

EFFICIENT ALGORITHMS FOR FINITE \mathbb{Z} -ALGEBRAS

MARTIN KREUZER AND FLORIAN WALSH

Fakultät für Informatik und Mathematik, Universität Passau, D-94030 Passau, Germany
e-mail address: martin.kreuzer@uni-passau.de

Fakultät für Informatik und Mathematik, Universität Passau, D-94030 Passau, Germany
e-mail address: florian.walsh@uni-passau.de

ABSTRACT. For a finite \mathbb{Z} -algebra R , i.e., for a \mathbb{Z} -algebra which is a finitely generated \mathbb{Z} -module, we assume that R is explicitly given by a system of \mathbb{Z} -module generators G , its relation module $\text{Syz}(G)$, and the structure constants of the multiplication in R . In this setting we develop and analyze efficient algorithms for computing essential information about R . First we provide polynomial time algorithms for solving linear systems of equations over R and for basic ideal-theoretic operations in R . Then we develop ZPP (zero-error probabilistic polynomial time) algorithms to compute the nilradical and the maximal ideals of 0-dimensional affine algebras $K[x_1, \dots, x_n]/I$ with $K = \mathbb{Q}$ or $K = \mathbb{F}_p$. The task of finding the associated primes of a finite \mathbb{Z} -algebra R is reduced to these cases and solved in ZPPIF (ZPP plus one integer factorization). With the same complexity, we calculate the connected components of the set of minimal associated primes $\text{minPrimes}(R)$ and then the primitive idempotents of R . Finally, we prove that knowing an explicit representation of R is polynomial time equivalent to knowing a strong Gröbner basis of an ideal I such that $R = \mathbb{Z}[x_1, \dots, x_n]/I$.

1. INTRODUCTION

Computing the radical and the primary decomposition of an ideal, the associated primes and the primitive idempotents of an algebra, or the connected components of its spectrum, are among the hardest tasks in Computer Algebra. For a finitely generated algebra $R = K[x_1, \dots, x_n]/I$ over a field K with an ideal I that is given by its generators, the usual solutions of these tasks involve computing Gröbner bases and factoring multivariate polynomials over extension fields of K (see for instance [9], [15], [17], [21], [22], [23]).

The difficulty of the problem increases further when we consider algebras over the integers, i.e., algebras of the form $R = \mathbb{Z}[x_1, \dots, x_n]/I$ with an ideal I given by a system of generators. In this case we will also have to factor (potentially large) integers, as already the example $R = \mathbb{Z}/n\mathbb{Z}$ shows. Since the 1970s, various approaches have been taken to tackle these tasks, starting with the case of an algebra R which is a finitely generated \mathbb{Z} -module (see [2], [4], [30], [27]). At the core of most of these algorithms lies the calculation of strong Gröbner bases for ideals in $\mathbb{Z}[x_1, \dots, x_n]$ which tends to be quite demanding. It is

Key words and phrases: Finite \mathbb{Z} -algebra, efficient algorithm, polynomial complexity, primary decomposition, primitive idempotents.

also possible to apply more general algorithms for associative, not necessarily commutative algebras here (see [10], [11], [28]), but we can expect the efficiency of such very general methods to be usually even lower than the ones for commutative algebras.

The situation changes substantially when a \mathbb{Z} -algebra R is *explicitly given*, i.e. a \mathbb{Z} -algebra for which we know a system of generators $G = (g_0, \dots, g_n)$ of its additive group, a system of generators of the \mathbb{Z} -linear relation module $\text{Syz}_{\mathbb{Z}}(G) \subseteq \mathbb{Z}^{n+1}$, and the *structure constants* $c_{ijk} \in \mathbb{Z}$ such that $g_i \cdot g_j = \sum_{k=0}^n c_{ijk} g_k$ for $i, j = 0, \dots, n$.

To define algebras by their module generators and relations, as well as their structure constants, is a very classical approach, followed for instance by Bourbaki in [7], Ch. III, §1, Sect. 7. Knowing the structure constants is equivalent to knowing the multiplication matrices of an algebra. In particular, when the algebra is defined over a field, this point of view is one of the key methods to study 0-dimensional affine algebras and to solve 0-dimensional polynomial systems (see for instance [8] and [23]).

In a recent paper [20], we encountered explicitly given \mathbb{Z} -algebras in a different way: when a non-commutative algebra is given by representing its left and right multiplications via endomorphisms, one can efficiently compute a ring of scalars. As a result, the ring of scalars is an explicitly given, finite commutative \mathbb{Z} -algebra. For further examination of the original rings, it is necessary to find algorithms that perform some of the operations mentioned above on the ring of scalars. In [20] we formulated a few of those algorithms using the calculation of strong Gröbner bases. Here we avoid Gröbner bases and provide precise worst-case complexity bounds which are *almost* polynomial time.

Thus the main task tackled in this paper can be described as follows: assume that a finite \mathbb{Z} -algebra R is given explicitly, i.e., by generators, relations, and structure constants. Develop algorithms for computing their nilradical, associated primes and maximal ideals, primitive idempotents and connected components of $\text{Spec}(R)$ with the lowest possible worst-case complexity. More precisely, we shall show that all these tasks can be solved in ZPPIF, i.e., in zero-error probabilistic polynomial time plus possibly one integer factorization.

Let us discuss the contents of the paper in more detail. Throughout we work with an explicitly given finite \mathbb{Z} -algebra R defined as above. In Section 2 we start by using the well-known facts that the Smith and Hermite normal forms of an integer matrix can be calculated in polynomial time (see [19], [24], [31], [32]), in order to construct a polynomial time algorithm for solving linear systems of equations over R (see Proposition 2.6). Based on this algorithm we perform various operations with ideals in R efficiently, for instance ideal intersections (see Proposition 2.9). Moreover, we are able to compute preimages under the isomorphism given by the Chinese Remainder Theorem (see Proposition 2.10).

In Section 3 we prepare later applications to \mathbb{Z} -algebras by reconsidering and reanalyzing some algorithms for 0-dimensional algebras over a field K . In order to compute the nilradical of an explicitly given K -algebra R , we need to calculate the factorization of univariate polynomials over K . The currently best algorithms have polynomial time complexity (P) in the case $K = \mathbb{Q}$ and zero-error probabilistic polynomial time complexity (ZPP) in the case of a prime field \mathbb{F}_p . Using such polynomial factorization algorithms, Algorithm 3.3 then determines the nilradical of R with these time complexities (P resp. ZPP).

Next we want to compute the primary decomposition of the zero ideal of R . In the case $K = \mathbb{F}_p$, we apply the method of Frobenius spaces (see [23], Alg. 5.2.7) and get an algorithm in ZPP (see Algorithm 3.6). In the case $K = \mathbb{Q}$, we can use the method of [23], Alg. 5.4.2 and get an algorithm in P. Altogether, by applying the primary decomposition algorithms

to $R/\text{Rad}(0)$, we are able to find the maximal ideals of R in P and ZPP for $K = \mathbb{Q}$ and $K = \mathbb{F}_p$, respectively (see Corollary 3.8).

In Section 4 we then use the ideas of [27] to compute the associated primes of an explicitly given finite \mathbb{Z} -algebra R (see Algorithm 4.2). The method is to distinguish between the prime ideals which contain an integer prime number and those which don't. In both cases the computation is reduced to the setting of the preceding section, i.e., to computations of 0-dimensional algebras over fields. Since the determination of associated primes may involve the factorization of an integer, the best time complexity we can achieve here is ZPPIF, i.e., ZPP plus one integer factorization. More precisely, the integer which has to be factored is the torsion exponent of the additive group of R .

In Section 5 we treat the next topics, namely the computation of the primitive idempotents of an explicitly given finite \mathbb{Z} -algebra R and the connected components of its prime spectrum. It turns out that it is advisable to solve the latter task first. More precisely, since R may have infinitely many prime ideals, we compute the connected components of the set of minimal associated primes $\text{minPrimes}(R)$ in Algorithm 5.6. This algorithm uses the results of the preceding section, whence its worst-case time complexity is in ZPPIF. Finally, we calculate the primitive idempotents of R in Algorithm 5.8 by lifting them from the primitive idempotents of $R/\text{Rad}(0)$. This lifting process is performed using Algorithm 5.1. Once again the worst-case time complexity is in ZPPIF.

In the last section we connect the method of using an explicit representation of R to the more traditional method of calculating a strong Gröbner basis, when R is given as $R = P/I$ with $P = \mathbb{Z}[x_1, \dots, x_n]$ and an ideal I in P whose generators are known. Starting with an explicitly given finite \mathbb{Z} -algebra R , we can compute in polynomial time a strong Gröbner basis of a defining ideal I of R (see Corollary 6.5). For this direction we use a generalization of the Buchberger-Möller Algorithm (see Algorithm 6.3). Conversely, starting with a strong Gröbner basis of I , we can calculate an explicit representation of R in polynomial time (see Algorithm 6.7). For this direction, we use a generalization of Macaulay's Basis Theorem to finite \mathbb{Z} -algebras (see Proposition 6.6).

For the notation and basic definitions we adhere to conventions in [21] and [22]. All algorithms in this paper were implemented in the computer algebra system ApCoCoA (see [3]) and are available from the authors upon request. These implementations were used to calculate the examples given in the various sections.

2. POLYNOMIAL TIME COMPUTATIONS IN FINITE \mathbb{Z} -ALGEBRAS

Let R be a finite \mathbb{Z} -algebra, i.e., a \mathbb{Z} -algebra which is a finitely generated \mathbb{Z} -module. We denote the additive group of R by R^+ . In this section we collect operations in R which can be computed in polynomial time if a presentation of R is given as below.

Remark 2.1. (Explicitly Given \mathbb{Z} -Algebras)

Subsequently we assume that a \mathbb{Z} -algebra R is given by the following information.

- (a) A set of generators $\mathcal{G} = \{g_0, \dots, g_n\}$ of the \mathbb{Z} -module R^+ , together with a matrix $A = (a_{\ell k}) \in \text{Mat}_{m, n+1}(\mathbb{Z})$ whose rows generate the syzygy module $\text{Syz}_{\mathbb{Z}}(\mathcal{G})$ of \mathcal{G} .
- (b) Structure constants c_{ijk} such that $g_i g_j = \sum_{k=0}^n c_{ijk} g_k$ for $i, j = 0, \dots, n$.

Notice that we can assume that $g_0 = 1$, and encode this information as an ideal

$$I = \langle x_i x_j - \sum_{k=0}^n c_{ijk} x_k, \sum_{k=0}^n a_{\ell k} g_k \mid i, j = 1, \dots, n, \ell = 1, \dots, m \rangle$$

in $P = \mathbb{Z}[x_1, \dots, x_n]$ such that $R \cong P/I$. If R is given as above, we call it an **explicitly given \mathbb{Z} -algebra**.

The bit complexity of the matrix A in (a) which defines the \mathbb{Z} -module structure of R^+ is given by

$$\beta = (n+1)m \log_2(\|A\|) \quad \text{with} \quad \|A\| = \max\{|a_{\ell k}|\}.$$

The bit complexity of the entire input defining the \mathbb{Z} -algebra R is then given by

$$\gamma = ((n+1)^3 + (n+1)m) \log_2(M) \quad \text{with} \quad M = \max\{|a_{\ell k}|, |c_{ijk}|\}.$$

In this section we collect computations in R which can be performed in polynomial time in β or γ , respectively. More precisely, we will use the following complexity classes.

Definition 2.2. (Polynomial Time Complexity Classes)

Consider an algorithm which takes a tuple of integers as input.

- (a) The algorithm is in the complexity class **P (polynomial time)** if its running time is bounded by a polynomial expression in the bit complexity of the input.
- (b) The algorithm is in the complexity class **ZPP (zero-error probabilistic polynomial time)** if it is a Las Vegas algorithm which has polynomial running time in the bit complexity of the input.
- (c) The algorithm is in the complexity class **ZPPIF (zero-error probabilistic polynomial time plus integer factorization)** if, except for the factorization of one integer, the algorithm is in ZPP and the bit size of the integer to be factored is bounded by a polynomial expression in the bit complexity of the input.

It is useful to bring the \mathbb{Z} -module presentation of R^+ into a normal form.

Remark 2.3. Let $A = (a_{ij}) \in \text{Mat}_{m,n+1}(\mathbb{Z})$ be the matrix whose rows are given by the generators of $\text{Syz}(\mathcal{G})$. Then there exist unimodular transformation matrices $S \in \text{Mat}_{m,m}(\mathbb{Z})$ and $T \in \text{Mat}_{n+1,n+1}(\mathbb{Z})$ such that

$$S \cdot A \cdot T = \begin{pmatrix} k_1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & & \vdots \\ \vdots & \ddots & k_u & \ddots & & \vdots \\ \vdots & & \ddots & 0 & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & 0 \end{pmatrix}$$

and k_i divides k_j for $i < j$. This matrix is called the **Smith normal form** of A . It yields the following isomorphism:

$$R^+ \cong \mathbb{Z}^r \oplus \mathbb{Z}/k_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/k_u\mathbb{Z}.$$

The numbers r and k_1, \dots, k_u are uniquely determined by R^+ . We call r the **rank** and k_1, \dots, k_u the **invariant factors** of R^+ . The largest invariant factor k_u is the exponent of the torsion subgroup of R^+ . We call it the **torsion exponent** τ of R^+ .

In the following we shall show that certain algorithms run in polynomial time by reducing them to the following computations.

Remark 2.4. (Complexity of Integer Linear Algebra Operations)

- (a) The Smith and the Hermite normal form of a matrix $A \in \text{Mat}_{m,n}(\mathbb{Z})$ can be computed in polynomial time, as first shown by Kannan and Bachem [19] in 1979. Currently, the fastest deterministic algorithm for computing the Smith normal form is the one developed by Storjohann [31]. Note that in contrast to [19] this algorithm does not produce the unimodular transformation matrices.
- (b) Solving linear systems of equations over the integers can be reduced to computing a Smith normal form together with the unimodular transformation matrices (see for instance [24]). If the linear system is of the form $Ax = b$ where $A \in \text{Mat}_{m,n}(\mathbb{Z})$ and $b \in \text{Mat}_{n,1}(\mathbb{Z})$, then generators of the solution space can be computed in polynomial time in n , m , $\|A\|$, $\|b\|$ and the rank of A . Here $\|A\|$ denotes the maximal absolute value of the entries of A . A concrete complexity bound is given in [32], Theorem 19.
- (c) Computing the intersection of free submodules of \mathbb{Z}^n can be achieved by computing a basis of the solution space of an appropriate linear system of equations. The problem therefore reduces to (b).

Since the Smith normal form can be computed in polynomial time, it follows that the bit complexity of the torsion exponent of R is bounded by a polynomial in β . Below we give a concrete complexity bound.

Lemma 2.5. *Let R be an explicitly given finite \mathbb{Z} -algebra. Then the bit complexity of the torsion exponent τ is bounded by $n \log_2(n \|A\|)$.*

Proof. The product of the invariant factors of R^+ is given by the gcd of all maximal rank minors of A . The torsion exponent is therefore bounded by the absolute value of a non-zero maximal rank minor of A . Hadamard's inequality then yields $\tau \leq n^{n/2} \|A\|$, which means the bit complexity of τ is bounded by $n \log_2(n \|A\|)$. \square

Solving a linear system of equations over R can be reduced to solving a linear system over the integers.

Proposition 2.6. (Solving Systems of Linear Equations over R)

Let R be an explicitly given finite \mathbb{Z} -algebra and $f_1, \dots, f_p \in R$. For $k = 1, \dots, p$, we write $f_k = b_{k0}g_0 + \dots + b_{kn}g_n$ with $b_{kj} \in \mathbb{Z}$. Let y_1, \dots, y_p be further indeterminates. Consider the following homogeneous linear equation over R .

$$f_1 y_1 + \dots + f_p y_p = 0 \tag{i}$$

Let $e_0, \dots, e_n \in \mathbb{Z}^{n+1}$ be the standard basis vectors. For the following system of homogeneous linear equations in the indeterminates z_{ki} and w_j over \mathbb{Z} , let \mathcal{L} be the projection of the solution space onto the z -coordinates.

$$\sum_{k=1}^p \sum_{i,j,\ell=0}^n z_{ki} b_{kj} c_{ij\ell} e_\ell - \sum_{j=1}^p \sum_{i=0}^n w_j a_{ij} e_i = 0 \tag{ii}$$

Then the following conditions are equivalent.

- (a) A tuple $(h_1, \dots, h_p) \in R^p$ with $h_k = d_{k0}g_0 + \dots + d_{kn}g_n \in R$ and $d_{ki} \in \mathbb{Z}$ is a solution of (i).
- (b) The tuple (d_{ki}) is an element of \mathcal{L} .

Proof. The tuple (h_1, \dots, h_p) is a solution of (i) if and only if

$$\sum_{k=1}^p \sum_{i,j=0}^n b_{ki} d_{kj} g_i g_j = 0.$$

This is the case if and only if there exist $\alpha_1, \dots, \alpha_m \in \mathbb{Z}$ such that the left hand side is equal to $\sum_{j=1}^m \sum_{i=1}^n \alpha_j a_{ij} g_i$. The claim then follows by rewriting the products $g_i g_j$ using the structure constants of R and applying the canonical isomorphism $R \cong \mathbb{Z}^{n+1} / \text{Syz}(G)$. \square

Let us illustrate this proposition with an example.

Example 2.7. Let R be the finite \mathbb{Z} -algebra generated by $\mathcal{G} = \{g_1, g_2, g_3\}$, where $\text{Syz}(\mathcal{G}) = \langle (3, 0, 0), (-1, 0, 4) \rangle$, and where the multiplication in R is commutative and given by $g_1^2 = 3g_1$, $g_1 g_3 = 2g_2$, $g_2^2 = g_1 + g_2$, and $g_i g_j = 0$ for all other combinations. Consider the homogeneous linear equation

$$(2g_3)x_1 + (g_1 + g_3)x_2 + (2g_1)x_3 = 0$$

over R . Every solution is of the form $(h_1, h_2, h_3) \in R^3$ with $h_i = d_{i1}g_1 + d_{i2}g_2 + d_{i3}g_3$, where $d_{ij} \in \mathbb{Z}$. To compute generators of the solution space $\mathcal{L} \subseteq R^3$, we follow Proposition 2.6 and substitute x_i by h_i . Using the structure constants, we then replace products $g_i g_j$ by \mathbb{Z} -linear combinations of the generators and obtain the system of equations

$$\begin{aligned} 4d_{11}g_2 &= 0 \\ 3d_{21}g_1 + 2d_{23}g_2 + 2d_{21}g_2 &= 0 \\ 6d_{31}g_1 + 4d_{33}g_2 &= 0. \end{aligned}$$

By substituting g_i with e_i and taking into account the generators of $\text{Syz}(\mathcal{G})$, we obtain a system of linear equations over \mathbb{Z} which is given by the following matrix.

$$\begin{pmatrix} 0 & 0 & 0 & 3 & 0 & 0 & 6 & 0 & 0 & 3 & -1 \\ 4 & 0 & 0 & 2 & 0 & 2 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 \end{pmatrix}$$

After projecting onto the first nine components of its solution space we obtain for example the tuple $(0, 0, 0, 1, 0, 1, 0, 0, -1) \in \mathbb{Z}^9$ which corresponds to the tuple $(0, g_1 + g_2, -g_3) \in R^3$. The whole solution space in R^3 is generated by this tuple together with seven further tuples.

Proposition 2.6 yields the following complexity bound for solving linear equations.

Corollary 2.8. *Let R be an explicitly given finite \mathbb{Z} -algebra. Generators of the solution space of a linear equation over R as in Proposition 2.6 can be computed in polynomial time in the bit complexity of the input which is given by γ (for R) and by $p(n+1)\log_2(M)$ where $M = \max\{b_{kj}\}$ (for the elements f_1, \dots, f_p).*

Proof. The coefficients in the system of equations (ii) in Proposition 2.6 are b_{kj} , c_{ijl} and a_{ij} . The claim therefore follows immediately from Remark 2.4.b. \square

The next proposition collects elementary operations in an explicitly given finite \mathbb{Z} -algebra which can be performed in polynomial time.

Proposition 2.9. (Elementary Ideal-Theoretic Operations)

Let R be an explicitly given finite \mathbb{Z} -algebra, and let $J = \langle f_1, \dots, f_k \rangle$ as well as $J' = \langle h_1, \dots, h_\ell \rangle$ be ideals in R . We assume that the elements $f_i, h_j \in R$ are given as elements in $\mathbb{Z}[g_0, \dots, g_n]$ and that the bit complexity of these sets of polynomials is given by δ_J and $\delta_{J'}$, respectively.

- (a) The rank and the invariant factors of R^+ can be computed in polynomial time in β .
- (b) Let $\bar{\mathcal{G}} = \{\bar{g}_0, \dots, \bar{g}_n\}$ be the set of residue classes in R/J of the elements of \mathcal{G} . Then generators of $\text{Syz}_{\mathbb{Z}}(\bar{\mathcal{G}})$ can be computed in polynomial time in $\gamma + \delta_J$.
- (c) We can decide whether $J \subseteq J'$ in polynomial time in $\gamma + \delta_J + \delta_{J'}$.
- (d) We can decide whether $J = \langle 1 \rangle$ in polynomial time in $\gamma + \delta_J$.
- (e) Generators of the intersection $J \cap J'$ can be computed in polynomial time in $\gamma + \delta_J + \delta_{J'}$.

Proof. To prove (a), let $A = (a_{ij}) \in \text{Mat}_{n+1,m}(\mathbb{Z})$ be the matrix whose rows are given by the generators of $\text{Syz}_{\mathbb{Z}}(\mathcal{G})$. The rank and the invariant factors of R^+ can be determined from the Smith normal form of A , which can be computed in polynomial time by Remark 2.4.

Next we show (b). Using the structure constants, we can rewrite the f_i as linear combinations $b_{i0}g_0 + \dots + b_{in}g_n$ of the generators of R^+ . This means that we obtain integer tuples $v_1, \dots, v_r \in \mathbb{Z}^{n+1}$ with $v_i = (b_{i0}, \dots, b_{in})$ such that v_1, \dots, v_r together with the generators of $\text{Syz}_{\mathbb{Z}}(\mathcal{G})$ generate $\text{Syz}_{\mathbb{Z}}(\bar{\mathcal{G}})$.

Using (b), we can compute presentations $R/J \cong \mathbb{Z}^{n+1}/V_1$ and $R/J' \cong \mathbb{Z}^{n+1}/V_2$, where V_1 and V_2 are submodules of \mathbb{Z}^{n+1} , in polynomial time. The ideal J is then contained in J' if and only if $V_1 \subseteq V_2$. This proves (c).

To show (d), we use part (b) to compute a presentation $R/J \cong \mathbb{Z}^{n+1}/\text{Syz}_{\mathbb{Z}}(\bar{\mathcal{G}})$. We can then apply (a) and compute the rank and the invariant factors of R/J in polynomial time. Notice that we have $J = \langle 1 \rangle$ if and only if the rank of R/J is zero and all invariant factors are equal to one.

For the proof of (e), we let

$$\mathcal{M} = \begin{pmatrix} 1 & f_1 & \cdots & f_k & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 & h_1 & \cdots & h_\ell \end{pmatrix}.$$

Generators of $\text{Syz}_R(\mathcal{M})$ can be computed in polynomial time by solving an appropriate linear system of equations over R using Proposition 2.6. The first non-zero coordinates of the generators then generate $J \cap J'$ by [21], Proposition 3.2.3. \square

The following algorithm will come in handy when we compute the primitive idempotents of a finite \mathbb{Z} -algebra.

Algorithm 2.10. (The Chinese Remainder Preimage Algorithm)

Let R be an explicitly given finite \mathbb{Z} -algebra. In particular, we assume that R^+ is generated by $\mathcal{G} = \{g_0, \dots, g_n\}$ with $g_0 = 1$. Let J_1, \dots, J_s be pairwise comaximal ideals in R , and assume that $J_1 \cap \dots \cap J_s = \langle 0 \rangle$. Given $i \in \{1, \dots, s\}$, consider the following sequence of instructions.

- (1) Using Proposition 2.9.b, compute \mathbb{Z} -submodules $V_j \subseteq \mathbb{Z}^{n+1}$ such that we have $R/J_j \cong \mathbb{Z}^{n+1}/V_j$ for $j = 1, \dots, s$.
- (2) Compute a \mathbb{Z} -module basis $\{v_1, \dots, v_k\} \subseteq \mathbb{Z}^{n+1}$ of $\bigcap_{j \neq i} V_j$.
- (3) Let $\{w_1, \dots, w_\ell\} \subseteq \mathbb{Z}^{n+1}$ be a \mathbb{Z} -basis of V_i . Compute a solution $(c_i) \in \mathbb{Z}^{k+\ell}$ of the linear system of equations in the indeterminates $y_1, \dots, y_{k+\ell}$ given by

$$v_1 y_1 + \dots + v_k y_k = w_1 y_{k+1} + \dots + w_\ell y_{k+\ell} + (1, 0, \dots, 0).$$

- (4) Let $h = (h_0, \dots, h_n) = c_1 v_1 + \dots + c_k v_k \in \mathbb{Z}^{n+1}$. Return the element $f = h_0 g_0 + \dots + h_n g_n$ of R and stop.

This is a polynomial time algorithm which computes an element $f \in R$ such that f is mapped to the i -th canonical basis vector e_i under the canonical \mathbb{Z} -linear map

$$\varphi: R \longrightarrow R/J_1 \times \cdots \times R/J_s.$$

Proof. The tuple h satisfies $h \in \bigcap_{j \neq i} V_j$ and $h - (1, 0, \dots, 0) \in V_i$. This shows that the residue class of h in $\mathbb{Z}^{n+1}/\text{Syz}_{\mathbb{Z}}(\mathcal{G})$ is mapped to e_i under the canonical map $\psi: \mathbb{Z}^{n+1}/\text{Syz}_{\mathbb{Z}}(\mathcal{G}) \longrightarrow \mathbb{Z}^{n+1}/V_1 \times \cdots \times \mathbb{Z}^{n+1}/V_s$. Hence f is mapped to e_i under the map φ . Steps (1) and (2) of the algorithm can be performed in polynomial time by Proposition 2.9. The linear system in Step (3) can also be solved in polynomial time by Remark 2.4. \square

Let us apply this algorithm to a concrete case.

Example 2.11. Consider the finite \mathbb{Z} -algebra $R = \mathbb{Z}[x, y]/\langle x^3 + x^2, 3x^2 + 3x, xy + y, y^2, 2y \rangle$. It is generated as a \mathbb{Z} -module by the elements of $\mathcal{G} = (1, \bar{x}^2, \bar{x}, \bar{y})$, and $\text{Syz}_{\mathbb{Z}}(\mathcal{G})$ is generated by $(0, 0, 0, 2), (0, 3, 3, 0)$. Consider the ideals $J_1 = \langle \bar{y}^2, \bar{x} + 1, 2\bar{y} \rangle$ and $J_2 = \langle \bar{x}^2, 3\bar{x}, \bar{y} \rangle$ in R . Our goal is to compute $f \in R$ such that f is mapped to e_2 under the canonical \mathbb{Z} -linear map $R \rightarrow R/J_1 \times R/J_2$.

- (1) Using Proposition 2.9.b, we find $V_1 = \langle (1, 0, 1, 0), (0, 0, 0, 2), (-1, 1, 0, 0) \rangle$ and $V_2 = \langle (0, 0, 3, 0), (0, 1, 0, 0), (0, 0, 0, 1) \rangle$ such that $R/J_1 \cong \mathbb{Z}^4/V_1$ and $R/J_2 \cong \mathbb{Z}^4/V_2$.
- (2) We have $\bigcap_{j \neq 2} V_j = V_1$.
- (3) A solution of the linear system

$$\begin{pmatrix} 1 & 0 & -1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & -3 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_7 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

is given by $(3, 0, 2, 1, 2, 0) \in \mathbb{Z}^6$.

- (4) This solution yields the tuple $h = (1, 2, 3, 0)$ which corresponds to the element $f = 1 + 3\bar{x} + 2\bar{x}^2$ in R . It is the preimage of e_2 under the canonical map $R \rightarrow R/J_1 \times R/J_2$.

3. COMPUTING THE MAXIMAL IDEALS OF A 0-DIMENSIONAL K -ALGEBRA

In this section we assume that K is either the field of rational numbers \mathbb{Q} or a finite field \mathbb{F}_p . Our goal is to study the complexity of computing the maximal components of a 0-dimensional K -algebra R which is explicitly given in the following sense.

Definition 3.1. A 0-dimensional K -algebra R is **explicitly given** if it is given by a K -vector space basis $\mathcal{B} = \{b_1, \dots, b_n\}$ and structure constants c_{ijk} such that $b_i b_j = \sum_{k=1}^n c_{ijk} b_k$ for all $i, j = 1, \dots, n$.

Note that a 0-dimensional K -algebra as in this definition can equivalently be given by a basis together with multiplication matrices. The crucial step in computing the maximal ideals of R is the factorization of univariate polynomials over K .

Remark 3.2. In 1982 Lenstra et al. [26] published a deterministic algorithm for factoring univariate polynomials in $\mathbb{Q}[x]$. The running time of their algorithm is polynomial in $\deg(f)$ and $\log(|f|)$, where for a polynomial $f = \sum_i a_i x^i \in \mathbb{Q}[x]$ we define $|f| = \sqrt{\sum_i a_i^2}$. This means it requires only a polynomial number of bit operations measured in the input size.

For univariate polynomials over finite fields, the situation is slightly more complicated. A deterministic algorithm for factoring polynomials over finite fields was presented by Berlekamp in [5]. Its running time for factoring a polynomial $f \in \mathbb{F}_p$ is polynomial in p and $\deg(f)$. But this is not polynomial in the bit complexity of the input which is given by $(1 + \deg(f)) \log_2(p)$. In 1970 Berlekamp published a Las Vegas algorithm [6] for the problem which has polynomial running time in the input. Since then many new and faster algorithms were developed, see e.g. [16]. But it is still unknown whether the factorization can be performed in deterministic polynomial time. It was shown by Evdokimov [12] that under the generalized Riemann hypothesis (GRH) the problem can be solved in subexponential time. Furthermore, there have been efforts to drop the GHR assumption (see [18]). In addition, there exist deterministic polynomial time algorithms [14, 29] for many special classes of polynomials over finite fields. Indeed, it is conjectured that the set of polynomials which do not satisfy any of the conditions in [29] is empty.

The first step in computing the maximal ideals of R is to compute its nilradical.

Algorithm 3.3. (Computing the Nilradical of a 0-Dimensional Algebra)

Let R be an explicitly given 0-dimensional K -algebra. Consider the following sequence of instructions.

- (1) Let $J = \langle 0 \rangle$ and $\mathcal{B} = \{b_1, \dots, b_n\}$.
- (2) For $i = 1, \dots, n$, perform the following steps (3)-(7).
- (3) Compute the minimal polynomial $\mu_{b_i+J}(z)$ of $b_i + J$ in R/J .
- (4) Calculate $g_i(z) = \text{sqfree}(\mu_{b_i+J}(z))$.
- (5) Replace J with $J + \langle g_i(b_i) \rangle$.
- (6) Using the structure constants, rewrite $g_i(b_i)$ and try to obtain a representation of some $b_j \in \mathcal{B}$ as a linear combination of the remaining elements. If such linear combinations exist remove those elements b_j from \mathcal{B} and update the structure constants to obtain an explicit presentation of R/J .
- (7) If $\deg(g_i(z)) = \dim_K(R/J)$, return the ideal J together with the explicit presentation of R/J and stop.
- (8) Return the ideal J together with the explicit presentation of R/J and stop.

This is an algorithm which computes the nilradical $\text{Rad}(0)$ of R together with an explicit presentation of $R/\text{Rad}(0)$. If $K = \mathbb{Q}$, or if K is a finite prime field, then it has polynomial running time. In particular, the bit complexity of the explicit representation of $R/\text{Rad}(0)$ is polynomially bounded by the bit complexity of the input.

Proof. The correctness of this algorithm is shown in [23] Algorithm 5.4.2. It remains to prove that it runs in polynomial time. The minimal polynomial in step (3) can be computed using [23], Algorithm 1.1.8. It involves finding linear dependencies among the elements $1 + J$, $b_i + J$, \dots , $b_i^d + J$ where $d = \dim_K(R/J)$. Using the structure constants, we rewrite b_i^j for $j = 2, \dots, d$ as linear combinations of the elements of \mathcal{B} . The linear dependencies can then clearly be found in polynomial time. The squarefree part of $g_i(z)$ in step (4) can also be computed in polynomial time (see [17] Section 14.6).

The bit complexity of the presentation of $R/\text{Rad}(0)$ is polynomially bounded by the bit complexity of the input, since during each iteration the bit complexity of the structure constants obtained in step (6) is polynomially bounded by the bit complexity of the structure constants of the previous iteration. \square

The following example illustrates how this algorithm can be applied.

Example 3.4. Consider the zero-dimensional \mathbb{Q} -algebra R with basis $\{1, b_1, b_2, b_3\}$ and multiplication given by $b_1^2 = 2b_1 - 1$, $b_1b_2 = b_3$, $b_1b_3 = 2b_3 - b_1$, $b_2^2 = -b_2 - 1$, $b_2b_3 = -b_3 - b_1$ and $b_3^2 = -2b_3 + b_2 - 2b_1 + 1$.

- (1) We let $J = \langle 0 \rangle$ and $\mathcal{B} = \{b_1, b_2, b_3, 1\}$.
- (3) The minimal polynomial $\mu_{b_1}(z)$ of b_1 is $z^2 - 2z + 1$.
- (4) We calculate $g_1(z) = \text{sqfree}(\mu_{b_1}(z)) = z - 1$.
- (5) We set $J = \langle b_1 - 1 \rangle$.
- (6) Substituting $b_1 = 1$ into $b_1b_2 = b_3$ yields $b_2 = b_3$. Therefore we set $\mathcal{B} = \{b_2, 1\}$ and obtain $\dim_{\mathbb{Q}}(R/J) = 2$.
- (3) The minimal polynomial $\mu_{b_2+J}(z)$ of $b_2 + J$ is $z^2 + z + 1$.
- (4) We calculate $g_2(z) = \text{sqfree}(\mu_{b_2}(z)) = \mu_{b_2}(z)$.
- (5) We set $J = \langle b_1 - 1, b_2^2 + b_2 + 1 \rangle$.
- (6) Rewriting $b_2^2 + b_2 + 1$ using $b_2^2 = -b_2 - 1$, we only obtain the trivial relation given by $0 = 0$. Thus \mathcal{B} is not updated and $\dim_{\mathbb{Q}}(R/J) = 2$.
- (7) Since $\dim_{\mathbb{Q}}(R/J) = 2 = \deg(g_2)$ we return the ideal $J = \langle b_1 - 1, b_2^2 + b_2 + 1 \rangle$ together with the \mathbb{Q} -basis $\{1, \bar{b}_2\}$ of R/J and the structure constant $b_2^2 = -b_2 - 1$.

Having computed the nilradical of R , we can then obtain its maximal ideals as follows. In the case $K = \mathbb{Q}$, we can use Algorithm 7.2 in [25]. It has polynomial running time in the bit complexity of the input. For $K = \mathbb{F}_p$, we can only hope for an algorithm in ZPP since we need to factor univariate polynomials over \mathbb{F}_p . In the more general case of associative algebras over finite fields, the complexity of computing their structure, i.e., their simple components was studied in [13], [28], and [11]. But let us take advantage of the fact that we are in the commutative case and analyze the complexity of the algorithm presented in [23], which was inspired by [15]. In contrast to the methods cited above it has the advantage of being well-suited for an actual implementation.

Definition 3.5. Let R be a 0-dimensional \mathbb{F}_p -algebra.

- (a) The map $\phi_p : R \rightarrow R$ defined by $a \mapsto a^p$ is an \mathbb{F}_p -linear ring endomorphism of R . It is called the **Frobenius endomorphism** of R .
- (b) The \mathbb{F}_p -vector subspace

$$\text{Frob}_p(R) = \{f \in R \mid f^p - f = 0\}$$

of R , i.e., the fixed-point space of R with respect to ϕ_p , is called the **Frobenius space** of R .

In [23], Algorithm 5.2.7, it is explained how one can calculate the Frobenius space of a 0-dimensional \mathbb{F}_p -algebra. Based on this result, we obtain the following algorithm.

Algorithm 3.6. (Primary Decomposition in Characteristic p)

Let R be an explicitly given 0-dimensional \mathbb{F}_p -algebra. In particular, we assume that $\mathcal{B} = \{b_1, \dots, b_n\}$ is a K -vector space basis of R . Consider the following sequence of instructions.

- (1) Form the multiplication matrix $M_{\mathcal{B}}(\phi_p)$ of the Frobenius endomorphism of R , and compute the number $s = n - \text{rank}(M_{\mathcal{B}}(\phi_p) - I_n)$ of primary components of the zero ideal of R . If $s = 1$ then return $\langle 0 \rangle$ and stop.
- (2) Let L be the list consisting of the pair $(\langle 0 \rangle, s)$. Repeat steps (3)–(6) until the second component of all pairs in L is 1. Then return the tuple consisting of all first components of the pairs in L and stop.
- (3) Choose the first pair (J, t) in L for which $t > 1$ and remove it from L .
- (4) Using Algorithm 5.2.7 in [23], compute the Frobenius space of R/J . Choose a non-constant element f in it.
- (5) Calculate the minimal polynomial of the element f and factor it in the form $\mu_f(z) = (z - a_1) \cdots (z - a_u)$ with $a_1, \dots, a_u \in \mathbb{F}_p$.
- (6) For $i = 1, \dots, u$, let $J_i = J + \langle f - a_j \rangle$. Compute the dimension d_i of $\text{Frob}_p(R/J_i)$ and append the pair (J_i, d_i) to L .

This is an algorithm which calculates the list of primary components of the zero ideal of R . It is in ZPP.

Proof. The correctness of this algorithm is shown in [23], Algorithm 5.2.11. In particular, it is proved there that $t = d_1 + \cdots + d_u$ throughout the course of this algorithm. Therefore the number of iterations of steps (3)–(6) is bounded by s which in turn is bounded by the vector space dimension n of R . Algorithm 5.2.7 in step (4) involves computing a basis for the kernel of a matrix over K and can therefore be done in polynomial time. As discussed in the proof of Algorithm 3.3, the minimal polynomial in step (5) can also be computed in polynomial time. Computing its factorization is in ZPP by Remark 3.2. \square

The following example shows this algorithm at work.

Example 3.7. Consider the zero-dimensional \mathbb{F}_2 -algebra R given by an \mathbb{F}_2 -basis $B = \{1, b_1, b_2, b_3\}$ and the multiplication $b_1^2 = b_1$, $b_1 b_2 = b_3$, $b_1 b_3 = b_3$, $b_2^2 = 1$, $b_2 b_3 = b_1$, and $b_3^2 = b_1$.

- (1) The structure constants provide for every $b \in B$ a representation of b^2 in terms of the basis B . This yields the matrix

$$M_{\mathcal{B}}(\phi_2) = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

and we obtain $s = 4 - \text{rank}(M_{\mathcal{B}}(\phi_2) - I_4) = 4 - 2 = 2$ for the number of primary components.

- (2) Let $L = ((\langle 0 \rangle, 2))$.
- (3) Choose the pair $(\langle 0 \rangle, 2)$, and let $L = ()$.
- (4) The kernel of the matrix $M_{\mathcal{B}}(\phi_2) - I_4$ has the basis $\{(1, 0, 0, 0), (0, 1, 0, 0)\}$. Therefore the Frobenius space of R is given by $\langle 1, b_1 \rangle$. We choose $f = b_1$.
- (5) The minimal polynomial of f is given by $\mu_f(z) = z(z + 1)$.
- (6) Let $J_1 = \langle b_1 \rangle$ and $J_2 = \langle b_1 + 1 \rangle$. Using the structure constants we see that the residue classes of $B' = \{1, b_2\}$ in R/J_1 and R/J_2 form a basis of the respective algebras. In both cases we determine $s = 2 - \text{rank}(M_{B'}(\phi_2) - I_2) = 2 - 1 = 1$. Hence we set $L = (J_1, 1), (J_2, 1)$.
- (2) Since the second component of both pairs in L is 1, we return the primary components $\langle b_1 \rangle$ and $\langle b_1 + 1 \rangle$ of the zero ideal of R .

Using this algorithm, we can now calculate the maximal ideals of explicitly given 0-dimensional algebras.

Corollary 3.8. (Complexity of Computing the Maximal Ideals)

Let K be the field of rational numbers or a finite prime field, and let R be an explicitly given 0-dimensional K -algebra.

- (a) If $K = \mathbb{Q}$, then the maximal ideals of R can be computed in polynomial time.
- (b) If $K = \mathbb{F}_p$, then the maximal ideals of R can be computed in ZPP.

Proof. Using Algorithm 3.3, we compute the nilradical $\text{Rad}(0)$ of R in polynomial time. This algorithm also yields an explicit presentation of $R/\text{Rad}(0)$. If $K = \mathbb{Q}$, we then apply Algorithm 7.2 from [25] to $R/\text{Rad}(0)$ and obtain the maximal ideals of R in polynomial time. Similarly, in the case $K = \mathbb{F}_p$, we apply Algorithm 3.6 to $R/\text{Rad}(0)$. \square

For further details and more examples which illustrate the algorithms presented in this section, we refer to Chapter 5 in [23].

4. COMPUTING THE ASSOCIATED PRIMES OF FINITE \mathbb{Z} -ALGEBRAS

In this section we let R be a finite \mathbb{Z} -algebra. We show that the associated primes of R can be computed in ZPIIF, if R is explicitly given. Note that the associated primes of R are given by the primary decomposition of its nilradical $\text{Rad}(0)$. Algorithms for computing the primary decomposition of ideals in $\mathbb{Z}[x_1, \dots, x_n]$ date back to 1978 [4, 30]. More recently, Pfister et al. [27] presented a slightly different approach. Inspired by this algorithm, we gave an efficient algorithm in [20] for computing the primary decomposition of ideals $I \subseteq \mathbb{Z}[x_1, \dots, x_n]$ such that P/I is a finite \mathbb{Z} -algebra. Let us now apply this approach to explicitly given finite \mathbb{Z} -algebras.

The following lemma is used to split the computation into computing the associated primes of 0-dimensional ideals in $\mathbb{Q}[x_1, \dots, x_n]$ and $\mathbb{F}_p[x_1, \dots, x_n]$.

Lemma 4.1. *Let $R = P/I$ be an explicitly given finite \mathbb{Z} -algebra and let τ be its torsion exponent.*

- (a) *The ideal $(I : \langle \tau \rangle)/I$ is the torsion subgroup of R^+ .*
- (b) *We have $I = (I : \langle \tau \rangle) \cap (I + \langle \tau \rangle)$.*
- (c) *If R is finite, then $I \cap \mathbb{Z} = \langle \tau \rangle$.*

Proof. Part (a) follows immediately from the definition of the exponent of the torsion subgroup of R^+ . It then implies $I : \langle \tau \rangle = I : \langle \tau \rangle^\infty$, which means that claim (b) is a standard lemma in commutative algebra. To prove (c), we note that the ring P/I is finite if and only if there exists a positive integer $k \in \mathbb{Z}$ with $I \cap \mathbb{Z} = \langle k \rangle$. If such a number k exists, we have $k \cdot f = 0$ for all $f \in R$, and therefore $\tau \mid k$. But we also have $n \cdot 1 = 0$ in $R = P/I$, and hence $\tau \in I$. This implies $k \mid \tau$, and thus $k = \tau$. \square

The associated primes of R can now be computed as described in the following algorithm.

Algorithm 4.2. (Computing the Associated Primes)

Let $R = P/I$ be an explicitly given finite \mathbb{Z} -algebra. Consider the following sequence of instructions.

- 1: Set $L := []$.

2: Compute the torsion exponent τ of R^+ .
 3: **if** the rank of R is not zero **then**
 4: Compute the prime components $\bar{\mathfrak{p}}_1 \cap \cdots \cap \bar{\mathfrak{p}}_\ell$ of $I\mathbb{Q}[x_1, \dots, x_n]$.
 5: Compute $\bar{\mathfrak{p}}_j \cap P$ and append these ideals to L .
 6: Recursively apply the algorithm to $I + \langle \tau \rangle$ and obtain the set M .
 7: Compute $J := \bigcap_{\mathfrak{p} \in L} \mathfrak{p}$.
 8: Remove all ideals in M that contain J .
 9: **return** $L \cup M$
 10: **else**
 11: Compute all prime factors p_1, \dots, p_r of τ .
 12: Set $M := []$.
 13: **for** $i = 1, \dots, r$ **do**
 14: Compute the prime components $\bar{\mathfrak{p}}_1 \cap \cdots \cap \bar{\mathfrak{p}}_m$ of $I\mathbb{F}_{p_i}[x_1, \dots, x_n]$.
 15: Compute the preimages \mathfrak{p}_j of $\bar{\mathfrak{p}}_j$ in P and append them to M .
 16: **end for**
 17: **return** M
 18: **end if**

This is an algorithm which computes the associated primes $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ of R . It is in ZPPIF.

Proof. The correctness of the algorithm follows from Lemma 4.1 and Proposition 4.7 in [20]. Let us analyze the complexity of each of its steps. The torsion exponent and the rank of R can be computed in polynomial time in β using Proposition 2.9.a, and the bit complexity of the torsion exponent is polynomially bounded by Lemma 2.5. Since P/I is a finite \mathbb{Z} -algebra, the ideals $I\mathbb{Q}[x_1, \dots, x_n]$ and $I\mathbb{F}_p[x_1, \dots, x_n]$ are 0-dimensional and therefore define 0-dimensional \mathbb{Q} - and \mathbb{F}_p -algebras, respectively. Their vector space dimension is less than or equal to the number of generators of R , and their structure constants are given by the structure constants of R . Thus we obtain the maximal components in lines (4) and (14) in polynomial and probabilistic polynomial time, respectively, by applying the algorithms in Section 3. The intersection of the prime ideals in line (7) can be computed in polynomial time by Proposition 2.9.e. Finally, Proposition 2.9.c allows us to check the containment of ideals in line (8) in polynomial time.

In summary, all steps except for the integer prime factorization in line (11) are in ZPP. \square

Note that, since the exponent τ of R is the largest invariant factor of R , all other invariant factors of R are divisors of τ . This means that we might already have a partial factorization of τ . Let us compute the associated primes in a concrete case.

Example 4.3. Consider the finite \mathbb{Z} -algebra R given by the explicit presentation $R = \mathbb{Z}[x, y, z]/I$ with $I = \langle 6z, 6y, x^2 + x - 6, z^2, y^2, xy - y, xz - y, yz \rangle$. We follow the above algorithm and compute the associated primes of R .

- (2) Using Proposition 2.9.a, we find that the torsion exponent of R is 6.
- (4) Since the rank of R is 2, we then compute the minimal associated prime ideals of $I\mathbb{Q}[x, y, z]$ using [23], Alg. 5.4.2 and obtain $\bar{\mathfrak{p}}_1 = \langle z, y, x + 3 \rangle$ as well as $\bar{\mathfrak{p}}_2 = \langle z, y, x - 2 \rangle$.
- (5) Let $\mathfrak{p}_1 = \bar{\mathfrak{p}}_1 \cap P$ and $\mathfrak{p}_2 = \bar{\mathfrak{p}}_2 \cap P$.
- (6) We apply the algorithm recursively to $I + \langle 6 \rangle$.
- (11) Here we calculate the prime factorization $6 = 2 \cdot 3$.
- (14) We determine the minimal associated primes $\bar{\mathfrak{p}}_3 = \langle x + 1, y, z \rangle$ and $\bar{\mathfrak{p}}_4 = \langle x, y, z \rangle$ of $I\mathbb{F}_3[x, y, z]$ using Algorithm 3.6.

- (15) Their canonical liftings are $\mathfrak{p}_3 = \langle x + 1, y, z, 3 \rangle$ and $\mathfrak{p}_4 = \langle x, y, z, 3 \rangle$.
- (14) We determine the minimal associated primes $\bar{\mathfrak{p}}_5 = \langle x + 1, y, z \rangle$ and $\bar{\mathfrak{p}}_6 = \langle x, y, z \rangle$ of $\mathbb{F}_2[x, y, z]$ using Algorithm 3.6.
- (15) Their canonical liftings are $\mathfrak{p}_5 = \langle x + 1, y, z, 2 \rangle$ and $\mathfrak{p}_6 = \langle x, y, z, 2 \rangle$.
- (7) We compute $J = \mathfrak{p}_1 \cap \mathfrak{p}_2 = \langle z, y, x^2 + x - 6 \rangle$.
- (8) The ideal J is contained in $\mathfrak{p}_3, \mathfrak{p}_4, \mathfrak{p}_5,$ and \mathfrak{p}_6 .
- (9) The minimal associated prime ideals of R are given by \mathfrak{p}_1 and \mathfrak{p}_2 .

5. COMPUTING PRIMITIVE IDEMPOTENTS

In this section our goal is to compute the primitive idempotents of an explicitly given finite \mathbb{Z} -algebra R . We describe a variant of the method presented in Section 4 of [20] and analyze its complexity. We will use the fact that the idempotents modulo a nilpotent ideal can be lifted. The following algorithm is based on Lemma 3.2.1 in [10].

Algorithm 5.1. (Lifting Idempotents)

Let R be an explicitly given finite \mathbb{Z} -algebra, and let $\text{Rad}(0) \subseteq R$ be its nilradical. Let $e \in R$ be such that $e^2 \equiv e \pmod{\text{Rad}(0)}$. Consider the following instructions.

- (1) Set $h = e$.
- (2) Compute $f = h + r - 2hr$ where $r = h^2 - h$.
- (3) Represent $f^2 - f$ as a \mathbb{Z} -linear combination $f^2 - f = c_0g_0 + \dots + c_n g_n$ using the structure constants.
- (4) If $(c_0, \dots, c_n) \in \text{Syz}_{\mathbb{Z}}(\mathcal{G})$, return f and stop. Otherwise set $h = f$ and continue with step (2).

This is an algorithm which computes an idempotent $f \in R$ such that $f \equiv e \pmod{\text{Rad}(0)}$. Furthermore, if e is a primitive idempotent modulo $\text{Rad}(0)$, then f is a primitive idempotent in R .

Proof. The algorithm terminates since $\text{Rad}(0)$ is a nilpotent ideal. To prove the correctness, we show that if h is an idempotent modulo $\text{Rad}(0)^{2^k}$, then f is an idempotent modulo $\text{Rad}(0)^{2^{k+1}}$. By assumption, we have $h^2 - h \in \text{Rad}(0)^{2^k}$, and therefore $h^2r - hr = (h^2 - h)r = r^2 \in \text{Rad}(0)^{2^{k+1}}$. Then we get

$$f^2 \equiv h^2 + 2hr - 4h^2r \equiv h + r + 2hr - 4hr \equiv f \pmod{\text{Rad}(0)^{2^{k+1}}}$$

and $f \equiv h \pmod{\text{Rad}(0)^{2^k}}$. Now assume that $e \pmod{\text{Rad}(0)}$ is a primitive idempotent and that $f = e' + e''$ can be written as the sum of two orthogonal idempotents. Then we have $e' \in \text{Rad}(0)$ or $e'' \in \text{Rad}(0)$, since e is primitive. But $\text{Rad}(0)$ consists only of nilpotent elements. Therefore e' or e'' has to be zero. \square

Let us apply this algorithm to an example.

Example 5.2. Consider the finite \mathbb{Z} -algebra R generated by $\mathcal{G} = \{1, g_1, \dots, g_5\}$ with relation ideal $\langle 6, 3g_1, 3g_2, 3g_3 \rangle$. The non-trivial structure constants are given by $g_4^2 = g_5, g_5^2 = g_4$ and $g_4g_5 = 1$. We have $\text{Rad}(0) = \langle 6, 2g_5 - 2, g_2 + 2, g_2 - g_3 \rangle$, and the residue class of $e = g_4 + g_5 + 1$ in $R/\text{Rad}(0)$ is a primitive idempotent. We apply Algorithm 5.1 to lift e to an idempotent of R .

- (1) We set $h = e$.
- (2) We compute $r = h^2 - h = 2g_4 + 2g_5 + 2$ and $f = h + r - 2hr = -3g_4 - 3g_5 - 3$.
- (3) Using the structure constants, we calculate $f^2 - f = 30g_4 + 30g_5 + 30$.
- (4) Since $(30, 0, 0, 0, 30, 30) \in \text{Syz}_{\mathbb{Z}}(\mathcal{G})$, we return the primitive idempotent f .

The number of iterations in Algorithm 5.1 necessary to lift the idempotents can be bounded as follows.

Proposition 5.3. *Let R be a finite \mathbb{Z} -algebra of rank r , and let T be the torsion subgroup of R^+ .*

- (a) *We have $\text{Rad}(0)^m = \{0\}$ for $m = r + \text{length}_{\mathbb{Z}}(T)$.*
- (b) *Let $p_1^{e_1}, \dots, p_s^{e_s}$ be the elementary divisors of R . Then Algorithm 5.1 terminates after at most $\lceil \log_2(r + e_1 + \dots + e_s) \rceil$ steps.*

Proof. To prove (a), note that an element $f \in \text{Rad}(0)$ yields a nilpotent \mathbb{Z} -linear endomorphism φ of R given by multiplication with f . One therefore obtains a chain

$$\text{Ker}(\varphi) \subsetneq \text{Ker}(\varphi^2) \subsetneq \dots \subsetneq R.$$

Now we show that if $\text{rank}(\text{Ker}(\varphi^i)) > 0$, then $\text{rank}(\text{Ker}(\varphi^i)) < \text{rank}(\text{Ker}(\varphi^{i+1}))$. Note that $\text{rank}(\text{Ker}(\varphi^i)) = \text{rank}(\text{Ker}(\varphi^{i+1}))$ if and only if $\text{Ker}(\varphi^{i+1})/\text{Ker}(\varphi^i)$ is a torsion module. Let $\text{Ker}(\varphi^{i+1})/\text{Ker}(\varphi^i)$ be a torsion module. We prove by induction that this implies $\text{Ker}(\varphi^{i+k+1})/\text{Ker}(\varphi^{i+k})$ is a torsion module for all $k \in \mathbb{N}$. For $k = 0$ the claim is true by assumption. Now assume that $\text{Ker}(\varphi^{i+k})/\text{Ker}(\varphi^{i+k-1})$ is a torsion module, and let $x \in \text{Ker}(\varphi^{i+k+1})$. Then we have $\varphi(x) \in \text{Ker}(\varphi^{i+k})$, and there exists a non-zero $c \in \mathbb{Z}$ with $c\varphi(x) \in \text{Ker}(\varphi^{i+k-1})$. Hence we obtain $cx \in \text{Ker}(\varphi^{i+k})$.

Thus we conclude that $\text{Ker}(\varphi^r)$ has rank r , and therefore that $\varphi^r(R)$ is a submodule of T . This forces $\varphi^{r+\text{length}_{\mathbb{Z}}(T)} = 0$.

Part (b) follows immediately from (a), since the length of the torsion is given by the number of elementary divisors $p_i^{e_i}$ counted with multiplicity e_i . \square

In order to compute the primitive idempotents of $R = P/I$, we can now use Algorithm 5.1 to lift the idempotents of $R/\text{Rad}(0)$. For the task of finding the primitive idempotents of $R/\text{Rad}(0)$, we consider the minimal associated primes of I . Let us recall the following remark from [20].

Remark 5.4. Let T be a commutative, unitary, noetherian ring.

- (a) Given an idempotent $e \in T$, the set $\mathcal{V}(1 - e)$ is both open and closed in $\text{Spec}(T)$.
- (b) If $U \subseteq \text{Spec}(T)$ is a subset which is both open and closed, there exists a unique idempotent $e \in T$ such that in $T_{\mathfrak{p}}/\mathfrak{p}T_{\mathfrak{p}}$ we have $\bar{e} = 1$ for $\mathfrak{p} \in U$ and $\bar{e} = 0$ otherwise.
- (c) The correspondence given in (a) and (b) is 1-1. The primitive idempotents correspond uniquely to the connected components of $\text{Spec}(T)$.

Therefore, in order to compute the primitive idempotents of $R/\text{Rad}(0)$, we need to calculate the connected components of $\text{Spec}(R/\text{Rad}(0))$. Since the ring $R/\text{Rad}(0)$ might have infinitely many prime ideals, we use the following approach to describe the connected components of $\text{Spec}(R/\text{Rad}(0))$.

Definition 5.5. Let R be a finite \mathbb{Z} -algebra, and let $\text{minPrimes}(R)$ be the set of minimal associated prime ideals of R . A maximal subset of $\text{minPrimes}(R)$ such that all corresponding prime ideals are part of the same connected component of $\text{Spec}(R)$ is called a **connected component** of $\text{minPrimes}(R)$.

Since R is a finite \mathbb{Z} -algebra, the associated primes of R are either of height n and do not contain a non-zero integer, or they are of height $n + 1$ and hence maximal ideals. Now Algorithm 5.6 determines the connected components of $\text{minPrimes}(R)$.

Algorithm 5.6. (Computing the Connected Components of $\text{minPrimes}(R)$)

Let R be an explicitly given finite \mathbb{Z} -algebra. Consider the following sequence of instructions.

- (1) Compute the set of minimal associated prime ideals of R . Let $\mathfrak{m}_1, \dots, \mathfrak{m}_\ell$ be the minimal associated prime ideals of height $n + 1$, and let $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ be the minimal associated primes ideals of height n .
- (2) Let $M = \{\{\mathfrak{p}_1\}, \dots, \{\mathfrak{p}_m\}\}$.
- (3) While there are sets $C, C' \in M$ such that there exist $\mathfrak{p}_i \in C$ and $\mathfrak{p}_j \in C'$ with $\mathfrak{p}_i + \mathfrak{p}_j \neq \langle 1 \rangle$ replace C and C' in M by $C \cup C'$.
- (4) For every ideal \mathfrak{m}_i , append the set $\{\mathfrak{m}_i\}$ to M .
- (5) Return M .

This is an algorithm which computes a set $M = \{C_1, \dots, C_\nu\}$ such that C_1, \dots, C_ν are the connected components of $\text{minPrimes}(R)$. It is in ZPPIF.

Proof. The following observations show the correctness of this algorithm. An associated prime ideal of height $n + 1$ is maximal and therefore forms its own connected component. Two prime ideals \mathfrak{p}_i and \mathfrak{p}_j of height n belong to the same connected component if and only if there is a maximal ideal \mathfrak{m} containing both \mathfrak{p}_i and \mathfrak{p}_j , which is equivalent to $\mathfrak{p}_i + \mathfrak{p}_j \neq \langle 1 \rangle$.

Let us now show that the algorithm is in ZPPIF. The associated primes of R can be computed in ZPPIF using Algorithm 4.2. Then only two types of computations remain. Namely, we need to decide whether the sum of two primes is equal to $\langle 1 \rangle$ and whether one prime ideal is contained in another. Both of these tasks can be achieved in polynomial time by Proposition 2.9. \square

A more general version of this algorithm which computes the connected components of a set of (non-minimal) associated prime ideals is given in Section 4 of [20].

Example 5.7. Consider the finite \mathbb{Z} -algebra R given by the explicit presentation $R = \mathbb{Z}[x, y]/I$ with $I = \langle x^2 + 5x, xy, y^2 - y, 6y \rangle$. We follow the above algorithm and compute the connected components of $\text{minPrimes}(R)$.

- (1) Algorithm 4.2 yields the minimal associated primes $\mathfrak{m}_1 = \langle \bar{x}, \bar{y} - 1, 3 \rangle$ and $\mathfrak{m}_2 = \langle \bar{x}, \bar{y} + 1, 2 \rangle$ of height 3, as well as and the minimal associated primes $\mathfrak{p}_1 = \langle \bar{x}, \bar{y} \rangle$ and $\mathfrak{p}_2 = \langle \bar{y}, \bar{x} + 5 \rangle$ of height 2.
- (2) We let $M = \{\{\mathfrak{p}_1\}, \{\mathfrak{p}_2\}\}$.
- (3) Since $\mathfrak{p}_1 + \mathfrak{p}_2 = \langle \bar{x}, \bar{y}, 5 \rangle \neq \langle 1 \rangle$, we replace $\{\mathfrak{p}_1\}$ and $\{\mathfrak{p}_2\}$ by $\{\mathfrak{p}_1 + \mathfrak{p}_2\}$ and obtain $M = \{\{\mathfrak{p}_1 + \mathfrak{p}_2\}\}$.
- (4) We add $\{\mathfrak{m}_1\}$ and $\{\mathfrak{m}_2\}$ to M .
- (5) Thus the connected components of $\text{minPrimes}(R)$ are $\{\{\mathfrak{m}_1\}, \{\mathfrak{m}_2\}, \{\mathfrak{p}_1, \mathfrak{p}_2\}\}$.

From the connected components of $\text{minPrimes}(R)$ we can now derive the primitive idempotents of R .

Algorithm 5.8. (Computing the Primitive Idempotents)

Let R be an explicitly given finite \mathbb{Z} -algebra. The following steps define an algorithm which computes the primitive idempotents of R in ZPPIF.

- (1) Compute the connected components C_1, \dots, C_ν of $\text{minPrimes}(R)$ using Alg. 5.6.

- (2) Compute $J = \bigcap_{\mathfrak{p} \in \text{minPrimes}(R)} \mathfrak{p}$.
- (3) For $i = 1, \dots, \nu$, compute $J_i = \bigcap_{\mathfrak{p} \in C_i} \mathfrak{p}$.
- (4) Compute the preimages q_1, \dots, q_ν of e_1, \dots, e_ν under the canonical \mathbb{Z} -linear map $R/J \rightarrow R/J_1 \times \dots \times R/J_\nu$.
- (5) Using Algorithm 5.1, lift the idempotents q_1, \dots, q_ν of R/J to idempotents of R and return them.

Proof. For a proof of the correctness of this algorithm, we again refer to Section 4 of [20]. Let us analyze the complexity of this algorithm. Step (1) can be performed in ZPPIF using Algorithm 5.6. The remaining steps can be performed in polynomial time by Proposition 2.9, Algorithm 2.10, and Algorithm 5.1. The number of iterations necessary to perform Algorithm 5.1 has a polynomial bound by Proposition 5.3. \square

Example 5.9. Let us continue Example 5.7 and compute the primitive idempotents of the finite \mathbb{Z} -algebra $\mathbb{Z}[x, y]/I$ with $I = \langle x^2 + 5x, xy, y^2 - y, 6y \rangle$.

- (1) Using Algorithm 5.6, we already computed the connected components $\{\mathfrak{m}_1\}$, $\{\mathfrak{m}_2\}$, and $\{\mathfrak{p}_1, \mathfrak{p}_2\}$ of $\text{minPrimes}(R)$ in Example 5.7.
- (2) Using Proposition 2.9.e, we calculate $J = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}_1 \cap \mathfrak{m}_2 = I$.
- (3) Using Proposition 2.9.e, we compute $\mathfrak{p}_1 \cap \mathfrak{p}_2 = \langle \bar{y}, \bar{x}^2 + 5\bar{x} \rangle$.
- (4) We apply Algorithm 2.10 to the \mathbb{Z} -linear map $R/I \rightarrow R/(\mathfrak{p}_1 \cap \mathfrak{p}_2) \times R/\mathfrak{m}_1 \times R/\mathfrak{m}_2$ and obtain the preimages $\bar{y} + 1, 3\bar{y}, -2\bar{y}$ of e_1, e_2, e_3 .
- (5) Since $I = J$, we do not need to lift the idempotents. Thus we return the primitive idempotents $\bar{y} + 1, 3\bar{y}, -2\bar{y}$ of R .

6. EXPLICIT \mathbb{Z} -ALGEBRA PRESENTATIONS AND STRONG GRÖBNER BASES

In the previous sections we made the assumption that a \mathbb{Z} -algebra is explicitly given, i.e., given by \mathbb{Z} -module generators, their linear relations, and structure constants. This information can be encoded in an ideal $I \subseteq P = \mathbb{Z}[x_1, \dots, x_n]$ such that $R = P/I$. More precisely, let

$$I = \langle x_i x_j - \sum_{k=0}^n c_{ijk} x_k, \sum_{k=0}^n a_{\ell k} g_k \mid i, j = 1, \dots, n, \ell = 1, \dots, m \rangle \quad (*)$$

be the ideal in $P = \mathbb{Z}[x_1, \dots, x_n]$ encoding the information of an explicitly given \mathbb{Z} -algebra $R = P/I$ as in Remark 2.1.

In this section we show that this representation of R is polynomial time equivalent to computing a strong Gröbner basis of I . This notion is defined as follows.

Definition 6.1. Let I be an ideal in $P = \mathbb{Z}[x_1, \dots, x_n]$, and let σ be a term ordering on \mathbb{T}^n . A set of polynomials $G = \{g_1, \dots, g_r\}$ in I is called a **strong σ -Gröbner basis** of I if, for every polynomial $f \in I \setminus \{0\}$, there exists an index $i \in \{1, \dots, r\}$ such that $\text{LM}_\sigma(f)$ is a multiple of $\text{LM}_\sigma(g_i)$.

In the first subsection we show that a presentation $R = P/I$ with I as above allows us to compute a strong Gröbner basis of I in polynomial time. In the second subsection we prove that, conversely, if $R = P/I$ and we know a strong Gröbner basis of I , then we can calculate a presentation as in Remark 2.1 in polynomial time.

6.1. Computing a Strong Gröbner Basis of an Explicitly Given \mathbb{Z} -Algebra. Let us begin with the task of computing a strong Gröbner basis for an ideal I as above. More generally, consider the following situation. Let $P = \mathbb{Z}[x_1, \dots, x_n]$, and let $I_1, \dots, I_s \subseteq P$ be ideals such that P/I_j is a finite \mathbb{Z} -algebra for $j = 1, \dots, s$. Our goal is to compute a strong Gröbner basis of their intersection $I_1 \cap \dots \cap I_s$. For 0-dimensional ideals in a polynomial ring over a field, an intersection like this can be computed using the generalized Buchberger-Möller algorithm (see [1]). In the following we extend this algorithm to ideals in $\mathbb{Z}[x_1, \dots, x_n]$.

Before formulating this generalization, we need to address the task of representing the residue classes in P/I_j using suitable systems of generators.

Remark 6.2. Let I be an ideal in P such that P/I is a finite \mathbb{Z} -algebra, and let $\pi : P \rightarrow P/I$ be the canonical epimorphism. We need to be able to express the image $\pi(f)$ of an element $f \in P$ as a linear combination of some system of \mathbb{Z} -module generators of P/I .

Let (t_1, \dots, t_μ) be a tuple of terms such that $\bar{\mathcal{O}} = (\bar{t}_1, \dots, \bar{t}_\mu)$ generates P/I as a \mathbb{Z} -module. Then a tuple $(a_1, \dots, a_\mu) \in \mathbb{Z}^\mu$ such that $\pi(f) = a_1 \bar{t}_1 + \dots + a_\mu \bar{t}_\mu$ is called a **representation vector** of f with respect to \mathcal{O} . Representation vectors are in general not unique, but can be calculated efficiently in several settings.

- (a) If I is given as in (*) and $f \in P$, we can replace products $x_i x_j$ in f repeatedly by linear combinations $\sum_{k=0}^n c_{ijk} x_k$ until the resulting polynomial g is linear. Then $\pi(f) = \pi(g)$ is a \mathbb{Z} -linear combination of the residue classes of the terms in $\{1, x_1, \dots, x_n\}$.
- (b) If I is given by a strong Gröbner basis with respect to a term ordering σ , we can use $\mathcal{O}_\sigma(I) = \mathbb{T}^n \setminus L$, where $L = \{m \in \text{LM}_\sigma(I) \mid \text{LC}_\sigma(m) = 1\}$, and represent $\pi(f)$ for an element $f \in P$ by the residue class of its normal form $\text{NF}_{\sigma, I}(f)$ which is a \mathbb{Z} -linear combination of the terms in $\mathcal{O}_\sigma(I)$.

In either case, if we have an implementation of a function that represents $\pi(f)$ for every polynomial $f \in P$ in the form $\pi(f) = a_1 \bar{t}_1 + \dots + a_\mu \bar{t}_\mu$ then we write $\text{RV}_{\mathcal{O}}(f) = (a_1, \dots, a_\mu)$ for the corresponding representation vector.

Now we can formulate the generalized Buchberger-Möller algorithm for ideals in $P = \mathbb{Z}[x_1, \dots, x_n]$.

Algorithm 6.3. (Intersecting Ideals in $\mathbb{Z}[x_1, \dots, x_n]$)

For $i = 1, \dots, s$, let I_1, \dots, I_s be ideals in P such that P/I_i is a finite \mathbb{Z} -algebra, and let $\mathcal{O}_i = \{t_{i1}, \dots, t_{i\mu_i}\} \subseteq \mathbb{T}^n$ be a set of μ_i terms such that their residue classes generate P/I_i as a \mathbb{Z} -module. Furthermore, we assume that a \mathbb{Z} -submodule U_i of \mathbb{Z}^{μ_i} is given such that the \mathbb{Z} -linear map $P/I_i \rightarrow \mathbb{Z}^{\mu_i}/U_i$ defined by $\bar{t}_{ij} \mapsto \bar{e}_i$ is an isomorphism. Finally, let σ be a degree compatible term ordering on \mathbb{T}^n . Consider the following instructions.

- (1) Start with empty lists $G = []$, $\mathcal{O} = []$, $M = []$, and a list $L = [1]$.
- (2) Let $N = \{n_1, \dots, n_k\} \subseteq \mathbb{Z}^\mu$ such that $\mathbb{Z}^{\mu_1}/U_1 \oplus \dots \oplus \mathbb{Z}^{\mu_s}/U_s \cong \mathbb{Z}^\mu / \langle N \rangle$ for some $\mu \geq 1$.
- (3) If L is empty, return the pair $[G, \mathcal{O}]$ and stop. Otherwise, choose the power product $t = \min_\sigma(L)$ and remove it from L .
- (4) Compute the vector $v = \text{RV}_{\mathcal{O}_1}(t) \oplus \dots \oplus \text{RV}_{\mathcal{O}_s}(t) \in \mathbb{Z}^\mu$.
- (5) Let m_1, \dots, m_ℓ be the elements of M . Compute a \mathbb{Z} -basis B in Hermite normal form of the set of solutions of the homogeneous linear equation

$$vx_0 - \sum_{i=1}^{\ell} m_i x_i - \sum_{i=\ell+1}^{k+\ell} n_i x_i = 0$$

in the indeterminates $x_0, \dots, x_{k+\ell}$.

- (6) If it exists, let $(a_i) \in \mathbb{Z}^{k+\ell+1}$ be a basis element in B with $a_0 \neq 0$. Append the polynomial $a_0 t - \sum_{i=1}^{\ell} a_i t_i$ to the list G , where t_i is the i -th power product in the list \mathcal{O} .
- (7) If there exists no such solution or if the first component a_0 of every solution is different from 1, append the vector v to M and the term t to the list \mathcal{O} . Add to L those elements of $\{x_1 t, \dots, x_n t\}$ which are neither multiples of an element of L nor of an element of $\{\text{LM}_{\sigma}(g) \mid g \in G\}$.
- (8) Continue with step (3).

This is an algorithm which computes a pair (G, \mathcal{O}) such that G is a reduced strong σ -Gröbner basis of $I = \bigcap_{i=1}^s I_s$ and the residue classes of the elements in \mathcal{O} generate the \mathbb{Z} -module P/I .

Proof. First we prove correctness using induction on the iterations of the algorithm. More precisely, we show that if the values of G and \mathcal{O} are correct at the start of an iteration then they are still correct at the end of the iteration.

If L is not empty then it contains a minimal element t with respect to σ . So, at the start of each iteration we have that the list G contains polynomials that can be extended to a minimal strong Gröbner basis of the intersection and whose leading terms are σ -smaller than t . Consider the case $t >_{\sigma} 1$. If $(a_i) \in \mathbb{Z}^{k+\ell+1}$ is the solution of the linear system in step (5) then $a_0 v - \sum_{i=1}^{\ell} a_i m_i \in \langle N \rangle$, and hence $f = a_0 t - \sum_{i=1}^{\ell} a_i t_i \in I_1 \cap \dots \cap I_s$. Since the solution space is in Hermite normal form, every other polynomial h in the intersection with $\text{LT}_{\sigma}(h) = t$ has to satisfy $a_0 t \mid \text{LM}_{\sigma}(h)$, and f cannot be reduced further using the elements in G . This means that a reduced strong Gröbner basis of the intersection has to contain f , and f is added to G in step (6).

If there exists no solution with non-zero first component, or the first component of all solutions is different from 1, there is no element g in G such that $\text{LM}_{\sigma}(g) \mid t$. Hence the term t has to be added to \mathcal{O} .

Finally, the list L is updated such that its σ -smallest element is always the σ -smallest term greater than t and not divisible by the leading monomial of some element of G . Since $P/(I_1 \cap \dots \cap I_s)$ is a finite \mathbb{Z} -module, there exists for every $i \in \{1, \dots, n\}$ a number $\alpha_i \geq 1$ such that $x_i^{\alpha_i} \in \text{LT}_{\sigma}(I_1 \cap \dots \cap I_s)$. Hence only a finite number of terms can be added to the list L . This proves that the procedure terminates. \square

Let us apply this algorithm to an example.

Example 6.4. Let $\sigma = \text{DegRevLex}$, and consider the ideals $I = \langle 2x - y, x^2, y^2, xy \rangle$ and $J = \langle x^2, y^2, 2 \rangle$ in $P = \mathbb{Z}[x, y]$. We have

$$\mathcal{O}_I = \mathbb{T}^n \setminus \langle x^2, y^2, xy \rangle = \{1, y, x\} \quad \text{and} \quad \mathcal{O}_J = \mathbb{T}^n \setminus \langle x^2, y^2 \rangle = \{1, y, x, xy\}.$$

The following table shows how Algorithm 6.3 can be applied to compute a strong σ -Gröbner basis of $I \cap J$. The first five rows of this table correspond to the elements of N . The algorithm considers the terms $1, y, x, y^2, xy, x^2$ in this order. Rows 6–11 in the table correspond to the

representation vectors computed in step (4) of each iteration.

	1	y	x	1	y	x	xy	
	0	-1	2	0	0	0	0	
	0	0	0	2	0	0	0	
	0	0	0	0	2	0	0	
	0	0	0	0	0	2	0	
	0	0	0	0	0	0	2	
1	1	0	0	1	0	0	0	$\rightarrow G = []$
y	0	1	0	0	1	0	0	$\rightarrow G = []$
x	0	0	1	0	0	1	0	$\rightarrow G = [4x - 2y]$
y^2	0	0	0	0	0	0	0	$\rightarrow G = [4x - 2y, y^2]$
xy	0	0	0	0	0	0	1	$\rightarrow G = [4x - 2y, y^2, 2xy]$
x^2	0	0	0	0	0	0	0	$\rightarrow G = [4x - 2y, y^2, 2xy, x^2]$

For instance, let us examine the 5-th iteration, where the algorithm handles the term xy . In step (5) of this iteration we solve the homogeneous linear system of equations given by rows 1–8 and row 10 of the table. This is because in the 4-th iteration we did not add the representation vector to the set M . The Hermite normal form of a basis of the solution space is given by

$$\begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 4 & -2 & 0 & -2 & 0 & 1 & -2 & 0 \end{bmatrix}.$$

Hence we append the element $2xy$ to G . Altogether, we obtain the strong σ -Gröbner basis $\{4x - 2y, y^2, 2xy, x^2\}$ of $I \cap J$.

If the \mathbb{Z} -algebras P/I_i determined by the ideals I_i are given as in Remark 2.1, then it is not necessary to compute their strong Gröbner bases separately, as the following corollary shows.

Corollary 6.5. (Computing a Strong Gröbner Basis)

Suppose that a finite \mathbb{Z} -algebra R is explicitly given as in Remark 2.1, and let I be the ideal in P such that $R = P/I$ and I is of the form described in (*). Let σ be a degree compatible term ordering on \mathbb{T}^n . Then Algorithm 6.3 computes a strong σ -Gröbner basis of I in polynomial time.

Proof. As mentioned in Remark 6.2.a, the representation vector in step (4) of an element $f \in P$ can be obtained by simplifying every product of indeterminates using the structure constants. The linear equation in step (6) can be solved in polynomial time by Remark 2.4. The claim then follows from the fact that the number of iterations is bounded by the number of generators of R . □

6.2. Computing an Explicit Representation. Now let $I \subseteq P$ be an ideal such that $R = P/I$ is a finite \mathbb{Z} -algebra. Given a strong Gröbner basis of I with respect to some term ordering σ , our goal is to compute a representation of R as in Remark 2.1. The first step is to find a suitable system of \mathbb{Z} -module generators of R .

Proposition 6.6. (Macaulay’s Basis Theorem for Finite \mathbb{Z} -Algebras)

Let $I \subseteq P$ be an ideal such that P/I is a finite \mathbb{Z} -algebra, let σ be a term ordering on \mathbb{T}^n , and let $L = \{m \in \text{LM}_\sigma(I) \mid \text{LC}_\sigma(m) = 1\}$ be the set of all monic leading monomials of I .

Then the residue classes of the terms in $\mathcal{O}_\sigma = \mathbb{T}^n \setminus L$ form a generating set of the \mathbb{Z} -module P/I .

Proof. It suffices to show that the \mathbb{Z} -submodule $Q = \sum_{t \in \mathcal{O}_\sigma} \mathbb{Z}(t + I) = \sum_{t \in \mathcal{O}_\sigma} \mathbb{Z}t + I$ of P is equal to P . Suppose that $Q \subsetneq P$, and let $f \in P \setminus Q$ be a polynomial with minimal leading term. Then $\text{LT}_\sigma(f) \in \mathcal{O}$ would imply $f - \text{LC}_\sigma(f) \text{LT}_\sigma(f) \in P \setminus Q$ which would contradict the minimality of f . Hence we have $\text{LT}_\sigma(f) \in L$. This means there exist a polynomial $g \in I$ and a term $t \in \mathbb{T}^n$ such that $\text{LC}_\sigma(g) = 1$ and $\text{LT}_\sigma(f) = t \text{LT}_\sigma(g)$. But then $f - \text{LC}_\sigma(f)tg$ has smaller leading term, again contradicting the minimality of f . \square

The set \mathcal{O}_σ in this proposition can be determined from a strong Gröbner basis of I . Having obtained a tuple of \mathbb{Z} -module generators of P/I , it remains to determine its relation module.

For every polynomial $f \in P$, the Division Algorithm with respect to a σ -Gröbner basis of I yields its normal form $\text{NF}_{\sigma,I}(f) = \sum_{i=1}^{\mu} a_i t_i$ with $a_i \in \mathbb{Z}$ and $t_i \in \mathbb{T}^n$. The canonical epimorphism $\pi : P \rightarrow P/I$ satisfies $\pi(f) = \sum_{i=1}^{\mu} a_i \bar{t}_i$. Moreover, for a given generating set of P/I , we have a canonical surjective map $\varphi : P/I \rightarrow \mathbb{Z}^\mu$. Combining this map with π , we obtain a \mathbb{Z} -linear surjective map $\text{RV}_{\mathcal{O}_\sigma} : P \rightarrow \mathbb{Z}^\mu$ which sends f to (a_1, \dots, a_μ) .

Given a strong Gröbner basis of the ideal I , we can now compute the kernel of the map φ as follows.

Algorithm 6.7. (Computing a Module Presentation)

Let I be an ideal in P , let σ be a term ordering on \mathbb{T}^n , let G be a minimal strong σ -Gröbner basis of I , and let $\{t_1, \dots, t_k\} = \mathbb{T}^n \setminus L$, where L equals $\{m \in \text{LM}_\sigma(I) \mid \text{LC}_\sigma(m) = 1\}$ as in Proposition 6.6. Consider the following instructions.

- (1) Start with an empty list $U = []$ and $\mathcal{O} = [t_1, \dots, t_k]$.
- (2) If \mathcal{O} is empty, return the list U and stop. Otherwise, choose a term t in \mathcal{O} and remove it from \mathcal{O} .
- (3) Find the smallest integer $\ell > 1$ such that $\ell s \in \text{LM}_\sigma(G)$ for some $s \in \mathbb{T}^n$ with $s \mid t$. If no such integer exists, continue with step (2).
- (4) Let $c \in \mathbb{Z}^k$ be the coefficient vector representing ℓt , and let $d \in \mathbb{Z}^k$ be the coefficient vector representing $\text{NF}_{\sigma,I}(\ell t)$ with respect to (t_1, \dots, t_k) . Append $c - d$ to U and continue with step (2).

This is an algorithm which computes a list of tuples $U \subseteq \mathbb{Z}^k$ such that we have $P/I \cong \mathbb{Z}^k / \langle U \rangle$.

Proof. By Proposition 6.6, the residue classes of the terms t_1, \dots, t_k generate the \mathbb{Z} -module P/I . Assume that $t_1 >_\sigma t_2 >_\sigma \dots >_\sigma t_k$, and consider the \mathbb{Z} -module homomorphism

$$\varphi : \mathbb{Z}^k \rightarrow P/I \quad \text{given by } (c_1, \dots, c_k) \mapsto c_1 t_1 + \dots + c_k t_k.$$

Clearly, we have $\text{Ker}(\varphi) \supseteq \langle U \rangle$. Assume that the converse containment does not hold. Then there exists a tuple $c = (c_1, \dots, c_k) \in \text{Ker}(\varphi)$ such that $f = c_1 t_1 + \dots + c_k t_k \in I$ and $c \notin U$. Choose c with this property such that $\text{LT}_\sigma(f)$ is minimal. Since $f \in I$, there exists a polynomial $g \in G$ with $\text{LM}_\sigma(g) \mid \text{LM}_\sigma(f) = c_i t_i$.

Notice that this implies $\text{LC}_\sigma(g) > 1$. Otherwise, the term t_i would be divisible by $\text{LT}_\sigma(g)$, and this would imply $t_i \in L$, a contradiction.

Consequently, there is an element $d = (d_1, \dots, d_k) \in U$ with $d_1 = \dots = d_{i-1} = 0$ and $\ell d_i = c_i$ for some $\ell \in \mathbb{Z}$. The tuple $c - \ell d$ corresponds to a polynomial whose leading term is smaller than $\text{LT}_\sigma(f)$. This shows $c - \ell d \in U$, but then we get $c \in U$ in contradiction to

our assumption. Hence we have the equality $\text{Ker}(\varphi) = \langle U \rangle$ and φ induces the inverse of the desired isomorphism. \square

Given a strong Gröbner basis of an ideal I as above, an explicit representation of P/I can now be obtained as follows.

Corollary 6.8. (Computing an Explicit Representation)

Let I be an ideal in P such that P/I is a finite \mathbb{Z} -algebra, let σ be a term ordering on \mathbb{T}^n , and let G be a minimal strong σ -Gröbner basis of I . Consider the following instructions.

- (1) Compute the set $\{t_1, \dots, t_k\} = \mathbb{T}^n \setminus L$, where the set L equals $\{m \in \text{LM}_\sigma(I) \mid \text{LC}_\sigma(m) = 1\}$.
- (2) Apply Algorithm 6.7 to compute generators of a submodule $V \subseteq \mathbb{Z}^k$ such that $P/I \cong \mathbb{Z}^k/V$.
- (3) For $i, j = 1, \dots, k$, use the Division Algorithm with respect to G to compute the normal form $\text{NF}_{\sigma, I}(t_i t_j) = \sum_{\ell=1}^k c_{ij\ell} t_\ell$ with $c_{ij\ell} \in \mathbb{Z}$.
- (4) Return the residue classes of t_1, \dots, t_k in P/I , the generators of V , and the coefficients $c_{ij\ell}$ for $i, j, \ell = 1, \dots, k$.

This is an algorithm which computes an explicit representation of P/I in polynomial time in the bit complexity of the input G .

Proof. The residue classes of t_1, \dots, t_k generate P/I as a \mathbb{Z} -module by Proposition 6.6. Algorithm 6.7 then correctly computes V such that $P/I \cong \mathbb{Z}^k/V$. Finally, we check that $\text{NF}_{\sigma, I}(t_i t_j)$ is of the form given in step (4). Let s be a term not contained in $\{t_1, \dots, t_k\}$. Suppose that $\text{NF}_{\sigma, I}(t_i t_j)$ contains a monomial ds with $d \in \mathbb{Z}$. Then we have $ds \notin \text{LM}_\sigma(I)$, and in particular $s \notin L$, a contradiction. The time complexity of each step is clearly polynomial. \square

In conclusion, we can see that an explicit representation of a finite \mathbb{Z} -algebra R as in Remark 2.1 is equivalent to knowing a strong Gröbner basis of an ideal I in $P = \mathbb{Z}[x_1, \dots, x_n]$ such that $R = P/I$. Traditionally, many of the algorithms presented in this paper were executed using the calculation of a strong Gröbner basis. However, as there is no polynomial time bound for a suitable version of Buchberger's Algorithm, the complexity bounds shown here would be impossible if R were only given via $R = P/I$. As explicit representations of the type described in Remark 2.1 occur in many contexts (see for instance [20]), we hope that the algorithms and complexity bounds developed here may prove useful.

REFERENCES

- [1] J. Abbott, M. Kreuzer, and L. Robbiano, Computing zero-dimensional schemes, *J. Symbolic Comput.* **39** (2005), 31-49.
- [2] W. Adams and P. Lousstanaun, *An Introduction to Gröbner Bases*, Graduate Studies in Math. **3**, Amer. Math. Soc., Providence 1994.
- [3] The ApCoCoA Team, ApCoCoA: Applied Computations in Computer Algebra, available at apcocoa.uni-passau.de
- [4] C. W. Ayoub, The decomposition theorem for ideals in polynomial rings over a domain, *J. Algebra* **76** (1982), 99-110.
- [5] E. R. Berlekamp, Factoring polynomials over finite fields, *Bell Syst. Tech. J.* **46** (1967), 1853-1859.
- [6] E. R. Berlekamp, Factoring polynomials over large finite fields, *Math. Comp.* **24** (1970), 713-735.
- [7] N. Bourbaki, *Elements of Mathematics, Algebra I, Chapters 1-3*, Addison Wesley Publ., Reading 1974

- [8] D.A. Cox, Solving equations via algebras, in: A. Dickenstein and I. Emiris (eds), *Solving Polynomial Equations*, Alg. and Comp. in Math. **14**, Springer-Verlag, Berlin 2005, pp. 63-124.
- [9] W. Decker, G.-M. Greuel, and G. Pfister, Primary decomposition: algorithms and comparisons, in: B. H. Matzat, G.-M. Greuel, and G. Hiss(eds), *Algorithmic Algebra and Number Theory*, Springer, Berlin 1999, pp. 187-220.
- [10] Y. A. Drozd and V. V. Kirichenko, *Finite Dimensional Algebras*, Springer-Verlag, Berlin 1994.
- [11] W. Eberly and M. Giesbrecht, Efficient decompositions of associative algebras over finite fields, *J. Symb. Comput.* **29** (2000), 441-458.
- [12] S. A. Evdokimov, Factorization of polynomials over finite fields in subexponential time under GRH, in: *Proceedings of the First International ANTS Symposium*, LNCS **877**, Springer-Verlag, Berlin 1994, pp. 209-219.
- [13] K. Friedl and L. Rónyai, Polynomial time solutions of some problems in computational algebra, in: *Proceedings of the seventeenth annual ACM symposium on Theory of computing*, Association for Computing Machinery, New York 1985, pp. 153-162.
- [14] S. Gao, On the deterministic complexity of factoring polynomials, *J. Symb. Comput.* **31** (2001), 19-36.
- [15] S. Gao, D. Wan, M. Wang, Primary decomposition of zero-dimensional ideals over finite fields, *Math. Comput.* **78** (2008), 509-521.
- [16] J. von zur Gathen, Factoring polynomials over finite fields: a survey, *J. Symb. Comput.* **31** (2001), 3-17.
- [17] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*, Cambridge University Press, Cambridge 1999.
- [18] G. Ivanyos, M. Karpinski, L. Rónyai, and N. Saxena, Trading GRH for algebra: algorithms for factoring polynomials and related structures, *Math. Comp.* **81** (2012), 493-531.
- [19] R. Kannan, and A. Bachem, Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix, *SIAM J. Comput.* **4** (1979), 499-507.
- [20] M. Kreuzer, A. Miasnikov, and F. Walsh, Decomposing finite \mathbb{Z} -algebras, preprint 2023, available at [arXiv:2308.01735](https://arxiv.org/abs/2308.01735) [math.RA].
- [21] M. Kreuzer and L. Robbiano, *Computational Commutative Algebra 1*, Springer-Verlag, Berlin 2000.
- [22] M. Kreuzer and L. Robbiano, *Computational Commutative Algebra 2*, Springer-Verlag, Berlin 2008.
- [23] M. Kreuzer and L. Robbiano, *Computational Linear and Commutative Algebra*, Springer Int. Publ., Cham 2016.
- [24] F. Lazebnik, On systems of linear Diophantine equations, *Math. Mag.* **4** (1996), 261-266.
- [25] H. W. Lenstra and A. Silverberg, Algorithms for commutative algebras over the rational numbers, *Found. Comput. Math.* **18** (2018).
- [26] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, Factoring polynomials with rational coefficients, *Math. Ann.* **261** (1982), 515-534.
- [27] G. Pfister, A. Sadiq, and S. Steidel, An algorithm for primary decomposition in polynomial rings over the integers, *Central Europ. J. Math.* **9** (2011), 897-904.
- [28] L. Rónyai, Computing the structure of finite algebras, *J. Symb. Comput.* **9** (1990), 355-373.
- [29] C. Saha, Factoring polynomials over finite fields using balance test, in: *25th International Symposium on Theoretical Aspects of Computer Science*, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl 2008, pp. 609-620.
- [30] A. Seidenberg, Constructions in a polynomial ring over the ring of integers, *Amer. J. Math.* **100** (1978), 685-703.
- [31] A. Storjohann, Near optimal algorithms for computing Smith normal forms of integer matrices, in: *Proc. Int. Symp. on Symbolic and Algebraic Computation (ISSAC'96)*, ACM, New York 1996, pp. 267-274.
- [32] A. Storjohann, A fast + practical + deterministic algorithm for triangularizing integer matrices, Technical Report **255**, ETH Zürich, 1996.