and lattice Gaussian sampling without floats. In Canteaut, A. and Ishai, Y., editors, *EUROCRYPT 2020*, pages 608–637. Springer.

Fouque, P.-A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T., Ricosset, T., Seiler, G., Whyte, W., and Zhang, Z. (2020). Falcon: Fast-fourier lattice-based compact signatures over NTRU – specifications v1.2. 2020. Technical Report, NIST.

Genise, N. and Micciancio, D. (2018). Faster Gaussian sampling for trapdoor lattices with arbitrary modulus. In Nielsen, J. B. and Rijmen, V., editors, *EUROCRYPT 2018*, pages 174–203. Springer.

Genise, N., Micciancio, D., Peikert, C., and Walter, M. (2020). Improved discrete Gaussian and subGaussian analysis for lattice cryptography. In Kiayias, A., Kohlweiss, M., Wallden, P., and Zikas, V., editors, *PKC 2020*, pages 623–651. Springer.

Gentry, C., Peikert, C., and Vaikuntanathan, V. (2008). Trapdoors for hard lattices and new cryptographic constructions. In *STOC '08*, page 197–206. ACM.

Golub, G. H. and Van Loan, C. F. (1996). *Matrix Computations (3rd Ed.).* Johns Hopkins University Press.

Hoffstein, J., Pipher, J., and Silverman, J. H. (1998). NTRU: A ring-based public key cryptosystem. In Buhler, J. P., editor, *ANTS 1998*, pages 267–288. Springer.

Kiltz, E., Lyubashevsky, V., and Schaffner, C. (2018). A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model. In Nielsen, J. B. and Rijmen, V., editors, *EUROCRYPT 2018*, pages 552–586. Springer.

Langlois, A. and Stehlé, D. (2015). Worst-case to average-case reductions for module lattices. *Des. Codes Cryptogr.*, 75(3):565–599.

Lyubashevsky, V., Peikert, C., and Regev, O. (2010). On ideal lattices and learning with errors over rings. In Gilbert, H., editor, *EUROCRYPT 2010*, pages 1–23. Springer.

Micciancio, D. and Peikert, C. (2012). Trapdoors for lattices: Simpler, tighter, faster, smaller. In Pointcheval, D. and Johansson, T., editors, *EUROCRYPT 2012*, pages 700–718. Springer.

Micciancio, D. and Regev, O. (2007). Worst-case to average-case reductions based on Gaussian measures. *SIAM J. Comput.*, 37(1):267–302.

Micciancio, D. and Walter, M. (2017). Gaussian sampling over the integers: Efficient, generic, constant-time. In Katz, J. and Shacham, H., editors, *CRYPTO 2017*, pages 455–485. Springer.

Nguyen, H. H. and Vu, V. H. (2016). Normal vector of a random hyperplane. *International Mathematics Research Notices*, 2018(6):1754–1778.

Okada, H., Fukushima, K., Kiyomoto, S., and Takagi, T. (2023). Spherical gaussian leftover hash lemma via the Rényi divergence. In Tibouchi, M. and Wang, X., editors, *ACNS 2023*, pages 695–724. Springer Nature Singapore.

Peikert, C. (2009). Public-key cryptosystems from the worst-case shortest vector problem: Extended abstract. In *STOC '09*, page 333–342. ACM.

Peikert, C. (2010). An efficient and parallel Gaussian sampler for lattices. In Rabin, T., editor, *CRYPTO 2010*, pages 80–97. Springer.

Rabin, M. O. and Shallit, J. O. (1986). Randomized algorithms in number theory. *Communications on Pure and Applied Mathematics*, 39(S1):S239–S256.

Regev, O. (2005). On lattices, learning with errors, random linear codes, and cryptography. In *STOC '05*, pages 84–93. ACM.

Stehlé, D., Steinfeld, R., Tanaka, K., and Xagawa, K. (2009). Efficient public key encryption based on ideal lattices. In Matsui, M., editor, *ASIACRYPT 2009*, pages 617–635. Springer.

Tao, T. (2012). Topics in random matrix theory. *Graduate Studies in Mathematics*, 132.