# ON IDEAL LATTICES, GRÖBNER BASES AND GENERALIZED HASH FUNCTIONS

MARIA FRANCIS AND AMBEDKAR DUKKIPATI

Abstract. In this paper, we draw connections between ideal lattices and multivariate polynomial rings over integers using Gröbner bases. Univariate ideal lattices are ideals in the residue class ring, $\mathbb{Z}[x]/\langle f\rangle$ (here $f$ is a monic polynomial) and cryptographic primitives have been built based on these objects. Ideal lattices in the univariate case are generalizations of cyclic lattices. We introduce the notion of multivariate cyclic lattices and show that ideal lattices are a generalization of them in the multivariate case too. Based on multivariate ideal lattices, we construct hash functions using Gröbner basis techniques. We define a worst case problem, shortest substitution problem w.r.t. an ideal in $\mathbb{Z}[x_1, \ldots, x_n]$, and use its computational hardness to establish the collision resistance of the hash functions.

## 1. Introduction

Ideals in the residue class ring, $\mathbb{Z}[x]/\langle f\rangle$ for any monic polynomial $f \in \mathbb{Z}[x]$, are integer lattices as well and hence are known as ideal lattices. This is because $\mathbb{Z}[x]/\langle f\rangle$ is isomorphic to $\mathbb{Z}^N$ (as a $\mathbb{Z}$-module) if and only if $f$ is monic. The presence of both ideal and lattice properties make ideal lattices a powerful tool in lattice based cryptography. The reason why ideal lattices are popular in lattice cryptography is because they provide a compact representation for integer lattices. In fact, ideal lattices have been used to build several cryptographic primitives that include digital signatures (Lyubashevsky & Micciancio, 2008), hash functions (Lyubashevsky & Micciancio, 2006) and identification schemes (Lyubashevsky, 2008). Unfortunately, ideal lattices have not been studied much outside the periphery of lattice cryptography.

After Ajtai (1996) built functions that on an average generated hard instances of standard lattice problems, research progressed in the direction of building cryptographic primitives based on them. The fundamental challenge to this direction of research was describing lattices as $n \times n$ integer matrices, since that meant the size of the key and the computation time of the cryptographic functions will be atleast quadratic in $n$. Micciancio (2002) introduced a class of lattices called 'cyclic lattices' to remedy this problem and built certain efficient one-way functions called generalized compact knapsack functions using them. But one way functions are of theoretical interest and Lyubashevsky & Micciancio (2006) introduced the class of ideal lattices, which not only gave a succinct representation for lattices but was also a practical tool in building cryptographic primitives. In this paper, we look at how to extend ideal lattices to the multivariate polynomial ring, $\mathbb{Z}[x_1, \ldots, x_n]$.

In algebra, extensions of solutions of problems from the one variable case to the multivariate case have led to important theories, an example being the theory of Gröbner bases (Buchberger, 1965) which is a generalization of the Euclidean polynomial division algorithm in $\Bbbk[x]$. Gröbner bases have since then become a standard tool in computational algebra and algebraic geometry. We show that in the study of multivariate ideal lattices the theory of Gröbner bases plays an important role. We give a condition for residue class polynomial rings over $\mathbb{Z}$ to have ideal lattices in terms of 'short reduced Gröbner bases' (Francis & Dukkipati, 2014). We also establish the existence of collision resistant generalized hash functions based on multivariate ideal lattices.

**Contributions.** Given an ideal $\mathfrak{a}$ in $\mathbb{Z}[x_1, \ldots, x_n]$, we study the cases for which ideals in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ are also lattices. First, we define cyclic lattices in the multivariate case. We then show that multivariate ideal lattices are a generalization of multivariate cyclic lattices. We show that ideal lattices exist only when the residue class polynomial ring over $\mathbb{Z}$ is a free $\mathbb{Z}$-module, for which we give a characterization based on short reduced Gröbner bases (Francis & Dukkipati, 2014). For the construction of many cryptographic primitives, full rank lattices are essential and we derive the condition for a multivariate ideal lattice to be full rank. We also give an example of a class of binomial ideals in $\mathbb{Z}[x_1, \ldots, x_n]$, that gives rise to full rank integer lattices. To show the existence of collision resistant hash functions, we define an expansion factor w.r.t. each variable to accommodate the growth of coefficients. We extend the smallest polynomial problem ($SPP$) for multivariate ideal lattices. An important result of this work is showing the hardness of $SPP$. In the univariate case, the hardness of $SPP$ was shown by using a known hard problem called the Shortest Conjugate Problem ($SCP$). To show the hardness of $SPP$ in the multivariate case we formulate a new problem called the Smallest Substitution Problem ($SSub$) and show that $SCP$ can be polynomially reduced to $SSub$. In the univariate case, $SCP$ is based on the isomorphism of number fields. In the multivariate case, the hardness of $SSub$ is based on determining if two functional fields are isomorphic, which is a known hard problem (Pukhlikov, 1998).

**Outline of the paper.** The rest of the paper is organized as follows. In Section 2, we look at preliminaries relating to lattices and ideal lattices. We study cyclic lattices in the multivariate case in Section 3. In Section 4, we prove that only free and finitely generated $\mathbb{Z}$-modules have ideal lattices. In Section 5, we define worst case problems for multivariate ideal lattices and show the hardness of these problems in Section 6. In Section 7, we show that the hash functions built from multivariate ideal lattices are collision resistant.

## 2. Background & Preliminaries

Let $\Bbbk$ be a field, $A$ a Noetherian commutative ring, $\mathbb{Q}$ the field of rational numbers, $\mathbb{Z}$ the ring of integers and $\mathbb{N}$ the set of positive integers including zero. Let $\mathbb{R}^m$ be the $m$-dimensional Euclidean space. A polynomial ring in an indeterminate $x$ is denoted by $A[x]$. $A[x_1, \ldots, x_n]$ denotes the multivariate polynomial ring in indeterminates

$x_1, \ldots, x_n$ over $A$. A monomial $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ is denoted by $x^\alpha$, where $\alpha \in \mathbb{Z}^n_{\geq 0}$. If an ideal $\mathfrak{a}$ in $A[x_1, \ldots, x_n]$ is generated by polynomials, $f_1, \ldots, f_s$, then we write $\mathfrak{a} = \langle f_1, \ldots, f_s \rangle$. We assume that there is a monomial order, $\prec$ on the monomials in $A[x_1, \ldots, x_n]$. With respect to this monomial order, we have the leading monomial (lm), leading coefficient (lc) and leading term (lt) of a polynomial where $\mathrm{lt}(f) = \mathrm{lc}(f)\mathrm{lm}(f)$.

The set of all integral combinations of $n$ linearly independent vectors $b_1, \ldots, b_n$ in $\mathbb{R}^m$ $(m \geq n)$ is called a lattice, which is denoted by $\mathcal{L}(b_1, \ldots, b_n)$. That is, $\mathcal{L}(b_1, \ldots, b_n) = \{\sum_{i=1}^n x_i b_i \mid x_i \in \mathbb{Z}\}$. The integers $n$ and $m$ are called the rank and dimension of the lattice, respectively. The sequence of vectors $b_1, \ldots, b_n$ is called a lattice basis. When $n = m$, we say that $\mathcal{L}$ is full rank or full dimensional. An example of $n$-dimensional lattice is the set $\mathbb{Z}^n$ of all vectors with integral coordinates. In sequel, whenever we mention lattices we mean integer lattices, lattices where the basis vectors have integer coordinates. Integer lattices are additives subgroups of $\mathbb{Z}^N$, $N \in \mathbb{N}$.

Determining the minimum distance $(\lambda_1)$, successive minima ( $\lambda_1, \ldots, \lambda_n$) and covering radius $(\rho)$ of a lattice, efficiently, are well-known hard problems. The approximate algorithms that run in polynomial time give rise to approximation factors that are exponential in the dimension of the lattice. In fact, cryptographic functions based on lattices are built under the assumption that there exists no efficient algorithm that can achieve polynomial approximation factors at most $\gamma(n) = n^{O(1)}$, at least, in the worst case. For a good exposition on lattices and lattice problems one can refer to (Micciancio & Goldwasser, 2002).

We give below a formal definition of ideal lattices in one variable.

**Definition 2.1.** Given a monic polynomial $f \in \mathbb{Z}[x]$ of degree $N$, an ideal lattice is an integer lattice $\mathcal{L} \subseteq \mathbb{Z}^N$ such that it is isomorphic, as a $\mathbb{Z}$-module, to an ideal, $\mathfrak{A}$ in $\mathbb{Z}[x]/\langle f \rangle$.

The following $\mathbb{Z}$-module homomorphism between $\mathbb{Z}[x]/\langle f \rangle$ and $\mathbb{Z}^N$, where $f$ is a monic polynomial of degree $N$, further elucidates the definition of ideal lattices.

$$\begin{aligned} \psi : \mathbb{Z}[x]/\langle f \rangle &\longrightarrow \mathbb{Z}^N \\ \sum_{i=0}^{N-1} a_i x^i + \langle f \rangle &\longmapsto (a_0, \ldots, a_{N-1}). \end{aligned}$$

Clearly, $\psi$ is a $\mathbb{Z}$-module isomorphism that implies all $\mathbb{Z}$-submodules (including ideals) in $\mathbb{Z}[x]/\langle f \rangle$ are isomorphic to $\mathbb{Z}$- submodules of $\mathbb{Z}^N$. Note that $\mathbb{Z}$-submodules of $\mathbb{Z}^N$ are subgroups of $\mathbb{Z}^N$ and hence are integer lattices. Therefore, all ideals in $\mathbb{Z}[x]/\langle f \rangle$ are ideal lattices.

Hash functions are keyed functions that take long strings as inputs and output short digests that have the following property: it is computationally hard to find two distinct inputs $x \neq y$ such that $f(x) = f(y)$, where $f$ is a hash function. Consider the residue class ring, $\mathbb{Z}_p[x]/\langle f \rangle$, where $f \in \mathbb{Z}_p[x]$ is a monic, irreducible polynomial of degree $n$ and $p$ is an integer of order approximately $n^2$. A hash function, $h$, can be designed for ideal lattices in $\mathbb{Z}_p[x]/\langle f \rangle$ by selecting $m$ random elements $a_1, \dots, a_m$ to form an ordered $m$-tuple, $(a_1, \dots, a_m)$. Let $D$ be a strategically chosen subset of $\mathbb{Z}_p[x]/\langle f \rangle$ (Lyubashevsky & Micciancio, 2006, Section 5.1). Then the hash function $h$ maps the elements of $D^m$ to $\mathbb{Z}_p[x]/\langle f \rangle$ as follows: if $b = (b_1, \dots, b_m) \in D^m$, then $h(b) = \sum_{i=1}^{m} a_i \cdot b_i$. A problem called the "Shortest Polynomial Problem" ($SPP$) equivalent to known hard problems is used to prove the collision resistance of the hash function (Lyubashevsky & Micciancio, 2006). It can be shown that if there is a polynomial time algorithm that can find a collision with non-negligible probability, then $SPP$ can be solved in polynomial time for every lattice in the the ring, $\mathbb{Z}_p[x]/\langle f \rangle$.

## 3. Multivariate Cyclic Lattices

Before we look into the multivariate case we recall the definition of cyclic lattices.

**Definition 3.1.** A lattice $\mathcal{L}$ in $\mathbb{Z}^N$ is a cyclic lattice if for all $v \in \mathcal{L}$, a cyclic shift of $v$ is also in $\mathcal{L}$.

One can easily verify the following fact.

**Lemma 3.2.** *A set $\mathcal{L}$ in $\mathbb{Z}^N$ is a cyclic lattice if $\mathcal{L}$ is an ideal in $\mathbb{Z}[x]/\langle x^N - 1 \rangle$.*

Now consider $\mathbb{Z}[x_1, \dots, x_n]/\langle {x_1}^{r_1} - 1, \cdots, {x_n}^{r_n} - 1 \rangle$, for some $r_1, \dots, r_n \in \mathbb{N}$. Let $\mathfrak{a} = \langle {x_1}^{r_1} - 1, \cdots, {x_n}^{r_n} - 1 \rangle$ and $r_1 \times r_2 \times \cdots \times r_n = N$. Then, $\mathbb{Z}[x_1, \dots, x_n]/\mathfrak{a}$ is a free $\mathbb{Z}$-module, isomorphic to $\mathbb{Z}^N$ with $\mathcal{B} = \{{x_1}^{\alpha_1} \dots {x_n}^{\alpha_n} + \mathfrak{a}, \alpha_k = 0, \dots, r_k - 1, k = 1, \dots, n\}$ as a $\mathbb{Z}$-module basis. Given an element of the residue class polynomial ring,

$$\sum_{j=1}^{N} a_{(\alpha_{1j}, \dots, \alpha_{nj})} {x_1}^{\alpha_{1j}} \dots {x_n}^{\alpha_{nj}} + \mathfrak{a},$$

where $\alpha_{kj} = 0, \dots, r_k - 1$ and $a_{(\alpha_{1j}, \dots, \alpha_{nj})} \in \mathbb{Z}$. This can be represented using a tensor, $\mathcal{A} \in \mathbb{Z}^{r_1 \times \cdots \times r_n}$ defined as $\mathcal{A}_{i_1, \dots, i_n} = a_{(i_1 - 1, \dots, i_n - 1)}$, where $A_{i_1, \dots, i_n}$ denotes $(i_1, \dots, i_n)$th element in the tensor $\mathcal{A}$.

Now consider $\mathbb{Z}^N$ and suppose $r_1, \dots, r_n \in \mathbb{N}$ such that $r_1 \times r_2 \times \cdots \times r_n = N$. Given a lattice $\mathcal{L} \subseteq \mathbb{Z}^N$, where $\mathbb{Z}^N = \mathbb{Z}^{r_1 \times \cdots \times r_n}$, it is easy to see that a one-to-one correspondence exists between a vector in $\mathcal{L}$ and a tensor in $\mathbb{Z}^{r_1 \times \cdots \times r_n}$.

Let $\mathcal{A}$ be a tensor in $\mathbb{Z}^{r_1 \times \cdots \times r_n}$. We define a $(n-1)^{\text{th}}$ order tensor for each $i = 1, \dots, n$ and denote it as $A_i(j)$, where $A_i(j) \in \mathbb{Z}^{r_1 \times r_2 \times \cdots \times r_{i-1} \times r_{i+1} \times \cdots \times r_n}$, $j = 0, \dots, r_i - 1$. We have,

$$A_i(j)_{(k_1, \dots, k_{i-1}, k_{i+1}, \dots, k_n)} = \mathcal{A}_{(k_1, \dots, k_{i-1}, j, k_{i+1}, \dots, k_n)}, \;\; j = 0, \dots, r_i - 1.$$

We construct the following ordered set of $(n-1)^{\text{th}}$ order tensors for each $i = 1, \dots, n$,

$$\mathcal{A}_i = (A_i(0), A_i(1), \cdots, A_i(r_i - 1)).$$

Using this set, we introduce the notion of multivariate cyclic shifts.

**Definition 3.3.** Let $\mathcal{L} \subseteq \mathbb{Z}^N = \mathbb{Z}^{r_1 \times \cdots \times r_n}$ be a lattice and $\mathcal{A} \in \mathbb{Z}^{r_1 \times \cdots \times r_n}$, a tensor in $\mathcal{L}$. The $i^{\text{th}}$-multivariate cyclic shift of $\mathcal{A}$, $\sigma_i(\mathcal{A})$ is a cyclic shift of elements in the ordered set $\mathcal{A}_i$.

Observe that multiplying an element in $\mathbb{Z}[x_1, \ldots, x_n]/\langle {x_1}^{r_1} - 1, \cdots, {x_n}^{r_n} - 1\rangle$ with $x_i$ results in a cyclic shift in the ordered set, $\mathcal{A}_i$, $i = 1, \ldots, n$. This is also equivalent to a cyclic permutation in the $n^{\text{th}}$ order tensor along the $i^{\text{th}}$ direction.
We now formerly define multivariate cyclic lattices.

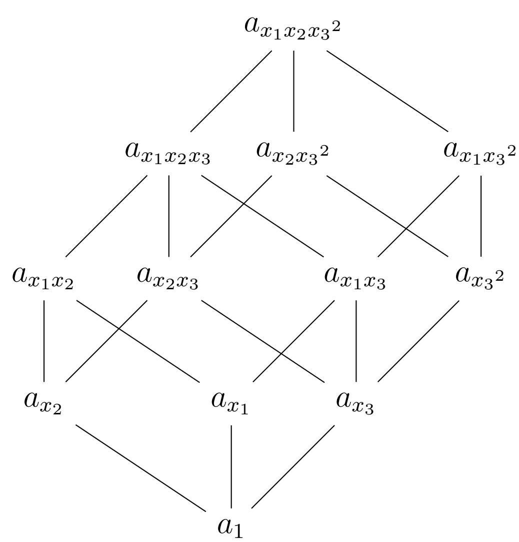
**Definition 3.4.** A lattice $\mathcal{L}$ in $\mathbb{Z}^N = \mathbb{Z}^{r_1\times\cdots\times r_n}$ is a multivariate cyclic lattice if for all $v \in \mathcal{L}$, a $i^{\text{th}}$-multivariate cyclic shift of $v$ is also in $\mathcal{L}$ for all $i = 1, \ldots, n$.

**Example 3.5.** Consider the case when $n = 3$ and we have $r_1 = 2$, $r_2 = 2$ and $r_3 = 3$. The residue class ring associated to it is $\mathbb{Z}[x_1, x_2, x_3]/\langle {x_1}^2 - 1, {x_2}^2 - 1, {x_3}^3 - 1\rangle$. It is isomorphic to the space of 3$^{\text{rd}}$ order tensors, $\mathbb{Z}^{2\times2\times3}(\cong \mathbb{Z}^{12})$. The following set of monomials form the set of coset representatives for a $\mathbb{Z}$-module basis,

$$\{1, x_1, x_2, x_3, {x_3}^2, x_1x_2, x_1x_3, x_1{x_3}^2, x_2x_3, x_2{x_3}^2, x_1x_2x_3, x_1x_2{x_3}^2\}.$$

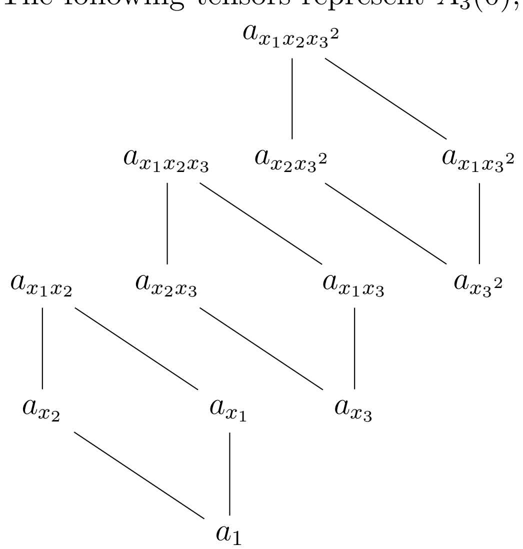
Any element in the residue class ring can be represented as a 3$^{\text{rd}}$ order tensor, $\mathcal{A} \in \mathbb{Z}^{2\times2\times3}$. Let $a_{x^\alpha}$ be the coefficient of the basis element, $x^\alpha$. We can represent $\mathcal{A}$ as follows,

$\mathcal{A} =$




.

The following tensors represent $A_3(0)$, $A_3(1)$ and $A_3(2)$ respectively.




.

$A_3(0)$, $A_3(1)$ and $A_3(2)$ represent $2^{\text{nd}}$ order tensors corresponding to $x_3 = 0$, $x_3 = 1$ and $x_3 = 2$ respectively. Similarly, $A_2(0)$ and $A_2(1)$ represent $2^{\text{nd}}$ order tensors corresponding to $x_2 = 0$ and $x_2 = 1$ and $A_1(0)$ and $A_1(1)$ represent $2^{\text{nd}}$ order tensors corresponding to $x_1 = 0$ and $x_1 = 1$. Multiplying with $x_3$ here results in a cyclic rotation of $A_3(0)$, $A_3(1)$ and $A_3(2)$.

Multiplying with a monomial ${x_1}^{\alpha_1} \cdots {x_n}^{\alpha_n}$ in the general case results in a composition of $\alpha_i$ shifts in $\mathcal{A}_i$ for each $i = 1, \ldots, n$. The commutativity of multiplication is taken care of as the shifts act on an independent set of subtensors and this makes the order of the composition of cyclic shifts irrelevant. That is, the order in which we perform the cyclic shifts between $\mathcal{A}_i$ and $\mathcal{A}_j$ does not matter for $i, j = 1, \ldots, n$.

**Proposition 3.6.** *Every ideal in*

$$\mathbb{Z}[x_1, \ldots, x_n]/\langle {x_1}^{r_1} - 1, {x_2}^{r_2} - 1, \cdots, {x_n}^{r_n} - 1\rangle$$

*is a multivariate cyclic lattice.*

## 4. Multivariate Ideal Lattices and Short Reduced Gröbner Basis

Now we give a formal definition of multivariate ideal lattices.

**Definition 4.1.** Given an ideal $\mathfrak{a} \subseteq \mathbb{Z}[x_1, \ldots, x_n]$, a multivariate ideal lattice is an integer lattice $\mathcal{L} \subseteq \mathbb{Z}^N$ that is isomorphic, as a $\mathbb{Z}$-module, to an ideal $\mathfrak{A}$ in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$.

In sequel, by ideal lattices we mean multivariate ideal lattices. The $\mathbb{Z}$-module structure of $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is crucial in locating ideal lattices in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$. In general, for a Noetherian ring $A$, one can use Gröbner basis methods to determine an $A$-module representation of $A[x_1, \ldots, x_n]/\mathfrak{a}$, where $\mathfrak{a}$ is an ideal in $A[x_1, \ldots, x_n]$ (Francis & Dukkipati, 2014). We describe this briefly below.

Consider an ideal $\mathfrak{a} \subseteq A[x_1, \ldots, x_n]$. Let $G = \{g_i : i = 1, \ldots, t\}$ be a Gröbner basis for $\mathfrak{a}$ w.r.t a monomial order, $\prec$. For each monomial, $x^\alpha$, let $J_{x^\alpha} = \{i : \text{lm}(g_i) \mid x^\alpha, g_i \in G\}$ and $I_{J_{x^\alpha}} = \langle \{\text{lc}(g_i) : i \in J_{x^\alpha}\}\rangle$. We refer to $I_{J_{x^\alpha}}$ as the leading coefficient ideal w.r.t. $G$. Let $C_{J_{x^\alpha}}$ represent a set of coset representatives of the equivalence classes in $A/I_{J_{x^\alpha}}$. Given a polynomial, $f \in A[x_1, \ldots, x_n]$, let $f = \sum_{i=1}^{m} a_i x^{\alpha_i} \bmod \langle G\rangle$, where $a_i \in A, i = 1, \ldots, m$. If $A[x_1, \ldots, x_n]/\langle G\rangle$ is a finitely generated $A$-module of size $m$, then corresponding to coset representatives, $C_{J_{x^{\alpha_1}}}, \ldots, C_{J_{x^{\alpha_m}}}$, there exists an $A$-module isomorphism,

$$\begin{aligned} \phi : A[x_1, \ldots, x_n]/\langle G\rangle &\longrightarrow A/I_{J_{x^{\alpha_1}}} \times \cdots \times A/I_{J_{x^{\alpha_m}}} \\ \sum_{i=1}^{m} a_i x^{\alpha_i} + \langle G\rangle &\longmapsto (c_1 + I_{J_{x^{\alpha_1}}}, \cdots, c_m + I_{J_{x^{\alpha_m}}}), \end{aligned} \tag{1}$$

where $c_i = a_i \bmod I_{J_{x^{\alpha_i}}}$ and $c_i \in C_{J_{x^{\alpha_i}}}$. We refer to $A/I_{J_{x^{\alpha_1}}} \times \cdots \times A/I_{J_{x^{\alpha_m}}}$ as the $A$-module representation of $A[x_1, \ldots, x_n]/\mathfrak{a}$ w.r.t. $G$ (or equivalently w.r.t. $\prec$). If $I_{J_{x^{\alpha_i}}} = \{0\}$, we have $C_{J_{x^{\alpha_i}}} = A$, for all $i = 1, \ldots, m$. This implies $A[x_1, \ldots, x_n]/\mathfrak{a} \cong A^m$, i.e. $A[x_1, \ldots, x_n]/\mathfrak{a}$ has an $A$-module basis and it is free. We say that $A[x_1, \ldots, x_n]/\mathfrak{a}$

has a free $A$-module representation w.r.t. $G$ (or equivalently w.r.t. $\prec$). When $A = \mathbb{Z}$ and $\mathbb{Z}[x_1, \dots, x_n]/\mathfrak{a} \cong \mathbb{Z}^m$, corresponding to every ideal, $\mathfrak{A}$ in $\mathbb{Z}[x_1, \dots, x_n]/\mathfrak{a}$, there exists a subgroup in $\mathbb{Z}^m$. Hence the ideals in $\mathbb{Z}[x_1, \dots, x_n]/\mathfrak{a}$ are indeed ideal lattices.

To find the various $\mathbb{Z}$-module representations of $\mathbb{Z}[x_1, \dots, x_n]/\mathfrak{a}$, one needs the notion of 'short reduced Gröbner bases' (Francis & Dukkipati, 2014). We describe this here for polynomial rings over any Noetherian, commutative ring, $A$.

**Definition 4.2.** Let $\mathfrak{a} \subseteq A[x_1, \dots, x_n]$ be an ideal. A reduced Gröbner basis $G$ of $\mathfrak{a}$ is called a short reduced Gröbner basis if for each $x^\alpha \in \mathrm{lm}(G)$, the length of the generating set of its leading coefficient ideal, $I_{J_{x^\alpha}}$ in (1), is minimal.

The reduced Gröbner basis in the above definition is as described in (Pauer, 2007). When $A = \mathbb{Z}$ in the above definition, the short reduced Gröbner basis is the reduced Gröbner basis of $\mathfrak{a}$, where the generator of the leading coefficient ideal is taken as the gcd of all generators. The short reduced Gröbner basis is unique for a particular monomial order and hence once we fix a monomial order, $A[x_1, \dots, x_n]/\mathfrak{a}$ has a unique $A$-module representation.

**Proposition 4.3.** *Let $\mathfrak{a} \subseteq A[x_1, \dots, x_n]$ be a non-zero ideal such that $A[x_1, \dots, x_n]/\mathfrak{a}$ is finitely generated. Let $G$ be a short reduced Gröbner basis for $\mathfrak{a}$ w.r.t. some monomial ordering, $\prec$. Then, $A[x_1, \dots, x_n]/\mathfrak{a}$ has a free $A$-module representation w.r.t. $\prec$ if and only if $G$ is monic.*

A monic basis is a basis where the leading coefficients of all its elements are equal to 1. We have, therefore, the following result for the case when $A = \mathbb{Z}$.

**Theorem 4.4.** *If the short reduced Gröbner basis w.r.t. some monomial ordering is monic, then every ideal in the $\mathbb{Z}$-module, $\mathbb{Z}[x_1, \dots, x_n]/\mathfrak{a}$ is an ideal lattice.*

We illustrate this by an example.

**Example 4.5.** Let $\mathfrak{a} = \langle 3x^2, 5x^2, y \rangle$ be an ideal in $\mathbb{Z}[x, y]$. The short reduced Gröbner basis for the ideal w.r.t. lex order $y \prec x$ is $G = \{x^2, y\}$. Since $G$ is monic, $\mathbb{Z}[x, y]/\mathfrak{a}$ has a free representation and hence the $\mathbb{Z}$-module is free and isomorphic to $\mathbb{Z}^2$. All ideals in $\mathbb{Z}[x, y]/\mathfrak{a}$ are ideal lattices. For example, the ideal generated by $6x + \langle x^2, y \rangle$ is isomorphic to the lattice, $\mathcal{L}([(0, 6)])$. Note that here $\mathcal{L}([(0, 6)])$ denotes the subgroup generated by $(0, 6)$ in $\mathbb{Z}^2$.

Below we show that if $\mathbb{Z}[x_1, \dots, x_n]/\mathfrak{a}$ is not a free $\mathbb{Z}$-module then it does not contain any ideal lattices.

**Proposition 4.6.** *If a finitely generated $\mathbb{Z}$-module, $\mathbb{Z}[x_1, \dots, x_n]/\mathfrak{a}$ is not free then no ideal in $\mathbb{Z}[x_1, \dots, x_n]/\mathfrak{a}$ is an integer lattice.*

*Proof.* We have the following structure theorem over a principal ideal domain (PID),

$$\mathbb{Z}[x_1, \dots, x_n]/\mathfrak{a} \cong \mathbb{Z}^l \oplus \mathbb{Z}/\langle w_1 \rangle \oplus \cdots \oplus \mathbb{Z}/\langle w_k \rangle.$$

Clearly, if there is a non zero torsion part in the above direct sum decomposition then $\mathbb{Z}[x_1, \dots, x_n]/\mathfrak{a}$ will not have a free $\mathbb{Z}$-module representation w.r.t. any Gröbner basis. Also, we assume w.l.o.g. that the free part is non zero. Let $G$ be the Gröbner basis of the ideal, $\mathfrak{a}$ w.r.t. to some monomial ordering. Consider the isomorphism in (1) w.r.t. $G$. Assume there exists an ideal, $\mathfrak{A} \subseteq \mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ such that it is an integer lattice. Let $x^{\alpha_r} + \mathfrak{a} \in \mathfrak{A}$ be an element such that the leading coefficient ideal of $x^{\alpha_r}$ in $\mathbb{Z}$, $I_{J_{x^{\alpha_r}}}$ is equal to $\{0\}$. This implies that the set of coset representatives, $C_{J_{x^{\alpha_r}}} = \mathbb{Z}$, and therefore the monomial corresponds to the free part in (1). Consider the ideal generated by $x^{\alpha_r} + \mathfrak{a}$. Since the $\mathbb{Z}$-module is not free we have $I_{J_{x^{\alpha_j}}} \neq \{0\}$ and $C_{J_{x^{\alpha_j}}} \neq \mathbb{Z}$ for some monomial $x^{\alpha_j}$ in (1). Let $c \in C_{J_{x^{\alpha_j}}}$. Since $c_i x^{\alpha_i} + \mathfrak{a} \in \mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$, $c x^{\alpha_j} x^{\alpha_r} + \mathfrak{a} \in \langle x^{\alpha_r} + \mathfrak{a} \rangle$. This implies, the ideal generated by a free element contains torsion elements. Thus the $\mathbb{Z}$-module, $\mathfrak{A}$ has torsion elements and is not isomorphic to an integer lattice, which is a contradiction. $\square$

**Corollary 4.7.** *Every ideal, $\mathfrak{a}$ in $\mathbb{Z}[x_1, \ldots, x_n]$ is an ideal lattice if and only if $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is a free and finitely generated $\mathbb{Z}$-module.*

We recall that in the definition of ideal lattices in $\mathbb{Z}[x]$ the choice of the polynomial $f$ in $\mathbb{Z}[x]/\langle f \rangle$ is restricted to monic polynomials. But in the construction of many cryptographic primitives like collision resistant hash functions $f$ is assumed to be an irreducible polynomial. This condition ensures that the ideal lattice is full rank and hence prevents easy collision attacks (Lyubashevsky & Micciancio, 2006). In the multivariate case, we derive a necessary and sufficient condition for full rank ideal lattices.

**Proposition 4.8.** *Let $\{g_1, \ldots, g_t\}$ be a monic short reduced Gröbner basis of an ideal $\mathfrak{a}$ in $\mathbb{Z}[x_1, \ldots, x_n]$ such that $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a} \cong \mathbb{Z}^N$ for some $N \in \mathbb{N}$. All ideals in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ are full rank lattices if and only if $\mathfrak{a}$ is a prime ideal.*

*Proof.* Let $\mathfrak{a} = \langle g_1, \ldots, g_t \rangle$ be a prime ideal. Consider an ideal $\mathfrak{A} = \langle f_1 + \mathfrak{a}, \ldots, f_s + \mathfrak{a} \rangle$ in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$, where $f_1, \ldots, f_s \in \mathbb{Z}[x_1, \ldots, x_n]$. Since $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a} \cong \mathbb{Z}^N$ we have a finite basis, $\mathcal{B} = \{b_1 + \mathfrak{a}, \ldots, b_N + \mathfrak{a}\}$. We have to prove that there are $N$ linearly independent vectors in $\mathfrak{A}$. Consider $f_1 b_1, \ldots, f_1 b_N$. Let $c_1 f_1 b_1 + \cdots + c_N f_1 b_N \in \langle g_1, \ldots, g_t \rangle$. This implies $f_1(c_1 b_1 + \cdots + c_N b_N) \in \langle g_1, \ldots, g_t \rangle$. Since $\langle g_1, \ldots, g_t \rangle$ is a prime ideal, either $f_1 \in \langle g_1, \ldots, g_t \rangle$ or $(c_1 b_1 + \cdots + c_N b_N) \in \langle g_1, \ldots, g_t \rangle$. But both cases cannot happen. Therefore $c_i = 0$ for all $i = 1, \ldots, N$. This implies that $f_1 b_1 + \mathfrak{a}, \ldots, f_1 b_N + \mathfrak{a}$ are linearly independent and the ideal lattice is full rank.

Conversely, assume that $\mathfrak{a}$ is not a prime ideal. Then there exists $l, h \in \mathbb{Z}[x_1, \ldots, x_n]$ such that $lh \in \langle g_1, \ldots, g_t \rangle$ but $l \notin \langle g_1, \ldots, g_t \rangle$ and $h \notin \langle g_1, \ldots, g_t \rangle$. This implies, $l = \sum_{i=1}^N c_i b_i$ and $h = \sum_{i=1}^N d_i b_i$, where $b_i + \mathfrak{a} \in \mathcal{B}$, the basis for $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ and $c_i, d_i \in \mathbb{Z}$. Consider the ideal lattice $\langle l + \mathfrak{a} \rangle$. We have $lh \in \langle g_1, \ldots, g_t \rangle$ and this implies $l \sum_{i=1}^N d_i b_i \in \langle g_1, \ldots, g_t \rangle$. But $l \notin \langle g_1, \ldots, g_t \rangle$ and $\sum_{i=1}^N d_i b_i \notin \langle g_1, \ldots, g_t \rangle$. The set $\{l b_1 + \mathfrak{a}, \ldots, l b_N + \mathfrak{a}\}$ contains linearly dependent vectors and the rank of the ideal lattice $\langle l + \mathfrak{a} \rangle$ is $\lneq N$. Therefore, if the ideal $\mathfrak{a}$ is not a prime ideal then there exist lattices in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ that are not full rank. $\square$

Determining if an ideal is prime or not is important for many practical applications. An algorithm for primality testing in polynomial rings, over any commutative, Noetherian ring, $A$ can be found in (Gianni *et al.*, 1988).

We now give an example of a class of binomial ideals that is prime and gives rise to free residue class polynomial rings. Given an integer lattice, $\mathcal{L}$, a lattice ideal, $\mathfrak{a}_{\mathcal{L}}$ in $\Bbbk[x_1,\ldots,x_n]$ is defined as the binomial ideal generated by $\{x^{v^+} - x^{v^-}\}$ where $v^+$ and $v^-$ are non-negative with disjoint support and $v^+ - v^- \in \mathcal{L}$ (Katsabekis *et al.*, 2010). Lattice ideals in polynomial rings over $\mathbb{Z}$ can be defined in the same way. In this case, the binomial ideal is generated over the polynomial ring, $\mathbb{Z}[x_1,\ldots,x_n]$. The generators of the ideal are binomials with the terms having opposite sign and the coefficients of both the terms equal to absolute value 1. One can show that the short reduced Gröbner basis of the lattice ideal is monic (Francis & Dukkipati, 2014). In this case, by Proposition 4.3, $\mathbb{Z}[x_1,\ldots,x_n]/\mathfrak{a}_{\mathcal{L}}$ is free. Hence, we have the following fact.

**Theorem 4.9.** *Every ideal in $\mathbb{Z}[x_1,\ldots,x_n]/\mathfrak{a}_{\mathcal{L}}$, where $\mathfrak{a}_{\mathcal{L}}$ is a lattice ideal, is an ideal lattice.*

The saturation of an integer lattice, $\mathcal{L} \subseteq \mathbb{Z}^m$ is a lattice, defined as

$$Sat(\mathcal{L}) = \{\alpha \in \mathbb{Z}^m \mid d\alpha \in \mathcal{L} \text{ for some } d \in \mathbb{Z}, d \neq 0\}.$$

We say that an integer lattice $\mathcal{L}$ is saturated if $\mathcal{L} = Sat(\mathcal{L})$. It can be easily shown that the lattice ideal $\mathfrak{a}_{\mathcal{L}}$ is prime if and only if $\mathcal{L}$ is saturated. Note that in the commutative algebra literature prime lattice ideals are also called toric ideals (Bigatti *et al.*, 1999). Thus, toric ideals in $\mathbb{Z}[x_1,\ldots,x_n]$ give rise to full rank integer lattices.

## 5. Hard Problems for Multivariate Ideal Lattices

5.1. **Expansion Factor.** Given $f \in \mathbb{Z}[x_1,\ldots,x_n]$, the following norms can be defined on $\mathbb{Z}[x_1,\ldots,x_n]$: the infinity norm $\|f\|_\infty$ that takes the maximum coefficient of all the terms in the polynomial and the norm w.r.t. an ideal $\mathfrak{a}$ and a monomial order $\prec$, $\|f\|_{\mathfrak{a},\prec}$ that takes the maximum coefficient of all the terms in the polynomial reduced modulo $\mathfrak{a}$ w.r.t. $\prec$.

Given a finitely generated residue class polynomial ring $\mathbb{Z}[x_1,\ldots,x_n]/\mathfrak{a}$ with a free $\mathbb{Z}$-module representation w.r.t a monomial order $\prec$, the ideal $\mathfrak{a}$ should satisfy the following properties that are essential for the security proofs of the hash function: (i) $\mathfrak{a}$ should be a prime ideal, which ensures that every ideal in $\mathbb{Z}[x_1,\ldots,x_n]/\mathfrak{a}$ is a full rank lattice, and (ii) the norm of any polynomial $f$ w.r.t. the ideal $\mathfrak{a}$ and monomial order $\prec$, $\|f\|_{\mathfrak{a},\prec}$ should not be much larger than $\|f\|_\infty$. The second property is formally captured with a parameter called the expansion factor that we define for the multivariate case below.

For a given finite set of generators, $\operatorname{maxdeg}_{x_i}(\mathfrak{a})$ denotes the maximum degree of a variable $x_i$ among the generators of the ideal $\mathfrak{a}$. We represent the maximum degree of a variable $x_i$ in a polynomial $g$ as $\operatorname{maxdeg}_{x_i}(g)$.

**Definition 5.1.** Let $\mathfrak{a} = \langle f_1,\ldots,f_s\rangle \subseteq \mathbb{Z}[x_1,\ldots,x_n]$ such that $\mathbb{Z}[x_1,\ldots,x_n]/\mathfrak{a}$ is finitely generated and has a free $\mathbb{Z}$-module representation w.r.t. $\prec$. The expansion factor $\mathcal{E}$ of $\mathfrak{a}$ is defined as

$$\mathcal{E}(\mathfrak{a}, \prec, (k_1, \dots, k_n)) = \max_{\substack{\mathrm{maxdeg}_{x_i}(g) \leq k_i (\mathrm{maxdeg}_{x_i}(\mathfrak{a})) \\ \forall i \in \{1, \dots, n\} \\ g \in \mathbb{Z}[x_1, \dots, x_n]}} \frac{\|g\|_{\mathfrak{a},\prec}}{\|g\|_\infty},$$

where $k_i \in \mathbb{N}$, $i = 1, 2, \dots, n$.

We give a result that bounds the expansion factor of ideals for which the residue class polynomial ring is finitely generated and has a free $\mathbb{Z}$-module representation.

**Theorem 5.2.** *Let $G = \{g_1, \dots, g_s\}$ be a short reduced Gröbner basis of an ideal $\mathfrak{a}$ w.r.t. a monomial order $\prec$ such that $\mathbb{Z}[x_1, \dots, x_n]/\mathfrak{a}$ is finitely generated and has a free $\mathbb{Z}$-module representation w.r.t. $\prec$ (i.e. $G$ is monic). Then for any $f \in \mathbb{Z}[x_1, \dots, x_n]$, $\|f\|_{\mathfrak{a},\prec} \leq \|f\|_\infty (2 \cdot (\|g\|_\infty)_{\max})^k$, where $(\|g\|_\infty)_{\max}$ denotes the maximum norm among the generators of the ideal and $k$ is of the order $O((\deg(f))^n (\max_{1 \leq i \leq s} \deg(g_i))^n)$.*

*Proof.* First we reduce $f$ with the generators $\{g_1, \dots, g_s\}$. Let $g_j$ be the generator such that $\mathrm{lm}(f) = x^\alpha \mathrm{lm}(g_j)$ for some $x^\alpha$. Then, $f_1 = f - \mathrm{lc}(f) x^\alpha g_j$. Since $G$ is monic, during the reduction process one needs to consider only one generator of the ideal at a time. We have,

$$\begin{aligned} \|f_1\|_\infty \leq \|f\|_\infty + \|f\|_\infty \|g_j\|_\infty &\leq 2\|f\|_\infty \|g_j\|_\infty \\ &\leq 2\|f\|_\infty (\|g\|_\infty)_{\max}. \end{aligned}$$

Next we can reduce $f_1$ by any of the generators in the Gröbner basis to get $f_2$ and continue this process. This process will terminate after $k$ steps, where $k$ is of the order $O((\deg(f))^n (\max_i \deg(g_i))^n)$ (Thieu, 2013). The exact number of iterations cannot be determined unless we know the exact structure of the ideal and the polynomial. Hence,

$$\|f\|_{\mathfrak{a},\prec} \leq \|f\|_\infty (2 \cdot (\|g\|_\infty)_{\max})^k.$$

□

5.2. **Worst Case Problems.** For any ideal $\mathfrak{A} \subseteq \mathbb{Z}[x_1, \dots, x_n]/\mathfrak{a}$ we use ${\lambda_i}^p(\mathfrak{A})$ to indicate ${\lambda_i}^p(\mathcal{L}(\mathfrak{A}))$, where $\lambda_i$ represents the $i$-th successive minima w.r.t. the $\ell_p$ norm.

**Definition 5.3.** The approximate Shortest Polynomial Problem ($SPP_\gamma(\mathfrak{A})$) is defined as follows: given an ideal $\mathfrak{A} \subseteq \mathbb{Z}[x_1, \dots, x_n]/\mathfrak{a}$, where $\mathbb{Z}[x_1, \dots, x_n]/\mathfrak{a}$ is finitely generated and has a free $\mathbb{Z}$-module representation w.r.t. $\prec$, determine a $g \in \mathfrak{A}$ such that $g \neq 0$ and $\|g\|_{\mathfrak{a},\prec} \leq \gamma {\lambda_1}^\infty(\mathfrak{A})$, where $\lambda_1$ represents the minimum distance.

We use the notation $\mathcal{L}(\mathfrak{a})$ to denote the set of all lattices associated with $\mathbb{Z}[x_1, \dots, x_n]/\mathfrak{a}$ and use $\mathfrak{a} - SPP$ when we consider $SPP$ for ideals in $\mathbb{Z}[x_1, \dots, x_n]/\mathfrak{a}$, where $\mathfrak{a}$ is as described above. In Section 6, we show how well known hard problems can be reduced to $\mathfrak{a} - SPP_\gamma$.

We give below a lemma that relates ${\lambda_1}^\infty$ with ${\lambda_N}^\infty$ for an ideal $\mathfrak{A} \subseteq \mathbb{Z}[x_1, \dots, x_n]/\mathfrak{a}$, where $\mathfrak{a}$ is a prime ideal and $\mathbb{Z}[x_1, \dots, x_n]/\mathfrak{a}$ is free and finitely generated of dimension $N$. It shows that ${\lambda_N}^\infty$ cannot be much bigger than ${\lambda_1}^\infty$ if the ideal is prime.

**Lemma 5.4.** *For every ideal $\mathfrak{A} \subseteq \mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$, where $\mathfrak{a}$ is a prime ideal and $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated of size $N$ and has a free $\mathbb{Z}$-module representation w.r.t. $\prec$, we have*

$$\lambda_N{}^{\infty}(\mathfrak{A}) \leq \mathcal{E}(\mathfrak{a}, \prec, (2, \ldots, 2))\lambda_1{}^{\infty}(\mathfrak{A}).$$

*Proof.* Let $g$ be a polynomial in $\mathfrak{A}$ reduced w.r.t. $\mathfrak{a}$ such that $\|g\|_\infty = \lambda_1{}^{\infty}(\mathfrak{A})$. Let $\mathcal{B} = \{b_1, \ldots, b_N\}$ be the basis for $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$. Then $\{gb_1, \ldots, gb_N\}$ is a linearly independent set because $\mathfrak{a}$ is a prime ideal. Also, $\operatorname{maxdeg}_{x_i}(gb_i) \leq 2 \cdot \operatorname{maxdeg}_{x_i}(\mathfrak{a})$. For $i = 1, \ldots, N$,

$$\begin{aligned}\|gb_i\|_{\mathfrak{a},\prec} \leq \mathcal{E}(\mathfrak{a}, \prec, (2, \ldots, 2))\|gb_i\|_\infty &\leq \mathcal{E}(\mathfrak{a}, \prec, (2, \ldots, 2))\|g\|_\infty, \\ &= \mathcal{E}(\mathfrak{a}, \prec, (2, \ldots, 2))\lambda_1{}^{\infty}(\mathfrak{A}).\end{aligned}$$

□

Now, we define an incremental version of $SPP$.

**Definition 5.5.** The approximate Incremental Shortest Polynomial Problem ($IncSPP_\gamma(\mathfrak{A}, g)$) is defined as follows: Given an ideal $\mathfrak{A} \subseteq \mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ and $g \in \mathfrak{A}$ such that $\|g\|_{\mathfrak{a},\prec} \lneq \gamma\lambda_1{}^{\infty}(\mathfrak{A})$, determine an $h \in \mathfrak{A}$ such that $\|h\|_{\mathfrak{a},\prec} \neq 0$ and $\|h\|_{\mathfrak{a},\prec} \leq \|g\|_{\mathfrak{a},\prec}/2$.

The following result directly follows.

**Lemma 5.6.** *There is a polynomial time reduction from $\mathfrak{a} - SPP_\gamma$ to $\mathfrak{a} - IncSPP_\gamma$.*

## 6. Hardness Results

Let $\mathfrak{a}$ and $\mathfrak{a}'$ be ideals in $\mathbb{Z}[x_1, \ldots, x_n]$ defined as $\mathfrak{a} = \langle x_1{}^{r_1} - 1, x_2{}^{r_2} - 1, \ldots, x_n{}^{r_n} - 1\rangle, r_i \in \mathbb{N}, i = 1, 2, \ldots, n$, and $\mathfrak{a}' = \langle x_1{}^{r_1-1} + x_1{}^{r_1-2} + \cdots + 1, \ldots, x_n{}^{r_n-1} + x_n{}^{r_n-2} + \cdots + 1\rangle$. We prove that solving $SPP_\gamma$ in an ideal in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is equivalent to finding the approximate shortest polynomial in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}'$. Note that if each $r_i$ is a prime number then $\mathfrak{a}'$ is a prime ideal and we have full rank lattices. It also means that each of the generators is irreducible. If one can solve the approximate shortest polynomial problem in the ideal lattices of $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}'$, then one can also solve the approximate shortest polynomial problem in multivariate cyclic lattices (where each $r_i$ is prime), that we conjecture is a hard problem.

**Lemma 6.1.** *Let $\mathfrak{A}$ be an ideal in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ such that the residue class polynomial ring is finitely generated of size $N$ and has a free $\mathbb{Z}$-module representation w.r.t. $\prec$. Given the generators for $\mathfrak{A}$, there is a polynomial time algorithm to find the basis for the lattice of $\mathfrak{A}$, $\mathcal{L}(\mathfrak{A})$.*

*Proof.* Let $\mathfrak{A} = \{g_1 + \mathfrak{a}, \ldots, g_m + \mathfrak{a}\}$. Let the residue classes of $\mathcal{B} = \{b_1, \ldots, b_N\}$ be a basis for $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$. Consider the set $G = \{g_1b_1 + \mathfrak{a}, \ldots, g_1b_N + \mathfrak{a}, \ldots, g_mb_1 + \mathfrak{a}, \ldots, g_mb_N + \mathfrak{a}\}$. All the elements of $\mathfrak{A}$ can be written as an integer combination of elements in $G$ and therefore $\mathfrak{A}$ is a $\mathbb{Z}$-module. Using Hermite normal form one can determine the basis of the $\mathbb{Z}$-module as an additive group in polynomial time. □

**Lemma 6.2.** *Let $\mathfrak{a}$ and $\mathfrak{a}^{'}$ be ideals as defined as above. Given a multivariate cyclic lattice $\mathfrak{A}$ in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ of dimension $N$, there is a polynomial time reduction from the problem of approximating the shortest vector in $\mathfrak{A}$ within a factor of $2\gamma$ to approximating the shortest vector in an ideal in the ring, $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}^{'}$ within a factor of $\gamma$.*

*Proof.* Let $f$ be a polynomial of smallest infinity norm such that $f+\mathfrak{a} \in \mathfrak{A}$ and $f+\mathfrak{a}$ is reduced modulo $\mathfrak{a}$ w.r.t. some monomial order, $\prec$. If $f \notin \mathfrak{a}^{'}$, $\|f\|_{\mathfrak{a}',\prec} \leq 2\|f\|_{\infty}$, since its residue class is reduced w.r.t. $\mathfrak{a}^{'}$. There exists a non zero polynomial in $\mathfrak{A}$ whose infinity norm is at most $2\|f\|_{\infty}$. Thus the algorithm for approximating the shortest polynomial in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}^{'}$ to within a factor of $\gamma$ will find a non-zero polynomial of infinity norm at most $2\gamma\|f\|_{\infty}$. Every non-zero polynomial in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}^{'}$ is non zero in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$. If $f \in \mathfrak{a}^{'}$, we have $f \in \mathfrak{a}^{'} \cap \mathfrak{A}$. Since $f$ is reduced w.r.t. $\mathfrak{a}$, $f$ is a sum of integer multiples of the generators of $\mathfrak{a}^{'}$. We can find a basis for the one dimensional lattice $\mathfrak{a}^{'} \cap \mathfrak{A}$ and the generator will be the shortest polynomial.

**Conjecture 6.3.** Approximation problems like $SVP_{\gamma}$ are computationally hard in multivariate cyclic lattices with prime powers.

The conjecture is based on the assumption that the $SVP_{\gamma}$ problem is hard for univariate cyclic lattices of prime powers (Micciancio, 2002). Given,

$$\mathbb{Z}[x_1, \ldots, x_n]/\langle {x_1}^{r_1} - 1, {x_2}^{r_2} - 1, \cdots, {x_n}^{r_n} - 1\rangle, \;\; r_i \in \mathbb{N},$$

where each $r_i$ is prime, the multivariate cyclic lattice in $n$ indeterminates is equivalent to $n$ independent univariate cyclic lattices of prime powers. This is because the multivariate cyclic shifts in the $n^{\text{th}}$ order tensor $\mathcal{A}_i$ for each $i = 1, \ldots, n$ are independent of each other (see Section 3). This implies, the assumption that the $SVP_{\gamma}$ problem is hard for univariate cyclic lattices of prime powers can be applied for each $i = 1, 2, \ldots, n$ individually. Therefore, if the approximation problems are hard for univariate cyclic lattices with prime powers then they are computationally hard for multivariate cyclic lattices with prime powers as well.

We now give the hardness results for multivariate ideal lattices based on results from function fields of algebraic varieties. A function field of an affine variety $\mathcal{V}$ is the quotient field of the coordinate ring $\mathbb{k}[x_1, \ldots, x_n]/\mathcal{I}(\mathcal{V})$, often described as the field of rational functions on $\mathcal{V}$. Note that in the univariate case, the $SPP$ problem can be reduced to the problem of finding small conjugates in ideals of subrings of a number field which is a hard problem (Lyubashevsky & Micciancio, 2006).

To prove the hardness of $SPP$ we define the following problem. Let $\mathfrak{a}$ be an ideal in $\mathbb{Z}[x_1, \ldots, x_n]$ such that $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is free and finitely generated. Consider the variety of $\mathfrak{a}$ in $\mathbb{C}^n$, $\mathcal{V}_{\mathbb{C}}(\mathfrak{a})$. Then for every $(a_1, \ldots, a_n) \in \mathcal{V}_{\mathbb{C}}(\mathfrak{a})$ the following mapping

$$\begin{aligned} \psi : \mathbb{Z}[a_1, \ldots, a_n] &\longrightarrow \mathbb{Z}[x_1, \ldots, x_n]/\sqrt{\mathfrak{a}} \\ \sum_{i=1}^{l} \alpha_i {a_1}^{i_1} \ldots {a_n}^{i_n} &\longmapsto \sum_{i=1}^{l} \alpha_i {x_1}^{i_1} \ldots {x_n}^{i_n} + \sqrt{\mathfrak{a}}, \end{aligned} \tag{2}$$

where $l \in \mathbb{N}$ and $\sqrt{\mathfrak{a}}$ is the radical of the ideal, is an isomorphism. When $\mathbb{Z}[x_1, \ldots, x_n]/\sqrt{\mathfrak{a}}$ is free and finitely generated, $\mathcal{V}_{\mathbb{C}}(\mathfrak{a})$ is a finite set. For ease of notation we will omit the subscript $\mathbb{C}$ and denote the variety as $\mathcal{V}(\mathfrak{a})$.

For $(a_1, \ldots, a_n) \in \mathcal{V}(\mathfrak{a})$ and $\alpha = \sum_{i=1}^{l} \alpha_i {a_1}^{i_1} \cdots {a_n}^{i_n}$, a polynomial in $\mathbb{Z}[a_1, \ldots, a_n]$, we define $\mathrm{maxCoeff}_{(a_1,\ldots,a_n)}(\alpha)$ as $\max_{1 \le i \le l}(\mid \alpha_i \mid)$. Let $\psi_j$ be the isomorphism defined as in Equation (2) for each element of the affine variety, $\mathcal{V}(\mathfrak{a})$. Given an ideal $I$ in $\mathbb{Z}[a_1, \ldots, a_n]$, $(a_1, \ldots, a_n) \in \mathcal{V}(\mathfrak{a})$, for an element $\alpha = \sum_{i=1}^{l} \alpha_i {a_1}^{i_1} \ldots {a_n}^{i_n}$ in $I$, we define

$$\mathrm{maxsub}(\alpha) = \max_{1 \le j \le N} \{ \sum_{i=1}^{l} \alpha_i {a_1^{(j)}}^{i_1} \ldots {a_n^{(j)}}^{i_n} : (a_1^{(j)}, \ldots, a_n^{(j)}) \in \mathcal{V}(\mathfrak{a}) \}.$$

**Definition 6.4.** (Approximate Smallest Substitution Problem ($SSub$)) Let $\mathfrak{a} \subseteq \mathbb{Z}[x_1, \ldots, x_n]$ be an ideal such that $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is free and finitely generated. Let the finite variety, $\mathcal{V}(\mathfrak{a})$ be of cardinality $N$. Given an ideal $I$ in $\mathbb{Z}[a_1, \ldots, a_n]$, $(a_1, \ldots, a_n) \in \mathcal{V}(\mathfrak{a})$, the approximate smallest substitution problem, $SSub_\gamma(I)$ is defined as follows: find an element $\alpha \in I$ such that $\mathrm{maxsub}(\alpha) \le \gamma \mathrm{maxsub}(\alpha^{'})$, for all $\alpha^{'} \in I$.

It is important to note that formulation of the smallest substitution problem in the multivariate case is quite different from the univariate case. In the univariate case, the problem that is mapped to $SPP$ is the smallest conjugate problem ($SCP$). For any $\alpha$ in the ideal $I$, first a function called maxConj analogous to the maxsub is defined. The function returns the maximum of the zeroes of the minimum polynomial of $\alpha$ over $\mathbb{Q}$. $SCP$ poses the problem of finding an $\alpha \in I$ such that it has the least maxConj among all the elements in $I$. This relates to the problem of isomorphism of number fields for which no polynomial time algorithm is determined (Cohen, 2013, Polynomial Reduction Algorithm). The hardness of $SCP$ is discussed in (Lyubashevsky & Micciancio, 2006). We argue that the smallest substitution problem, $SSub$, relates to the problem of isomorphism of function fields, the multivariate extension of number fields and a hard problem (Pukhlikov, 1998). We show below that $SCP$ is a special instance of the $SSub$ problem. That is, $SCP$ is polynomially reducible to $SSub$.

**Theorem 6.5.** *Given an monic irreducible polynomial $f \in \mathbb{Z}[x]$ of degree $N$, let $\mathfrak{a} = \langle f \rangle$ be an ideal in $\mathbb{Z}[x]$. There is a polynomial time reduction from $\mathfrak{a} - SCP$ to $\mathfrak{a} - SSub$.*

*Proof.* Let $\mathcal{V}$ be the variety associated with $\mathfrak{a}$ of cardinality $N$. For $a \in \mathcal{V}$, we have the isomorphism, $\psi$ given by Equation (2), $\mathbb{Z}[a] \cong \mathbb{Z}[x]/\mathfrak{a}$. An algorithm for $\mathfrak{a} - SSub_\gamma$ returns an $\alpha \in \mathbb{Z}[a]$, $a \in \mathcal{V}(\mathfrak{a})$ such that $\mathrm{maxsub}(\alpha) \le \gamma \mathrm{maxsub}(\alpha^{'})$, for all $\alpha^{'} \in \mathbb{Z}[a]$. Let $\alpha = \alpha_0 + \alpha_1 a + \cdots + \alpha_{N-1} a^{N-1}$ and

$$\mathrm{maxsub}(\alpha) = \max_{1 \le j \le N} \{ \sum_{i=0}^{N-1} \alpha_i {a^{(j)}}^{i} : a^{(j)} \in \mathcal{V}(\mathfrak{a}) \}.$$

Since the set, $\{\sum_{i=0}^{N-1} \alpha_i {a^{(j)}}^i\}$ is the set of zeroes of the minimal polynomial of $\alpha$ over $\mathbb{Q}$, we have $\mathrm{maxsub}(\alpha) = \mathrm{maxConj}(\alpha)$. Therefore, $\alpha$ is the solution for $\mathfrak{a} - SCP_\gamma$ as well. □

We proceed to find a relation between the maximum coefficient of an element $\alpha$ in the ideal $\mathfrak{A}$ in $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$, and the value of maximum substitution of $\alpha$ under the isomorphism described by Equation (2). This will help us to prove that $SPP$ is polynomially reducible to $SSub$ as the problem of finding an element with the smallest norm in an ideal, $\mathfrak{A}$ in $\mathbb{Z}[x_1, \ldots, x_n]/\sqrt{\mathfrak{a}}$ is equivalent to the problem of finding an element $\alpha$ in the ideal $\psi^{-1}(\mathfrak{A})$ in $\mathbb{Z}[a_1, \ldots, a_n]$ with the smallest $\mathrm{maxCoeff}_{(a_1,\ldots,a_n)}(\alpha)$.

The following result is easy to see.

**Lemma 6.6.** *Let $\mathfrak{a} \subseteq \mathbb{Z}[x_1, \ldots, x_n]$ be an ideal such that $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated and has a free $\mathbb{Z}$-module representation w.r.t. a monomial order, $\prec$. Let the finite set of zeroes, $\mathcal{V}(\mathfrak{a})$ be of cardinality $N$. Let $\mathcal{B}$ be the canonical basis of the free residue class ring constructed using (Francis & Dukkipati, 2014, Theorem 4.1). Let $\alpha \in \mathbb{Z}[a_1, \ldots, a_n]$, $(a_1, \ldots, a_n) \in \mathcal{V}(\mathfrak{a})$. Let $\psi$ be the isomorphism given by Equation (2) and corresponding to each element in $\mathcal{V}$ we have $\psi_i$, $1 \leq i \leq N$. Let $t = \max\limits_{x^\beta \in \mathcal{B}}(\mathrm{maxsub}(\psi^{-1}(x^\beta)))$. Then,*

$$\mathrm{maxsub}(\alpha) \leq Nt\, \mathrm{maxCoeff}_{({a_1}^{(i)},\ldots,{a_n}^{(i)})}(\alpha),$$

*where $({a_1}^{(i)}, \ldots, {a_n}^{(i)})$ corresponds to $\psi_i$, $i = 1, \ldots, N$.*

The above result allows us to upper bound the maximum substitution w.r.t. a factor (polynomial in $N$) of the maximum coefficient. To prove that $SPP$ can be polynomially reduced to $SSub$ and vice-versa, we need to give an upper bound for the maximum coefficient w.r.t. the maximum substitution value. We first give a result that upper bounds the maximum coefficient value to a factor (that is not a polynomial in $N$) of the maximum substitution value. Then for the specific case of

$$\mathfrak{a} = \langle {x_1}^{r_1-1} + {x_1}^{r_1-2} + \cdots + 1, \ldots, {x_n}^{r_n-1} + {x_n}^{r_n-2} + \cdots + 1 \rangle,$$

we give an upper bound to a factor of $N$.

**Lemma 6.7.** *Let $G$ be a short reduced Gröbner basis of an ideal $\mathfrak{a} \subseteq \mathbb{Z}[x_1, \ldots, x_n]$ such that $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated and has a free $\mathbb{Z}$-module representation w.r.t. $G$. Let the finite set of zeroes, $\mathcal{V}(\mathfrak{a})$ be of cardinality $N$ and $\mathcal{B}$ be the canonical basis of the free residue class ring. Let $\alpha \in \mathbb{Z}[a_1, \ldots, a_n], (a_1, \ldots, a_n) \in \mathcal{V}(\mathfrak{a})$. We have $\mathrm{maxsub}(\alpha) \in \mathbb{C}$. We denote the $\max\limits_{x^\beta \in \mathcal{B}}(\mathrm{maxsub}(\psi^{-1}(x^\beta)))$ by $t$. Let $\psi_i$ be the $N$ distinct isomorphisms in Equation (2) for each element in $\mathcal{V}$. For $i \in \{1, \ldots, n\}$, let*

$$r_i = \max\{\nu : \nu \in \mathbb{N}, \mathrm{lt}(g) = {x_i}^\nu, g \in G\}.$$

*Suppose the following conditions are satisfied.*

*(1) There exists an integer tuple $(m_1, \ldots, m_n)$, $m_i \in \mathbb{N}$, $m_i \geq r_i$ such that for all $1 \leq k \leq N$ and for $(j_1, \ldots, j_n)$ such that $j_i \leq m_i - 1$ we have,*
  *(a) $1 \leq \left|{a_1}^{(k)^{j_1}} \ldots {a_n}^{(k)^{j_n}}\right| \leq t$ and*

*(b) for every* $(a_1{}^{(k)},\ldots,a_n{}^{(k)})\in\mathcal{V}(\mathfrak{a})$,

$$\sum_{k=1}^{N}\left(a_1{}^{(k)}\right)^{m_1}\ldots\left(a_n{}^{(k)}\right)^{m_n}\geq N$$

*(2) There exists a constant $s$ such that for all $(j_1,\ldots,j_n)$, where $j_i\neq 0 \bmod m_i$ and for $k\in\{1,\ldots,N\}$, we have,*

$$\Big|\sum_{k=1}^{N}\left(a_1{}^{(k)}\right)^{j_1}\ldots\left(a_n{}^{(k)}\right)^{j_n}\Big|\leq s\leq 1.$$

*Then for all $\alpha\in\mathbb{Q}$, we have*

$$\mathrm{maxCoeff}_{(a_1{}^{(1)},\ldots,a_n{}^{(1)})}(\alpha)\leq\Big(\frac{Nt}{N(1-s)+s}\Big)\mathrm{maxsub}(\alpha).$$

*Proof.* The existence of $r_i, i=1,2,\ldots,n$ is assured by (Francis & Dukkipati, 2014, Theorem 4.3). For each $(j_1,\ldots,j_n)$ such that $0\leq j_i\leq r_i-1$, we have the following set of $N$ inequalities, $1\leq k\leq N$

$$\left|\psi_k(\alpha)a_1{}^{(k)^{m_1-r_1+j_1}}\cdots a_n{}^{(k)^{m_n-r_n+j_n}}\right|\leq\mathrm{maxsub}(\alpha)t.$$

This is because by definition $|\psi_k(\alpha)|\leq\mathrm{maxsub}(\alpha)$ and by (1.a),

$$|a_1{}^{(k)^{m_1-r_1+j_1}}\ldots a_n{}^{(k)^{m_n-r_n+j_n}}|\leq t.$$

We look at the the system of inequalities for a specific $(j_1,\ldots,j_n)$. Let $\alpha=\sum_{i=1}^{N}\alpha_{(i_1,\ldots,i_n)}a_1{}^{i_1}\cdots a_n{}^{i_n}$. We have,

$$\psi_j(\alpha)=\sum_{i=1}^{m}\alpha_{(i_1,\ldots,i_n)}a_1{}^{(j)^{i_1}}\ldots a_n{}^{(j)^{i_n}},$$

where $(a_1{}^{(j)},\ldots,a_n{}^{(j)})\in\mathcal{V}(\mathfrak{a})$. For $k\in\{1,\ldots,N\}$ we have,

$$\begin{aligned}&\left|\psi_k(\alpha)(a_1{}^{(k)^{m_1-r_1+j_1}}\ldots a_n{}^{(k)^{m_n-r_n+j_n}})\right|\\&=\Big|\alpha_{(0,0,\ldots,0)}a_1{}^{(k)^{m_1-r_1+j_1}}\cdots a_n{}^{(k)^{m_n-r_n+j_n}}+\cdots\\&\quad+\alpha_{(r_1-j_1,\ldots,r_n-j_n)}a_1{}^{(k)^{m_1}}\ldots a_n{}^{(k)^{m_n}}+\cdots+\alpha_{(r_1-1,\ldots,r_n-1)}a_1{}^{(k)^{m_1+j_1-1}}\ldots a_n{}^{(k)^{m_n+j_n-1}}\Big|\\&\leq\mathrm{maxsub}(\alpha)t.\end{aligned}$$

Let $A=\sum_{i=1}^{N}\alpha_{(i_1,\ldots,i_n)}$ and $S_{(j_1,\ldots,j_n)}=\sum_{i=1}^{N}a_1{}^{(i)^{m_1-r_1+j_1}}\cdots a_n{}^{(i)^{m_n-r_n+j_n}}$. Then,

$$\begin{aligned}&N|\alpha_{r_1-j_1,\ldots,r_n-j_n}|-s(A-|\alpha_{r_1-j_1,\ldots,r_n-j_n}|)\\&=N|\alpha_{r_1-j_1,\ldots,r_n-j_n}|-s(|\alpha_{(0,\ldots,0)}|+\cdots+|\alpha_{(r_1-j_1-1,\ldots,r_n-j_n-1)}|\\&\quad+|\alpha_{(r_1-j_1+1,\ldots,r_n-j_n+1)}|+\cdots+|\alpha_{(r_1-1,\ldots,r_n-1)}|)\\&\leq|\alpha_{(r_1-j_1,\ldots,r_n-j_n)}S_{(r_1,\ldots,r_n)}|-(|\alpha_{(0,\ldots,0)}S_{(j_1,\ldots,j_n)}|+\cdots+|\alpha_{(r_1-j_1-1,\ldots,r_n-j_n-1)}S_{(r_1-1,\ldots,r_n-1)}|+\\&\quad|\alpha_{(r_1-j_1+1,\ldots,r_n-j_n+1)}S_{(r_1+1,\ldots,r_n+1)}|+\cdots+|\alpha_{(r_1-1+j_1,\ldots,r_n-1+j_n)}|)\\&\leq|\psi_1(\alpha)a_1{}^{(1)^{m_1-r_1+j_1}}\cdots a_n{}^{(1)^{m_n-r_n+j_n}}|+\cdots+|\psi_N(\alpha)a_1{}^{(N)^{m_1-r_1+j_1}}\cdots a_n{}^{(N)^{m_n-r_n+j_n}}|\\&\leq Nt\,\mathrm{maxsub}(\alpha).\end{aligned}$$

This implies,

$$(N+s)|\alpha_{r_1-j_1,\dots,r_n-j_n}| - sA \le Nt \operatorname{maxsub}(\alpha)$$
$$|\alpha_{r_1-j_1,\dots,r_n-j_n}| \le \frac{Nt \operatorname{maxsub}(\alpha) + sA}{N+s}.$$

Let $B = \frac{Nt \operatorname{maxsub}(\alpha)+sA}{N+s}$. Since $A = \sum_{i=1}^{N} \alpha_{(i_1,\dots,i_n)}$ we get $A \le N \times B$. We have,

$$(N+s-ns)B \le Nt \operatorname{maxsub}(\alpha).$$

We have $|\alpha_{r_1-j_1,\dots,r_n-j_n}| \le B$, which implies,

$$\operatorname{maxCoeff}_{({a_1}^{(1)},\dots,{a_n}^{(1)})}(\alpha) \le \frac{Nt}{N(1-s)+s} \operatorname{maxsub}(\alpha).$$

□

The above lemma gives the bound that is similar to the univariate case. We now study the above lemma for the specific case of

$$\mathfrak{a} = \langle {x_1}^{r_1-1} + {x_1}^{r_1-2} + \cdots + 1, \dots, {x_n}^{r_n-1} + {x_n}^{r_n-2} + \cdots + 1 \rangle.$$

In this case, maxCoeff is bound by a factor of $N$.

**Proposition 6.8.** *Let*

$$\mathfrak{a} = \langle {x_1}^{r_1-1} + {x_1}^{r_1-2} + \cdots + 1, \dots, {x_n}^{r_n-1} + {x_n}^{r_n-2} + \cdots + 1 \rangle$$

*be an ideal in* $\mathbb{Z}[x_1, \dots, x_n]$*. Then,*

$\mathcal{V}(\mathfrak{a}) = \{(a_1, \dots, a_n) \in {\mathbb{A}_{\mathbb{C}}}^n : a_i$ *is a zero of* ${x_i}^{r_i-1} + {x_i}^{r_i-2} + \cdots + 1, i \in \{1, \dots, n\}\}$.

**Proposition 6.9.** *Let*

$$\mathfrak{a} = \langle {x_1}^{r_1-1} + {x_1}^{r_1-2} + \cdots + 1, \dots, {x_n}^{r_n-1} + {x_n}^{r_n-2} + \cdots + 1 \rangle$$

*be an ideal in* $\mathbb{Z}[x_1, \dots, x_n]$*,* $\mathcal{V}$*, the finite set of zeroes of cardinality* $N$ *and* $({a_1}^{(1)}, \dots, {a_n}^{(1)})$*, one of the zeroes. Let* $\alpha \in \mathbb{Z}[x_1, \dots, x_n]/\mathfrak{a}$*. Then,*

$$\operatorname{maxCoeff}_{({a_1}^{(1)},\dots,{a_n}^{(1)})}(\alpha) \le N \operatorname{maxsub}(\alpha)$$

and

$$\operatorname{maxsub}(\alpha) \le N \operatorname{maxCoeff}_{({a_1}^{(1)},\dots,{a_n}^{(1)})}(\alpha).$$

*Proof.* By Equation (2), $\mathbb{Z}[x_1, \dots, x_n]/\mathfrak{a}$ is isomorphic to $\mathbb{Z}[a_1, \dots, a_n]$, $(a_1, \dots, a_n) \in \mathcal{V}(\mathfrak{a})$. We have from Lemma 6.6 that

$$\operatorname{maxsub}(\alpha) \le Nt \operatorname{maxCoeff}_{({a_1}^{(1)},\dots,{a_n}^{(1)})}(\alpha).$$

The zeroes of this ideal are the zeroes of each individual generator (Proposition 6.8). Each individual generating polynomial is a cyclotomic polynomial and therefore all the zeroes of generators are of norm 1 and so we have $t = 1$ and the following inequality,

$$\operatorname{maxsub}(\alpha) \le N \operatorname{maxCoeff}_{({a_1}^{(1)},\dots,{a_n}^{(1)})}(\alpha).$$

Now to prove that $\mathrm{maxCoeff}_{(a_1{}^{(1)},\dots,a_n{}^{(1)})}(\alpha) \leq N \,\mathrm{maxsub}(\alpha)$. If the conditions in Lemma 6.7 are satisfied we have that

$$\mathrm{maxCoeff}_{(a_1{}^{(1)},\dots,a_n{}^{(1)})}(\alpha) \leq \frac{Nt}{N(1-s)+s}\mathrm{maxsub}(\alpha).$$

Now we show that the conditions in Lemma 6.7 are indeed satisfied. We have $t = 1$ and $m_i = r_i$. We need to determine if

$$\Big|\sum_{i=1}^{N} a_1{}^{(i)m_1} \dots a_n{}^{(i)m_n}\Big| \geq N,$$

and if we can find a $s$ such that

$$\Big|\sum_{i=1}^{N} a_1{}^{(i)j_1} \dots a_n{}^{(i)j_n}\Big| \leq s \leq 1.$$

We have that $a_i{}^{(j)}$ is the zero of $x_i{}^{r_i-1} + x_i{}^{r_i-2} + \dots + 1$. This implies

$$a_i{}^{(j)m_i} = (a_i{}^{(j)}(r_i-1) + a_i{}^{(j)}r_i - 2) + \dots + 1)(a_i{}^{(j)} - 1) + 1 = 1.$$

So, $\Big|\sum_{i=1}^{N} a_1{}^{(i)m_1} \dots a_n{}^{(i)m_n}\Big| = N$. Since each generator, $g_i = x_i{}^{r_i-1} + x_i{}^{r_i-2} + \dots + 1$, is a cyclotomic polynomial it has a zero, say $a_i{}^{(1)}$, such that all the remaining zeroes, $a_i{}^{(j)}$ is some power of this root, i.e. $a_i{}^{(1)^j} = a_i{}^{(j)}$. We also have, $a_i{}^{(j)^{r_i}} = 1$, $j = 1, \dots, n$. Therefore,

$$a_i{}^{(j)^k} = a_i{}^{(j)^{k \bmod r_i}}, k \in \mathbb{N}.$$

We will now find a $s$ such that the second condition in Lemma 6.7 is satisfied. For all $(j_1, \dots, j_n)$, where $j_i \neq 0 \bmod m_i$ for some $i = 1, \dots, n$, we have,

$$\Big|\sum_{i=1}^{m} (a_1{}^{(i)})^{j_1} \dots (a_n{}^{(i)})^{j_n}\Big| = \Big|\sum_{i=1}^{m} (a_1{}^{(i)})^{j_1 \bmod m_1} \dots (a_n{}^{(i)})^{j_n \bmod m_n}\Big|.$$

We replace the zeroes with powers of $a_i{}^{(1)}$ for $i = 1, \dots, n$. Therefore we have,

$$\Big|\sum_{i=1}^{m} (a_1{}^{(i)})^{j_1} \dots (a_n{}^{(i)})^{j_n}\Big| = \Big|\sum_{i=1}^{m} (a_1{}^{(1)})^{i\,j_1 \bmod m_1} \dots (a_n{}^{(1)})^{i\,j_n \bmod m_n}\Big|$$
$$= \Big|\sum_{i=1}^{m} (a_1^{(j_1 \bmod m_1)})^{i} \dots (a_n^{(j_n \bmod m_n)})^{i}\Big| = |-1| = 1.$$

We can take $s = 1$ and apply in the inequality from Lemma 6.7 to get,

$$\mathrm{maxCoeff}_{(a_1{}^{(1)},\dots,a_n{}^{(1)})}(\alpha) \leq N \,\mathrm{maxsub}(\alpha).$$

$\square$

The result below connects $SPP$ with $SSub$ by a factor that is polynomial in the cardinality of $\mathcal{V}(\mathfrak{a})$.

**Theorem 6.10.** *Let*

$$\mathfrak{a} = \langle {x_1}^{r_1-1} + {x_1}^{r_1-2} + \cdots + 1, \ldots, {x_n}^{r_n-1} + {x_n}^{r_n-2} + \cdots + 1\rangle$$

*be an ideal in* $\mathbb{Z}[x_1, \ldots, x_n]$ *. The residue class polynomial ring,* $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ *is free and finitely generated. Let* $\mathcal{V}(\mathfrak{a})$ *be of cardinality* $N$*. Let* $\psi$ *represent the isomorphism as described in Equation* (2)*. Then,*

$$\mathfrak{a} - SPP_{\gamma N^2}(\mathfrak{A}) \leq \mathfrak{a} - SSub_{\gamma}(\psi^{-1}(\mathfrak{A})) \text{ and} \tag{3}$$

$$\mathfrak{a} - SSub_{\gamma N^2}(\psi^{-1}(\mathfrak{A})) \leq \mathfrak{a} - SPP_{\gamma}(\mathfrak{A}). \tag{4}$$

*Proof.* Let $\psi^{-1}(\mathfrak{A}) \subseteq \mathbb{Z}[a_1, \ldots, a_n]$, $(a_1, \ldots, a_n) \in \mathcal{V}(\mathfrak{a})$, be an ideal given by its generators $\mathcal{F} = \{f_1, \ldots, f_k\}$. Then each element in $\mathcal{F}$ can be written in terms of the elements $\{a_1, \ldots, a_n\}$ such that $(a_1, \ldots, a_n) \in \mathcal{V}$. The oracle for $\mathfrak{a} - SPP_{\gamma}(\mathfrak{A}))$ finds us an element $h \in \mathfrak{A}$ such that its norm is less than $\gamma{\lambda_1}^{\infty}(\mathfrak{A})$. Let $\alpha = \psi^{-1}(h)$. We have,

$$\text{maxCoeff}_{(a_1,\ldots,a_n)}(\alpha) \leq \gamma \cdot \text{maxCoeff}_{(a_1,\ldots,a_n)}(\alpha^{'}),$$

for all $\alpha^{'} \in \psi^{-1}(\mathfrak{A})$. Applying Proposition 6.9 twice we get,

$$\begin{aligned}\text{maxsub}(\alpha) &\leq N \cdot \text{maxCoeff}_{(a_1,\ldots,a_n)}(\alpha),\\ &\leq N\gamma \cdot \text{maxCoeff}_{(a_1,\ldots,a_n)}(\alpha^{'}), \text{for all } \alpha^{'} \in \psi^{-1}(\mathfrak{A}),\\ &\leq N^2\gamma \cdot \text{maxsub}(\alpha^{'}), \text{ for all } \alpha^{'} \in \psi^{-1}(\mathfrak{A}).\end{aligned}$$

Thus we have a $\gamma \cdot N^2$ approximation for $\mathfrak{a} - SSub$. Hence Equation (4) holds.

Next, we show Equation (3) holds. The oracle for $\mathfrak{a} - SSub_{\gamma}(\psi^{-1}(\mathfrak{A}))$ finds an element $\alpha \in \psi^{-1}(\mathfrak{A})$ such that $\text{maxsub}(\alpha) \leq \gamma \cdot \text{maxsub}(\alpha^{'})$, for all $\alpha^{'} \in \psi^{-1}(\mathfrak{A})$. Again we apply Proposition 6.9 twice.

$$\begin{aligned}\text{maxCoeff}_{(a_1,\ldots,a_n)}(\alpha) &\leq N \cdot \text{maxsub}(\alpha),\\ &\leq N\gamma \cdot \text{maxsub}(\alpha^{'}), \text{ for all } \alpha^{'} \in \psi^{-1}(\mathfrak{A}),\\ &\leq N^2\gamma \cdot \text{maxCoeff}_{(a_1,\ldots,a_n)}(\alpha^{'}),\end{aligned}$$

for all $\alpha^{'} \in \psi^{-1}(\mathfrak{A})$. We have a $\gamma \cdot N^2$ approximation for $\mathfrak{a} - SPP$. □

## 7. Collision Resistant Generalized Hash Functions

We can construct hash function families described in Section 2 based on multivariate ideal lattices. Consider a prime ideal, $\mathfrak{a} \subseteq \mathbb{Z}[x_1, \ldots, x_n]$ such that the residue class polynomial ring, $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is free and finitely generated and is of size $N \in \mathbb{N}$. The hash function family $\mathcal{H}(R, D, m)$ is given by $R = \mathbb{Z}_p[x_1, \ldots, x_n]/\mathfrak{a}$, where $p \in \mathbb{N}$ is approximately of the order $N^2$ and $D$ is a strategically chosen subset of $R$ and $m \in \mathbb{N}$. Let the expansion factor, $\mathcal{E}(\mathfrak{a}, \prec, (3, 3, \ldots, 3)) \leq \eta$, for some $\eta \in \mathbb{R}$. Let $D = \{g \in R : \|g\|_{\mathfrak{a},\prec} \leq d\}$ for some positive integer $d$. Then $\mathcal{H}$ maps elements from $D^m$ to $R$. We have $|D^m| = (2d+1)^{Nm}$ and $|R| = p^N$. If $m \gnsim \frac{\log p}{\log 2d}$, then $\mathcal{H}$ will have collisions. We show that finding a collision for a hash function randomly chosen from $\mathcal{H}$ is as hard as solving $\mathfrak{a} - SPP_{\gamma}$ for a particular ideal in $\mathfrak{A} \subseteq \mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$. As we mentioned before, even though the hardness results of univariate and multivariate ideal lattices are based on different problems, other properties like collision resistance of hash functions are exactly analogous. The reader can refer to (Lyubashevsky & Micciancio, 2006) for detailed constructions.

**Theorem 7.1.** *Consider an ideal $\mathfrak{a} \subseteq \mathbb{Z}[x_1, \ldots, x_n]$ such that the residue class polynomial ring, $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is finitely generated of size $N \in \mathbb{N}$ and has a free $\mathbb{Z}$-module representation w.r.t. $\prec$. Let $\mathcal{H}(R, D, m)$ be the associated hash function family as mentioned above with $R = \mathbb{Z}_p[x_1, \ldots, x_n]/\mathfrak{a}$, $m \gneq \frac{\log p}{\log 2d}$ and $p \geq 8\eta dmN^{1.5}\sqrt{\log N}$. Then, for $\gamma = 8\eta^2 dmN \log^2 N$, there is a polynomial time reduction from $\mathfrak{a} - SPP_\gamma(\mathfrak{A})$, for any ideal $\mathfrak{A} \subseteq \mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$, to $Collision_{\mathcal{H}}(\mathfrak{h})$ where $\mathfrak{h}$ is chosen uniformly at random from $\mathcal{H}$.*

$Collision_{\mathcal{H}}(\mathfrak{h})$ is the problem of finding a collision given a hash function, $\mathfrak{h}$. The idea is that if one can solve in polynomial time the problem $Collision_{\mathcal{H}}(\mathfrak{h})$ for a randomly chosen $\mathfrak{h}$ then we can solve the $\mathfrak{a} - IncSPP_\gamma$ problem for any ideal $\mathfrak{A}$ and $\gamma = 8\eta^2 dmN \log^2 N$. This implies we have a polynomial reduction from $\mathfrak{a} - SPP_\gamma$ to $Collision_{\mathcal{H}}(\mathfrak{h})$.

We consider an oracle $\mathcal{C}$, which when given an $\mathfrak{h}$ returns a collision with non-negligible probability and in polynomial time. We are given an ideal $\mathfrak{A} \subseteq \mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ and an element of the ideal $g$ such that $\|g\|_\infty \gneq 8\eta^2 dmN \log^2 N \lambda_1{}^\infty(\mathfrak{A})$. We have to find a non-zero $h \in \mathfrak{A}$ such that $\|h\|_{\mathfrak{a},\prec} \leq \|g\|_{\mathfrak{a},\prec}/2$.

Given vectors $c, x \in \mathbb{R}^N$ and any $l \gneq 0$, $\rho_{l,c}(x) = e^{-\pi\|(x-c)/l\|^2}$ represents a Gaussian function that has its center at $c$ and is scaled by $l$. The total measure is $\int_{x\in\mathbb{R}^N} \rho_{l,c}(x)dx = l^N$ and therefore $\rho_{l,c}/l^N$ is a probability density function. Micciancio & Regev (2004) introduced certain techniques to approximate the distribution efficiently, effectively allowing us to sample from the distribution, $\rho_{l,c}/l^N$ exactly. In this paper, the results are used in the same way as in (Lyubashevsky & Micciancio, 2006) as the results are for integer lattices in general and not specifically for ideal lattices in one variable.

Let $s = \frac{\|g\|_\infty}{8\eta\sqrt{N}dm \log N}$. Therefore, $\|g\|_\infty = 8\eta dms\sqrt{N} \log N$. Also the results from (Micciancio & Regev, 2004, Lemma 4.1) imply that if we sample $y \in \mathbb{R}^N$ from the distribution $\rho_s/s^N$, then

$$\triangle(y + \mathfrak{A}, U(\mathbb{R}^N/\mathfrak{A})) \leq (\log N)^{-2 \log N}/2,$$

i.e. $y + \mathfrak{A}$ is a uniformly random coset. We list a procedure in Algorithm 1, by which using the access to the oracle one can determine an $h$ such that it is a solution to the $IncSPP_\gamma$ problem. Now, it is enough to show that Algorithm 1 runs in polynomial time, the inputs to the oracle are uniformly random, and $h$ satisfies all the desired properties.

**Lemma 7.2.** *Algorithm 1 runs in polynomial time.*

*Proof.* In Step (4), we need to generate a random coset of $\mathfrak{A}/\langle g\rangle$. Since $\mathfrak{a}$ is a prime ideal, the ideals $\mathfrak{A}$ and $\langle g\rangle$ are $\mathbb{Z}$-modules of dimension $n$. There is a polynomial time algorithm to generate a random element from $\mathfrak{A}/\langle g\rangle$ (Micciancio, 2002, Proposition 8.2). Step (5) and Step (6) will be justified in the following lemma. Step (7) just

**Algorithm 1** Finding the solution of the $IncSPP_\gamma$ problem given access to the *Collision* oracle

1: **Input** Finitely generated $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ with a free $\mathbb{Z}$-module representation w.r.t. $\prec$,
$\mathfrak{A} \subseteq \mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ an ideal, and
$g \in \mathfrak{A}$ such that $\|g\|_\infty = 8\eta dms\sqrt{N}\log N$.
2: **Output** $h \in \mathfrak{A}$ such that $\|h\| \neq 0$ $\|h\|_{\mathfrak{a},\prec} \leq \|g\|_{\mathfrak{a},\prec}/2$.
3: **for** $i = 1$ to $m$ **do**
4: Generate a random coset of $\mathfrak{A}/\langle g\rangle$ and let $v_i$ be a polynomial in that coset.
5: Generate $y_i \in \mathbb{R}^N$ such that $y_i$ has distribution $\rho_s/s^n$ and consider $y_i$ as a polynomial in $\mathbb{R}[x_1, \ldots, x_n]$.
6: Let $w_i \in \mathbb{R}[x_1, \ldots, x_n]$ be the unique polynomial such that $p(v_i + y_i) \equiv gw_i$ in $\mathbb{R}^N/\langle pg\rangle$. Note that the coefficients of $w_i$ lie in $[0, p)$.
7: Let $a_i = [w_i] \bmod p$ .
8: **end for**
9: Give $(a_1, \ldots, a_m)$ as input to the oracle $C$ and using its output determine polynomials $z_1, \ldots, z_m$ such that $\|z\|_{\mathfrak{a},\prec} \leq 2d$ and $\sum_{i=1}^m z_i a_i \equiv 0$ in the ring $\mathbb{Z}_p[x_1, \ldots, x_n]/\mathfrak{a}$. (Details of the construction of $z_i$ can be found in Lemma 7.2).
10: Output $h = \left(\sum_{i=1}^m \left(\frac{g(w_i - [w_i]}{p} - y_i\right) z_i\right) \bmod \mathfrak{a}$.

rounds off the coefficients and takes modulo $p$ and therefore can be done in polynomial time. In Step (9), we feed $(a_1, \ldots, a_m)$ to the *Collision* oracle and it returns $(\alpha_1, \ldots, \alpha_m), (\beta_1, \ldots, \beta_m)$ such that $\|\alpha_i\|_{\mathfrak{a},\prec}, \|\beta_i\|_{\mathfrak{a},\prec} \leq d$ and $\sum_{i=1}^m a_i\alpha_i \equiv \sum_{i=1}^m a_i\beta_i$ in $\mathbb{Z}_p[x_1, \ldots, x_n]/\mathfrak{a}$. Therefore, if we set $z_i = \alpha_i - \beta_i$, it satisfies the properties of Step (9). □

**Lemma 7.3.** *Consider the polynomials $a_i$ as elements in ${\mathbb{Z}_p}^N$. Then,*

$$\triangle((a_1, \ldots, a_m), U({\mathbb{Z}_p}^{N\times m})) \leq m(\log N)^{-2\log N}/2.$$

*Proof.* We have chosen $v_i$ from a uniformly random coset of $\mathfrak{A}/\langle g\rangle$. If $y_i$ is in a uniformly random coset of $\mathbb{R}^N/\langle g\rangle$, then $p(v_i + y_i)$ is a uniformly random coset of $\mathbb{R}^N/\langle pg\rangle$. A basis for $\mathbb{R}^N/\langle pg\rangle$ is $\{pgb_1, \ldots, pgb_N\}$ where $\{b_1, \ldots, b_N\}$ is the basis of $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$. Every element in $\mathbb{R}^N/\langle pg\rangle$ can be represented as $\alpha_0 pgb_1 + \cdots + \alpha_N pgb_N$ where $\alpha_i \in [0, 1)$. Therefore Step (6) is justified with $w_i = \alpha_0 pb_1 + \cdots + \alpha_N pb_N$. Since we have assumed $p(v_i + y_i)$ is a uniformly random coset of $\mathbb{R}^N/\langle pg\rangle$ the coefficients of $w_i$ are uniform over $[0, p)$ and the input to the oracle in Step (9) is correct. The only thing remaining is to check if the assumption that $y_i$ is in a uniformly random coset of $\mathbb{R}^N/\langle g\rangle$ is correct. It is not exactly uniformly random but very close to it. We have $\triangle(\rho_s/s^n + \mathfrak{A}, U(\mathbb{R}^N/\mathfrak{A})) \leq (\log N)^{-2\log N}/2$. Since $a_i$ is a function of $y_i$, we have $\triangle(a_i, U({\mathbb{Z}_p}^N)) \leq (\log N)^{-2\log N}/2$. Since all the $a_i$s are independent we have $\triangle((a_1, \ldots, a_m), U({\mathbb{Z}_p}^{N\times m})) \leq m(\log N)^{-2\log N}/2$. □

The following three lemmas ensure that the output of the algorithm, $h$ satisfies the desired properties of the $IncSPP_\gamma$ problem, i.e. $h$ is non zero, $h \in \mathfrak{A}$ and $\|h\|_{\mathfrak{a},\prec} \leq \frac{\|g\|_\infty}{2}$.

**Lemma 7.4.** $h \in \mathfrak{A}$.

*Proof.* The proof proceeds exactly in the same lines as the univariate case. See (Lyubashevsky & Micciancio, 2006, Lemma 5.4). □

**Lemma 7.5.** *With probability negligibly different from* 1, $\|h\|_{\mathfrak{a},\prec} \leq \frac{\|g\|_\infty}{2}$.

*Proof.* See proof of (Lyubashevsky & Micciancio, 2006, Lemma 5.5). □

**Lemma 7.6.** $Pr[h \neq 0 | (a_1, \ldots, a_m)(z_1, \ldots, z_m)] = \Omega(1)$.

*Proof.* See proof of (Lyubashevsky & Micciancio, 2006, Lemma 5.6). □

## 8. Concluding remarks

In this paper, we study ideal lattices in the multivariate case and show how short reduced Gröbner bases can be used to locate them. We show that ideal lattices in the multivariate case are a generalization of multivariate cyclic lattices, thus drawing parallels with univariate ideal lattices. We also provide a necessary and sufficient condition for full rank ideal lattices. We establish the existence of generalized hash functions based on multivariate ideal lattices and prove that they are indeed collision resistant. This class of generalized hash functions includes hash functions based on univariate ideal lattices that were previously studied in cryptography. We propose certain worst case problems based on which we establish the security of these hash functions. We show the hardness of these problems for $\mathfrak{a} = \langle {x_1}^{r_1-1} + {x_1}^{r_1-2} + \cdots + 1, \ldots, {x_n}^{r_n-1} + {x_n}^{r_n-2} + \cdots + 1 \rangle$. A possible future direction is to determine the hardness of these problems for other choices of $\mathfrak{a}$.

Unlike in the univariate case, here we cannot bound the expansion factor tightly because both the structure of the ideal and the polynomial being reduced have a role to play in the number of iterations in the reduction. In the univariate case an intuition can be given on how to select an ideal with a "small" expansion factor (Lyubashevsky & Micciancio, 2006). It would be an interesting problem to come up with similar observations in the multivariate case. Polynomial computations in the univariate case are well studied and efficient methods using FFT have been proposed. A major challenge for practical implementations using multivariate ideal lattices is coming up with similar efficient methods for multivariate polynomial computations. We also need to study the security issues of multivariate ideal lattices. Another interesting direction is to see if other cryptographic primitives like digital signatures, identification schemes can be built from multivariate ideal lattices.

## Acknowledgments

The authors would like to thank Debarghya Ghoshdastidar for useful discussions on tensor representations of cyclic lattices in the multivariate case.

## References

Ajtai, M. (1996). Generating Hard instances of Lattice Problems (Extended Abstract). In: *Proceedings of the 1996 ACM Symposium on the Theory of Computing, STOC*. ACM.

Bigatti, A., La Scala, R. & Robbiano, L. (1999). Computing Toric Ideals. *Journal of Symbolic Computation* **27**(4), 351 – 365.

Buchberger, B. (1965). *An Algorithm for Finding a Basis for the Residue Class Ring of a Zero-Dimensional Polynomial Ideal (in German)*. Ph.D. thesis, University of Innsbruck, Austria. (reprinted in Buchberger (2006)).

Buchberger, B. (2006). Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. *Journal of Symbolic Computation* **41**, 475–511.

Cohen, H. (2013). *A Course in Computational Algebraic Number Theory*, vol. 138. Springer.

Francis, M. & Dukkipati, A. (2014). On Reduced Gröbner Basis and Macaulay-Buchberger Basis Theorem over Noetherian Rings. *Journal of Symbolic Computation* **65**, 1–14.

Gianni, P., Trager, B. & Zacharias, G. (1988). Grbner Bases and Primary Decomposition of Polynomial Ideals. *Journal of Symbolic Computation* **6**(23), 149 – 167.

Katsabekis, A., Morales, M. & Thoma, A. (2010). Binomial generation of the radical of a lattice ideal. *Journal of Algebra* **324**(6), 1334 – 1346.

Lyubashevsky, V. (2008). Lattice Based Identification Schemes Secure Under Active Attacks. In: *Proceedings of the 11th International Workshop on Practice and Theory in Public Key Cryptography, 2008*, vol. 4939 of *Lecture Notes in Computer Science*. Springer.

Lyubashevsky, V. & Micciancio, D. (2006). Generalized Compact Knapsacks Are Collision Resistant. In: *ICALP (2)*, vol. 4052 of *Lecture Notes in Computer Science*. Springer.

Lyubashevsky, V. & Micciancio, D. (2008). Asymptotically Efficient Lattice-Based Digital Signatures. In: *Theory of Cryptography Conference, 2008*, vol. 4948 of *Lecture Notes in Computer Science*. Springer.

Micciancio, D. (2002). Generalized Compact Knapsacks, Cyclic Lattices, and Efficient One-Way Functions from Worst-Case Complexity Assumptions. In: *Symposium on Foundations of Computer Science (FOCS 2002) Proceedings*. IEEE Computer Society.

Micciancio, D. & Goldwasser, S. (2002). *Complexity of Lattice Problems: a Cryptographic Perspective*, vol. 671 of *The Kluwer International Series in Engineering and Computer Science*. Boston, Massachusetts: Kluwer Academic Publishers.

Micciancio, D. & Regev, O. (2004). Worst-Case to Average-Case Reductions based on Gaussian Measures. In: *45th Symposium on Foundations of Computer Science (FOCS 2004) Proceedings*. IEEE Computer Society.

Pauer, F. (2007). Gröbner Bases with Coefficients in Rings. *Journal of Symbolic Computation* **42**(11-12).

Pukhlikov, A. V. (1998). Birational Automorphisms of Higher-Dimensional Algebraic Varieties. *Doc. Math., J. DMV* , 97–107.

Thieu, V. (2013). *Reduction Modulo Ideals and Multivariate Polynomial Interpolation*. Master's thesis, Université Bordeaux 1 U.F.R. Mathématiques et Informatique.

*E-mail address*: mariaf@csa.iisc.ernet.in, ad@csa.iisc.ernet.in

Department of Computer Science & Automation, Indian Institute of Science, Bangalore - 560012