Abstract We introduce the concept of multiplication matrices for ideals of projective dimension zero. We discuss various applications and, in particular, we give a new algorithm to compute the variety of an ideal of projective dimension zero.

Keywords Multiplication matrix · System solving · Buchberger–Möller algorithm · Projective points

Mathematics Subject Classification (2000) Primary 13P10; Secondary 12Y05

1 Introduction

Eigenvalue methods to compute the variety of an affine zero-dimensional ideal have become an active area of research [9–11,25,26]. Recall that over an algebraically closed field, an ideal is defined to be of dimension zero if the corresponding variety is finite. The key of the eigenvalue methods is a nice one-to-one correspondence between the points on the variety and common eigenvectors to so-called multiplication matrices.

The notion of zero-dimensionality exists also for projective space. Let \( \mathbb{k} \) be a field. We say that an ideal \( I \subseteq \mathbb{k}[x_0, \ldots, x_n] \) is of projective dimension zero if \( \mathbb{k}[x_0, \ldots, x_n]/I \) is graded of Krull dimension one. The variety of an ideal of projective dimension zero consists of a finite number of projective points. We show that it is possible to define so-called projective multiplication matrices with respect to ideals of projective dimension zero and we establish a one-to-one correspondence between projective points on the variety and common eigenvectors to the projective multiplication matrices.

In order to be able to define the projective multiplication matrices, we need to choose appropriate vector space bases for the graded parts of the quotient ring \( \mathbb{k}[x_0, \ldots, x_n]/I \). The usual choice of a vector space basis is as the residues of the complement of the initial ideal of \( I \) (with respect to some monomial order). Our choice of bases differs from these—in general we consider non-monomial \( \mathbb{k} \)-bases.

We also consider a situation where there is an injection from the set of points on the variety to the set of common eigenvectors for a set of matrices which are related, but not the same, as the multiplication matrices. This algorithm, given in Sect. 5.2, gives an unexpected way to compute the variety of an ideal of projective dimension zero.
Although we rely on Gröbner basis computations, we show that we do not need to compute the whole Gröbner basis. Indeed, we give criteria when to stop the computations before the Buchberger algorithm terminates. This approach is different and independent of the nice criteria given in [1,2]. We also show how to use these multiplication matrices to compute normal forms and argue that the computations outperform the usual reduction method based on Gröbner bases.

2 Notation and Preliminaries

Throughout the paper, let $k$ be a field and let $S = k[x_0, \ldots, x_n]$ be the polynomial ring in $n + 1$ variables. Recall that the Hilbert series of a graded ring $R = R_0 \oplus R_1 \oplus R_2 \oplus \cdots$ is the power series $H_s(R, t) = \dim_k(R_0) + \dim_k(R_1)t + \dim_k(R_2)t^2 + \cdots$. The Hilbert function of a graded ring $R$ is the map $d \mapsto \dim_k(R_d)$. An ideal $I$ is of projective dimension zero exactly when $R = S/I$ is graded and satisfies $\dim_k(R_d) = m$ for some $m > 0$ and for all sufficiently large $i$. The minimal $i$ such that $\dim_k(R_i) = \dim_k(R_{i+1}) = \cdots$ is called the regularity index of $R$ and we denote it by $\text{ri}(R)$, using the notation from [17].

When $I$ is an ideal of projective dimension zero and $R = S/I$, we then say that $R$ is a ring of projective dimension zero. If $a$ is an element of $S$, we write $[a]$ to denote the equivalence class in $R$ containing $a$.

By $V(I)$, we denote the variety of $I$ with respect to the algebraic closure $\overline{k}$ of $k$, so that $|V(I)| \leq |V(\overline{I})|$. The number of projective points in $V(I)$ counting multiplicity equals $\dim_k(R_{\text{ri}(R)})$.

Let $I = Q_1 \cap \cdots \cap Q_s$ be a minimal primary decomposition of $I$. Let $P_i = \sqrt{Q_i}$. When no $P_i$ equals the unique graded maximal ideal $m = (x_0, \ldots, x_n)$ of $S$, we say that $I$ is unmixed. Otherwise we say that $I$ is mixed. If $I$ is unmixed, the Hilbert series of $R$ is strictly increasing until it reaches the degree $\text{ri}(R)$, whereas if $I$ is mixed, the Hilbert series of $R$ does not behave nicely in general, for instance, it can have an arbitrary number of valleys.

Recall that the saturation of a mixed ideal with $\sqrt{Q_i} = m$ with respect to $m$ is being equal to the ideal with the component $Q_j$ dropped. We write $I^{\text{sat}}$ to denote this unmixed version of $I$. This means that when $I$ is unmixed, we have the identity $I = I^{\text{sat}}$. We extend this definition to $R^{\text{sat}} = S/I^{\text{sat}}$.

Example 2.1 Let $I = x_1^2x_2^3 - x_2^4, x_1x_2^3 - x_3^5, x_1x_2^3 - x_3^5$. Then $I = (x_1 - x_2) \cap (x_2^3) \cap (x_1^3, x_2^3)$. Thus, $Q_1 = (x_1 - x_2), Q_2 = (x_2^3)$ and $Q_3 = (x_1^3, x_2^3)$. We have $P_1 = \sqrt{Q_1} = Q_1$, so $V(P_1) = \{(1:1)\}$, and $P_2 = \sqrt{Q_2} = (x_2)$ so $V(P_2) = \{(1:0)\}$. Finally, $m = \sqrt{Q_3}$. Thus, $I^{\text{sat}} = (x_1 - x_2) \cap (x_2^3) = (x_1x_2^2 - x_3^5)$. We have $H_s(R^{\text{sat}}, t) = 1 + 2t + 3t^2 + 3t^3 + \cdots$, where $H_s(R, t) = 1 + 2t + 3t^2 + 3t^3 + 4t^4 + 3t^5 + 3t^6 + \cdots$, so that $\text{ri}(R^{\text{sat}}) = 2$ and $\text{ri}(R) = 5$. (It does not in general hold though that $\text{ri}(R^{\text{sat}}) \leq \text{ri}(R)$.) The point $(1:1)$ has multiplicity one, while the point $(1:0)$ has multiplicity two.

We have a one-to-one correspondence of prime ideals $P_i$ generated in degree one and points on $V(I)$. If $V(I) = V(I)$, it follows that $|V(I)| = s$ and that $P_1, \ldots, P_s$ are all generated in degree one.

The concept of non-zero divisors is of particular importance in this paper. Recall that $I \neq 0$ is a non-zero divisor on the $S$-module $M$ if $\text{lm} = 0$ implies that $m = 0$. In Example 2.1, $[x_1]$ is a non-zero divisor on $R^{\text{sat}}$, while $[x_2]$ is not. The existence of non-zero divisors is connected to Cohen–Macaulayness and the primary decomposition in the following sense for a ring $R = S/I$ of projective dimension zero:

$I$ is unmixed $\iff$ $R$ is Cohen–Macaulay $\iff$ $R$ contains a non-zero divisor.

Although $R$ has no non-zero divisors if $I$ is mixed, we will show that there is a minimal degree $d$ for which there exists a non-zero divisor on the $S$-module $R_d^{\text{sat}} \oplus R_{d+1}^{\text{sat}} \oplus \cdots$. This degree $d$ is equal to $\max(\text{ri}(R), \text{ri}(R^{\text{sat}}))$. To simplify the notation, we will denote $\max(\text{ri}(R), \text{ri}(R^{\text{sat}}))$ by $\text{nz}(R)$. When there can not be any confusion, we will omit $R$ and only write $\text{nz}$. It holds that every non-zero divisor on $R^{\text{sat}}$ is also a non-zero divisor on $R_{\text{nz}} \oplus R_{\text{nz}+1} \oplus \cdots$.

In Example 2.1, $\text{nz}(R) = 5$ and $[x_1]$ is a non-zero divisor on $R_5 \oplus R_6 \oplus \cdots$.

Suppose that $V$ and $W$ are two $k$-spaces of dimension $m$ and $m'$ respectively. Let $\{[e_1], \ldots, [e_m]\}$ be a $k$-basis for $V$ and let $\{[e'_1], \ldots, [e'_{m'}]\}$ be a $k$-basis of $W$. Let $\phi$ be a $k$-linear map from $V$ to $W$ and let $A_\phi$ be the $m \times m'$
matrix, whose $i$’th row is the coefficient vector $(c_1, \ldots, c_m)$ and where $\phi([e_i]) = c_1[e'_1] + \cdots + c_m[e'_m]$. Notice that $A_\phi$ is the transpose of the standard matrix representation of $\phi$.

If the map $\phi$ is defined on a finite-dimensional algebra by $v \mapsto f v$, whenever $f$ is an element in the algebra, then the matrix $A_\phi$ is called the multiplication matrix with respect to $f$. We also denote $A_\phi$ by $A_f$.

**Example 2.2** Let $I = (x_1 - 1, x_2^2 - x_2) \subset \mathbb{Q}[x_1, x_2]$. The ideal $I$ is zero-dimensional and a $k$-basis for $\mathbb{Q}[x_1, x_2]/I$ can be chosen as $\{[1], [x_2]\}$. In this algebra we have $[x_1][1] = [1], [x_1][x_2] = [x_2], [x_2][1] = [x_2]$ and $[x_2][x_2] = [x_2]$, so the multiplication matrices with respect to $[x_1]$ and $[x_2]$ equals

$$A_{[x_1]} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad A_{[x_2]} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}.$$  

It is conventional to write $A_i$ instead of $A_{[x_i]}$ and we will do so in the sequel.

The case of rings of projective dimension zero is problematic, since these rings are infinite dimensional as vector spaces over $k$. But since each graded part of such a graded ring is finite dimensional, we could fix a degree $d$ and let $\phi$ be defined from $R_d$ to $R_{d+|f|}$ via multiplication by a form $f$ with respect to the bases $\{[e_1], \ldots, [e_m]\}$ and $\{[e'_1], \ldots, [e'_m]\}$ for $R_d$ and $R_{d+|f|}$ respectively. Then $A_f$ (or $A_\phi$) is the projective multiplication matrix in degree $d$ with respect to $f$. Later we will show that it is possible to choose bases such that the projective multiplication matrices agree for all degrees greater than or equal to $n z(R)$.

**Example 2.3** For the ring $R^\text{sat}$ from Example 2.1, we can choose $\{[x_1^2], [x_1 x_2], [x_2^2]\}$ as a $k$-basis in degree two and $\{[x_1^3], [x_1^2 x_2], [x_2^3]\}$ as a $k$-basis in degree three. If $\phi$ denotes the map from $R_2^\text{sat}$ to $R_3^\text{sat}$ induced by multiplication by $[x_2]$, then the projective multiplication matrix of degree two with respect to $[x_2]$ equals

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$  

since $[x_2][x_1^2] = 0[x_1^3] + [x_1^2 x_2] + 0[x_2^3], [x_2][x_1 x_2] = 0[x_1^3] + [x_1^2 x_2] + 1[x_2^3]$ and $[x_2][x_2^2] = 0[x_1^3] + 0[x_1^2 x_2] + 1[x_2^3]$.

### 3 Projective Multiplication Matrices

We will use the fact that the Hilbert function of rings of projective dimension zero eventually get constant in order to define the projective multiplication matrices.

#### 3.1 Linear Non-zero Divisors

We now state a classical lemma and for completeness we also give the proof.

**Lemma 3.1** Let $I$ be an ideal of projective dimension zero. Suppose that $V(I) = \overline{V(I)}$. That $[l]$ is a non-zero divisor on $R^\text{sat}$ is equivalent to $l(p) \neq 0$ for all $p \in V(I)$.

**Proof** Suppose that $l(p) \neq 0$ for all $p \in V(I)$. If $[a] \in R^\text{sat}$ is such that $[a] \cdot [l] = 0$ in $R^\text{sat}$, then $a \cdot l \in I^\text{sat}$, so that $(a \cdot l)(p) = a(p) \cdot l(p) = 0$ for all $p \in V(I)$. Hence $a(p) = 0$ for all $p \in V(I)$. Thus $a \in I$, so $[l]$ is a non-zero divisor on $R^\text{sat}$.

Suppose instead that $[l]$ is a non-zero divisor on $R^\text{sat}$. Let $q$ be an arbitrary point in $V(I)$. Let $[Q]$ be an element in $R^\text{sat}$ such that $Q(q) \neq 0$ and $Q(p) = 0$ for $p \in V(I) \setminus \{q\}$. (The element $Q$ is called a separator for the point $q$ with respect to $V(I)$. Separators exists, see for instance [1] or Sect. 6.2.) Suppose that $l(q) = 0$. Then $Q(p) \cdot l(p) = 0$ for all $p \in V(I)$, so that $[Q] \cdot [l] = 0$. Since $[Q] \neq 0$, it follows that $[l]$ is a zero-divisor, which is a contradiction. Hence $l(p) \neq 0$ for all $p \in V(I)$. \qed
Proposition 3.2 Suppose that $k$ contains at least $\lvert V(I) \rvert$ elements. Then $R$ has a linear non-zero divisor if and only if $I$ is unmixed. The requirement on $k$ is sharp in the sense that if $k$ contains $\lvert V(I) \rvert - 1$ elements, then there exists an unmixed ideal $I$ such that $R$ lacks linear non-zero divisors.

Proof If $I$ is mixed, then $R$ does not contain non-zero divisors. So suppose that $I$ is unmixed. Let $s = \lvert V(I) \rvert$ and let $I = Q_1 \cap \cdots \cap Q_s$ be a primary decomposition with respect to $R$. Let $P_I = \sqrt{Q_i}$. Each $P_I$ is generated in degree one. The set of zero-divisors in $R$ equals the union of the residues of the $P_i$’s (Proposition 4.7 in [5]). So if we let $\mathbb{N} = S \setminus \bigcup P_i$, then the set of linear non-zero divisors in $R$ is the residues of $\mathbb{N}$. Let $\mathbb{N} = S_1 \cap \mathbb{N}$. Then the linear non-zero divisors of $R$ is the residues of $\mathbb{N}$. Let $\eta_i = \overline{P_i} \cap S_i$.

Suppose that $k$ is infinite or finite and contains $\lvert k \rvert \geq s$ elements. Suppose that $v_i \in S_1$ but $v_i \notin \eta_1 \cup \cdots \cup \eta_s$ for $i < s$ (clearly $v_1$ exists). If $v_i \notin \eta_{i+1}$, then let $w_{i+1} = v_i$. Otherwise, take an element $w_i \in \eta_i$ such that $w_i \notin \eta_{i+1}$ (such an element must exist, since we assume that $v_i \notin \eta_{i+1}$). The element $v_i + \alpha w_i$ does not belong to $\eta_i$ nor to $\eta_{i+1}$ for any non-zero $\alpha \in k$. Pick $\alpha_i \in k \setminus \{0\}$. If $v_i + \alpha_i w_i \in \eta_{i-1}$, then $v_i + \alpha w_i \notin \eta_{i-1}$ for all $\alpha \in k \setminus \{\alpha_i\}$, since otherwise we would have $\alpha(v_i + \alpha_i w_i) - \alpha_i(v_i + \alpha w_i) = (\alpha - \alpha_i)v_i \in \eta_{i-1}$, which is a contradiction. So pick $\alpha_2 \in k \setminus \{\alpha_1\}$. Clearly $\eta_i + \alpha_2 w_i \notin \eta_{i-1} \cup \eta_i \cup \eta_{i+1}$. It is clear that we can continue in this way provided that there is at most $i - 1$ non-zero elements in $k$. Since $i$ ranges from 1 to $s$, this construction uses at most $s - 1$ non-zero elements in $k$.

Suppose instead that $k$ is a field with elements $\{a_0, a_1, a_2, \ldots, a_{s-1}\}$ with $a_0 = 0$ and $a_1 = 1$. Consider the points $p_1 = (1 : 0 : \cdots : 0)$, $p_2 = (1 : 1 : 0 : \cdots : 0)$, $p_3 = (1 : a_2 : 0 : \cdots : 0)$, ..., $p_s = (1 : a_{s-1} : 0 : \cdots : 0)$ and $p_{s+1} = (0 : 1 : 0 : \cdots : 0)$ in $P^s(k)$. Let $l(p_i)$ be the vanishing ideal with respect to $p_i$, which is prime. Let $I = \cap l(p_i)$ and let $l = b_0 x_0 + \cdots + b_n x_n$ be an arbitrary linear form. If $l$ is non-zero on $p_1, \ldots, p_s$, then $b_0 + b_1 a_0 \neq 0, b_0 + b_1 a_1 \neq 0, \ldots, b_0 + b_1 a_{s-1} \neq 0$. Now $b_1$ must equal zero, since otherwise we would have $b_0 + b_1 a_i = b_0 + b_1 a_j$ when $i \neq j$ and thus, by the pigeonhole principle, $b_0 + b_1 a_i = 0$ for some $i$, which contradicts the assumption that $l(p_i) \neq 0$. But if $b_1 = 0$, then $l(p_{s+1}) = 0$. Thus, the ring lacks linear non-zero divisors by Lemma 3.1.

Remark 3.3 When $k$ is finite, it is an interesting question to determine, given a degree $d$, the maximal number of points allowed to guarantee the existence of a non-zero divisor of degree $d$. This problem is solved in a separate paper [23] and Proposition 3.2 is a special case of the result therein. But the proof given here is better suited for our computational purposes.

Remark 3.4 We should also mention that Kreuzer has given a non-constructive proof of Proposition 3.2 in [16].

Remark 3.5 If $k$ contains less than $\lvert V(I) \rvert$ elements, then one can make a field extension $\overline{k}$ of $k$ so that the extended field contains at least $\lvert V(I) \rvert$ elements. It is then clear that there is a linear non-zero divisor in $\overline{k}[x_0, \ldots, x_n]/I$ (provided that $I$ is unmixed).

Example 3.6 Let $I = (x_0 + x_1, x_0 + x_2) \cap (x_0 + x_1, x_0 + 2x_2) \cap (x_0 + 2x_1, x_0 + 2x_2) \subseteq \mathbb{Z}[x_0, x_1, x_2]$. We have $V(I) = \{(1 : 2 : 2), (1 : 2 : 1), (1 : 1 : 1)\}$. To compute a non-zero divisor, we start by computing $v_1$. We pick an element of degree one in $(x_0 + x_1, x_0 + x_2)$, say $x_0 + x_1$. By changing one of the coefficients, we can assure that this element is not in $(x_0 + x_1, x_0 + x_2)$, so we let $v_1 = x_0 + 2x_1$. Since $v_1(p_2) \neq 0$ we let $v_2 = v_1$. But $v_2(p_3) = 0$, so we look for an element $w_2$ which is in $(x_0 + x_1, x_0 + 2x_2)$ but not in $(x_0 + 2x_1, x_0 + 2x_2)$. It is clear that we can find such an element by going through the generators of $(x_0 + x_1, x_0 + 2x_2)$ until we find an element which is not in $p_3$. Indeed, $w_2 = x_0 + x_1$ is such an element. We have $v_2 + w_2 = 2x_0$. Since $2x_0(p_1) \neq 0$ we can use $[2x_0]$ (or rather $[x_0]$) as a non-zero divisor.

Proposition 3.7 Let $I$ be a d of effective dimension zero. Suppose that $k$ contains at least $\lvert V(I) \rvert$ elements. Then there exists a linear form $l \in S_1$ such that $\mathcal{L} : R_d \to R_{d+1}, [a] \mapsto [l][a]$ is onto, for all $d \geq \text{nz}(R)$.

Proof If $R = R^{\text{sat}}$, then, by Proposition 3.2, $R$ contains a non-zero divisor of degree one which has the desired property. Otherwise, the maximal ideal is associated to $I$. Thus, the primary decomposition of $I$ can be written as $I = J \cap Q$, with $\sqrt{Q} = m$. Let $d \geq \text{nz}(R)$. Then $\dim_k(R_d) = \dim_k(R_d^{\text{sat}})$, which is equivalent to
Proposition 3.11 Let $I$ be an ideal of projective dimension zero. Suppose that $I$ is a non-zero divisor on $R_{d+1}$. Then there is a linear change of coordinates $T$ and a choice of bases elements such that the projective multiplication matrices $A_j$ representing the map $R_{d+1} \rightarrow R_{d+1}$, $a \mapsto [x_j a]$ with respect to the bases above, is independent of the choice of $i$.

We refer also to the papers [18, 19] by Lazard where this result is presented in a slightly different context.

3.2 An Affine Connection

To a ring $R$ of projective dimension zero, we will now associate an affine ring of dimension zero, whose multiplication matrices coincide with the projective multiplication matrices of the projective ring. In fact, the affine ring is obtained by dehomogenizing the ideal with respect to the first variable $x_0$ after a suitable linear change of coordinates.

Lemma 3.9 Suppose that $\mathbb{k}$ contains at least $|V(I)|$ elements. Then there is a linear change of coordinates $T$ and a variable $x_i$ such that $T(x_i)(p) \neq 0$ for all points $p \in V(I)$.

Proof Let $I$ be the form from Proposition 3.7. We can write $I = b_0 x_0 + \cdots + b_n x_n$. Some coefficient is non-zero, say $b_i \neq 0$. Let $T(x_i) = l$ and let $T(x_j) = x_j$ if $j \neq i$.

By changing coordinates we can, without loss of generality, assume that $x_0$ is a non-zero divisor. We write $I_{\text{deh}}$ to denote the dehomogenization of $I$ with respect to $x_0$, and by $R_{\text{deh}}$ we mean $R / (x_0 - 1)$.

We now recall the definition of multiplicity. Let $J \subseteq \mathbb{k}[x_1, \ldots, x_n]$ be an ideal of affine dimension zero and let $J = q_1 \cap \cdots \cap q_t$ be a minimal primary decomposition. The multiplicity of a point $p \in V(J)$, belonging to $\sqrt{q_i}$, is defined as $\dim_{\mathbb{k}}(\mathbb{k}[x_1, \ldots, x_n] / q_i)$. A similar definition holds for projective points. Indeed, if $I$ is an ideal of projective dimension zero and $I = q_1 \cap \cdots \cap q_t$, then the multiplicity of a point $p$ on $V(I)$ belonging to $\sqrt{q_i}$, is defined as $\dim_{\mathbb{k}}(\mathbb{k}[x_0, \ldots, x_n] / q_i)$.

These two multiplicity definitions are connected in the sense that if $p = (1 : a_1 : \cdots : a_n)$ is a projective point with multiplicity $r$ in $V(I)$, then $(a_1, \ldots, a_n)$ is an affine point with multiplicity $r$ in $V(I_{\text{deh}})$, for instance, see [15].

Lemma 3.10 Let $I$ be an ideal of projective dimension zero. Suppose that, after a linear change of coordinates, $[x_0]$ is a non-zero divisor on $R_{\text{sat}}$. Let $[\{e_1\}, \ldots, \{e_m\}]$ be a $\mathbb{k}$-basis for $R_d$, for some $d \geq \text{nz}(R)$. Then $[\{e_1\}, \ldots, \{e_m\}]$ is a $\mathbb{k}$-basis for $R_{\text{deh}}$, where $[\cdot \cdot \cdot]$ denotes an equivalence class in $R$ mod $[x_0] - 1$.

Proof Since the $\mathbb{k}$-dimension of $R_{\text{deh}}$ and $R_{\text{sat}}$ is determined by the sum of the points counting multiplicity, we have $\dim_{\mathbb{k}}(R_{\text{deh}}) = \dim_{\mathbb{k}}(R_d) = m$.

Suppose that $a_1 \{e_1\} + \cdots + a_m \{e_m\} = 0$. Then $f = a_1 e_1 + \cdots + a_m e_m \in I_{\text{deh}}$. Hence, $f(q) = 0$ for all $q \in V(I_{\text{deh}})$. But this is equivalent to $f(p) = 0$ for all $p \in V(I)$.

Thus $f \in I$. Since $[\{e_1\}, \ldots, \{e_m\}]$ is a $\mathbb{k}$-basis for $R_d$, we must have $a_1 = \cdots = a_m = 0$. Hence $[\{e_1\}, \ldots, \{e_m\}]$ is a $\mathbb{k}$-basis for $R_{\text{deh}}$.

Proposition 3.11 Let $I$ be an ideal of projective dimension zero. Suppose that $\mathbb{k}$ contains at least $|V(I)|$ elements. Then there is a change of coordinates and a choice of bases elements such that the projective multiplication matrices $A_1, \ldots, A_n$ for $R$ coincides with the multiplication matrices for $R_{\text{deh}}$ and that the projective multiplication matrix $A_0$ is the identity matrix.
Theorem 3.12

Let $I$ be a zero-dimensional ideal with variety $V(I) = \{p_1, \ldots, p_r\}$. Let $\{[e_1], \ldots, [e_m]\}$ be a $k$-basis for $R_{nz+1}$ and let $\{[e_1], \ldots, [e_m]\}$ be a $k$-basis for $R_{deh}^{\text{rel}}$, validated by Lemma 3.10.

Let $k > 0$ and let $A_k = (a_{ij})$ be the projective multiplication matrix with respect to $x_k$. Then $[x_k][e_1] = a_{11}[x_0e_1] + \cdots + a_{im}[x_0e_m]$. It follows that $[[x_k]]([e_1]) = a_{11}[[e_1]] + \cdots + a_{im}[[e_m]]$. Hence $A_k$ is the multiplication matrix of $R_{deh}^{\text{rel}}$ with respect to $x_k$. That $A_0$ is the identity follows directly from the definition.

3.3 Points on the Variety and Eigenvectors for the Projective Multiplication Matrices

The introduction of the matrices $A_i$ and their eigenvalues as a tool for solving was introduced in [4], and the theorem below appears in a series of papers, for instance [9–11, 24–26]. But as far as we know, it has only been considered over algebraically closed fields. We now provide a proof of the theorem for any field.

Theorem 3.12

Let $I \subseteq k[x_1, \ldots, x_n]$ be a zero-dimensional ideal with variety $V(I) = \{p_1, \ldots, p_r\}$. Let $\{[e_1], \ldots, [e_m]\}$ be a $k$-basis for $k[x_1, \ldots, x_n]/I$ and let $A_1, \ldots, A_n$ be the multiplication matrices with respect to this basis. Then there are exactly $r$ common (right) eigenvectors for the matrices $A_1, \ldots, A_n$ and they are, up to multiplication with a scalar, equal to $(e_1(p_i), \ldots, e_m(p_i))^t$ for $i = 1, \ldots, r$. Let $\lambda_{ij}$ denote the eigenvalue of $A_j$ with respect to the eigenvector $(e_1(p_i), \ldots, e_m(p_i))^t$. Then $p_i = \langle \lambda_{i1}, \ldots, \lambda_{in} \rangle$.

Proof

When $k$ is algebraically closed, the proof can be found in [25]. Otherwise, let $\overline{k}$ denote the algebraic closure of $k$ and let $\overline{V(I)}$ denote the variety of $I$ over $\overline{k}$. Since the ideal is defined over $k$, the shape of the multiplication matrices does not depend on $\overline{k}$ or $\overline{V(I)}$. It is also clear that if $p_i \in V(I)$, then $(e_1(p_i), \ldots, e_m(p_i))^t$ is a common eigenvector. It rests to show that there is no common eigenvector to the matrices which is not of the form $(e_1(p_i), \ldots, e_m(p_i))^t$ for $p_i \in V(I)$. But if $v = (v_1, \ldots, v_m)^t$ is a common eigenvector for the $A_j$’s, then $(v_1, \ldots, v_m)^t = \alpha(e_1(p_i), \ldots, e_m(p_i))^t$ for $p_i \in V(I)$ and for a non-zero $\alpha$. But the eigenvalues for $(e_1(p_i), \ldots, e_m(p_i))^t$ are exactly $p_{i1}, \ldots, p_{in}$, so $p_i \in V(I)$ since the eigenvalues of $v$ lies in $k$.

We have an almost identical theorem in the projective setting, but first we set some notation. If $p = (p_1 : \cdots : p_n)$ and $p_i$ is the first non-zero coordinate, we define the evaluation of $p$ on a form $f$ by $f(p) = f((0, \ldots, 0, 1, p_{i+1}/p_i, \ldots, p_m/p_i))$. This way of thinking of evaluation is implicit in [28].

With this evaluation method it follows that if $l_1$ and $l_2$ are elements of $S$ and $[l_1] = [l_2]$ in $R$, then $l_1(p) = l_2(p)$ for all points $p$ on $V(I)$. This property makes it possible to define evaluation on elements in $R$ by $[l](p) = l(p)$, where $p \in V(I)$.

Later we will need a notation for evaluating a set of points on a set of elements. If $P = \{p_1, \ldots, p_m\}$ is a set of projective points, we write $f(P) = (f(p_1), \ldots, f(p_m))$. If $F = \{f_1, \ldots, f_s\}$ is a set of forms in $S$, then $F(P)$ is defined to be the $(s \times m)$-matrix whose $i$’th row is $f_i(P)$.

Theorem 3.13

Let $I \subseteq k[x_0, \ldots, x_n]$ be an ideal of projective dimension zero. Suppose that $k$ contains at least $|V(I)|$ elements and let $V(I) = \{p_1, \ldots, p_r\}$. Let $\{[e_1], \ldots, [e_m]\}$ be a $k$-basis for $R_{nz+1}$ and let $l$ be a form of degree one such that $\{[e_1], \ldots, [e_m]\}$ is a $k$-basis for $R_{nz+1}$. Let $A_0, \ldots, A_n$ be the projective multiplication matrices with respect to this basis. Then there are exactly $r$ common (right) eigenvectors for the matrices $A_0, \ldots, A_n$ and they are, up to multiplication with a scalar, equal to $(e_1(p_i), \ldots, e_m(p_i))^t$ for $i = 1, \ldots, r$. Let $\lambda_{ij}$ denote the eigenvalue of $A_j$ corresponding to the eigenvector $(e_1(p_i), \ldots, e_m(p_i))^t$. Then $p_i = \langle \lambda_{i0}, \lambda_{i1}, \ldots, \lambda_{in} \rangle$.

Proof

By Proposition 3.11, there is a linear change of coordinates such that we can assume that $l = x_0$ and that there is choice $\{[e_1], \ldots, [e_m]\}$ of basis elements such that the affine and projective multiplication matrices agrees for $x_1, \ldots, x_n$. Call the multiplication matrices $B_0, \ldots, B_n$. Since the multiplication matrix with respect to $x_0$ is the identity, a common eigenvector for $B_1, \ldots, B_n$ is also a common eigenvector for $B_0, \ldots, B_n$ and vice versa.

But by linearity, $v$ is a common eigenvector to $B_0, \ldots, B_n$ if and only if $v$ is a common eigenvector to $A_0, \ldots, A_n$. Hence, the set of common eigenvectors for $A_0, \ldots, A_n$ equals $e_1(p_i), \ldots, e_m(p_i)$, for $i = 1, \ldots, r$, by Theorem 3.12.

\[ \square \]
To determine the multiplicity of a point \( p \in V(I) \), one can use the result of Corless et al. [9]. The method goes as follows.

Let \( A \) be a generic linear combination of the multiplication matrices. Let \( \lambda \) be the eigenvalue of \( A \) with respect to \( e(p) \) (clearly \( e(p) \) is an eigenvector of \( A \)). Then the multiplicity of \( p \) equals the algebraic multiplicity of \( \lambda \). There are also direct methods which one could use. For instance, see [26].

We now illustrate the method by a simple example.

**Example 3.14** The elements

\[
\begin{align*}
  f_1 &= xz + yz - z^2 \\
  f_2 &= x^2 - y^2 + 2yz - z^2 \\
  f_3 &= xy - y^2 + yz
\end{align*}
\]

generates an unmixed ideal \( I \) of projective dimension zero in \( \mathbb{C}[x, y, z] \). Choosing \( [x], [y], [z] \) and \([y^2],[yz],[z^2]\) as bases in degree 1 and 2 respectively, we see that neither \([x],[y]\) nor \([z]\) serve as non-zero divisors. Indeed, if we let \( M_x, M_y \) and \( M_z \) denote the multiplication matrices from \( R_1 \) to \( R_2 \) with respect to the bases chosen above, we compute

\[
\begin{align*}
  M_x &= \begin{pmatrix} 1 & -2 & 1 \\ 1 & -1 & 0 \\ 0 & -1 & 1 \end{pmatrix}, & \quad M_y &= \begin{pmatrix} 1 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, & \quad M_z &= \begin{pmatrix} 0 & -1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}
\end{align*}
\]

and we can see that all the matrices have a nontrivial kernel. However, \( M_y + M_z \) has full rank which is equivalent to \([y+z]\) being a non-zero divisor. Hence, if we use \([x(y+z)], [y(y+z)], [z(y+z)]\) as a \( k \)-basis in degree two, we can construct the projective multiplication matrices \( A_x, A_y \) and \( A_z \). From these matrices the solutions can be read off. Now \([x(y+z)] = [y^2] - 2[zy] + [z^2], [y(y+z)] = [y^2] + [zy], [z(y+z)] = [yz] + [z^2]\) by making use of the multiplication matrices above. Thus, with

\[
T = \begin{pmatrix} 1 & 1 & 0 \\ -2 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}
\]

we have \( A_x = M_x(T^t)^{-1} \) and similarly for \( A_y \) and \( A_z \), so that

\[
A_x = \frac{1}{2} \begin{pmatrix} 2 & 0 & 0 \\ 1 & 1 & -1 \\ 1 & -1 & 1 \end{pmatrix}, \quad A_y = \frac{1}{4} \begin{pmatrix} 2 & 2 & -2 \\ 1 & 3 & -1 \\ -1 & 1 & 1 \end{pmatrix}
\]

and

\[
A_z = \frac{1}{4} \begin{pmatrix} 2 & -2 & 2 \\ -1 & 1 & 1 \\ 1 & -1 & 3 \end{pmatrix}
\]

Common eigenvectors for the matrices are \((1, 1, 0), (1, 0, 1)\) and \((0, 1, 1)\). The eigenvalues corresponding to \((1, 1, 0)\) are \(1, 1, 0\) for \( A_x, A_y \) and \( A_z \) respectively. Likewise, the eigenvalues corresponding to \((1, 0, 1)\) are \(1, 0, 1\) and the eigenvalues corresponding to \((0, 1, 1)\) are \(0, 1, 1\). Thus, \( V(I) = \{(1 : 1 : 0), (1 : 0 : 1), (0 : 1 : 1)\} \).

Notice that since \( nz(R) = 1 \), we can also use the correspondence between eigenvectors and the \( k \)-basis to obtain the points. Indeed \([x](p_1), [y](p_1), [z](p_1)) = (1, 1, 0)\), thus we have \( p_1 = (1 : 1 : 0) \), etc.

### 3.4 Projective Multiplication Matrices and Normal Forms

As an application of the multiplication matrices, we obtain a fast normal form algorithm for high degree elements of \( S \). Suppose that we have a normal form algorithm \( \text{NF}(\ast, B) \) for elements of degree less than or equal to \( nz(R) \).
To extend this method to elements of degree > nz(R), we proceed as follows. Let \( a \cdot b \) be a monomial in \( S \) and suppose that \( |b| = nz(R) \). We use the normal form algorithm for low degree elements to obtain \( \text{Nf}(b, B) = b_1e_1 + \cdots + b_me_m \).

To determine \( \text{Nf}(ab, B) \), write \( a = x_1^{a_1} \cdots x_n^{a_n} \). It is straightforward to check that

\[
\text{Nf}(ab, B) = (b_1, \ldots, b_m)A_1^{a_1} \cdots A_n^{a_n}(l|e_1, \ldots, l|e_m)'.
\]

Thus, the arithmetic complexity of the normal form algorithm is \( O(|a|m^3) \) if one uses naive matrix multiplication or \( O(|a|m^{2.376}) \) if one uses the best known theoretical result [8]. To this we need to add the complexity for computing \( \text{Nf}(b, B) \).

**Example 3.15** Suppose that we want to compute the normal form of \( x^{17} \) with respect to the ideal \( I \) from Example 3.14. We have seen that \([x(y + z)]_0, [y(y + z)]_0, [z(y + z)]_0\) forms a \( k \)-basis for \( R/I \) and that

\[
A_x = \frac{1}{2} \begin{pmatrix} 2 & 0 & 0 \\ 1 & 1 & -1 \\ 0 & 1 & 1 \end{pmatrix}.
\]

Since \([x]_0\) is a basis element in degree one, the normal form of \( x^{17} \) equals

\((1, 0, 0)A^{16}x(y + z)^{16}, y(y + z)^{16}, z(y + z)^{16}\).

Since \( A^2 = 2 \cdot A \), we have \( A^{16} = 2^{15}A \). Hence

\[
\text{Nf}(x^{17}, x(y + z)^{16}, y(y + z)^{16}, z(y + z)^{16}) = 2^{15}x(y + z)^{16}.
\]

If we know the variety of \( I \), then the normal form computation can be simplified, see Example 6.4.

Similar approaches to Gröbner-free normal form computations can be read in the papers [3, 27].

**4 Computing More Gröbner Basis Elements Than What Is Needed?**

As we have seen, a convenient way to think of a ring \( R = S/I \) of projective dimension zero is as \( R_0 \oplus R_1 \oplus \cdots \oplus R_{nz+1} \) together with the linear map \( l \) and the multiplication matrices \( A_0, \ldots, A_n \). The \( k \)-dimension of the graded pieces of \( R_{\leq nz} \) describes the configuration of the points and also tells whether or not the maximal ideal is associated, while the multiplication matrices encode the variety as a set. From Sect. 3.4, we know that it is also possible to compute normal forms from this information.

So perhaps it would be better to present a ring of projective dimension zero by \( R_{\leq nz+1} \cdot l \) and the multiplication matrices rather than a Gröbner basis for \( I \)?

If \( G \) is a Gröbner basis for an ideal \( I \) of projective dimension zero, let \( G_{\leq d} \) denote the set of Gröbner basis elements of degree less than or equal to \( d \). From \( G_{\leq d} \), we can compute a vector space basis of \( R_i \) for \( i = 0, \ldots, d \) and also the projective multiplication matrices up to degree \( d - 1 \). Thus, in order to determine the multiplication matrices, it is enough to compute \( G_{\leq nz+1} \).

**Example 4.1** A Gröbner basis for the ideal \( I = (xz + yz - z^2, x^2 - y^2 + 2yz - z^2, xy - y^2 + yz) \) from Example 3.14 with respect to \( x > y > z \) and the Degree Reverse Lexicographical ordering is \( \{xz + yz - z^2, x^2 - y^2 + 2yz - z^2, xy - y^2 + yz, y^2z - yz^2\} \). Since \( nz(R) = 1 \), we only need to consider the \( k \)-spaces \( R_1 \) and \( R_2 \) to determine the variety, and for this purpose, it is enough to know \( G_2 \). Hence, the term \( y^2z - yz^2 \) in the Gröbner basis is superfluous.

By combining the forthcoming Theorem 4.4 and Proposition 4.6, we show

**Theorem 4.2** Let \( I \) be an ideal of projective dimension zero and let \( t \) be the maximal degree of the generators in a minimal generator set of \( I \). A bound for the maximal degree of an element in a reduced Gröbner basis is \( \text{max}(ri(R), m, t) \).
This theorem is a generalization of the result in [1], where it is shown that the highest degree element of a Gröbner basis is bounded by \( \max(m, t) \) in the case when \( I \) is unmixed. Recall that it holds that \( \text{ri}(R) \leq m - 1 \) when \( I \) is unmixed by the strictly increasing property of the Hilbert function of \( R \).

So when \( nz(R) + 1 < \max(\text{ri}(R), m, t) \), it would be a good choice to stop the Gröbner basis computation after finishing degree \( nz(R) + 1 \).

The bound in Theorem 4.2 is sharp. Indeed, in Example 3.14, \( nz(R) = 1 \), \( m = 3 \), \( t = 2 \) and the reduced Gröbner basis with respect to the Degree Reverse Lexicographical ordering and \( x \succ y \succ z \) has a generator in degree three, while in Example 5.3 below, we will see that \( nz(R) = 3 \), \( m = 1 \), \( t = 2 \) and a reduced Gröbner basis with respect to the Degree Reverse Lexicographical ordering and \( x \succ y \succ z \) is \( \{xy - z^2, x^2 - xz, y^2 - z^2, xz^2 - yz^2, -yz^2 + z^3\} \).

### 4.1 Binomial Expansions and Gotzmann’s Persistence Theorem

Recall that if \( h \) and \( i \) are positive integers, then \( h \) can be uniquely written as a sum

\[
h = \binom{n_i}{i} + \binom{n_{i-1}}{i-1} + \cdots + \binom{n_j}{j},
\]

where

\[
n_i > n_{i-1} > \cdots > n_j \geq j \geq 1.
\]

See [28] for an easy proof. This sum is called the binomial expansion of \( h \) in base \( i \). Define

\[
h^{<i>} = \binom{n_i + 1}{i+1} + \binom{n_{i-1} + 1}{i} + \cdots + \binom{n_j + 1}{j+1}.
\]

Macaulay characterized Hilbert functions by means of binomial expansions and showed that \( Hf \) is the Hilbert function of a graded algebra if and only if \( Hf(d + 1) \leq Hf(d)^{<d>} \) for all \( d \geq 1 \).

Let \( I \) be minimally generated by \( f_1, \ldots, f_m \), let \( t \) be the maximal degree of the \( f_i \)’s and let \( Hf \) be the Hilbert function of \( \mathbb{k}[x_0, \ldots, x_n]/I \). The least \( d \geq t \) for which \( Hf(d + 1) = Hf(d)^{<d>} \) is called the Gotzmann degree of \( \mathbb{k}[x_0, \ldots, x_n]/I \). In [20], Theorem 4.2, it is shown that every ring \( \mathbb{k}[x_0, \ldots, x_n]/I \) has a finite Gotzmann degree.

Gotzmann’s persistence theorem says the following.

**Theorem 4.3 (Gotzmann’s persistence theorem [14])** Let \( d \) be the Gotzmann degree of \( \mathbb{k}[x_0, \ldots, x_n]/I \), for any homogeneous ideal \( I \). Then \( Hf(d + 1) = Hf(d)^{<d>} \), \( Hf(d + 2) = Hf(d + 1)^{<d+1>} \), \( Hf(d + 3) = Hf(d + 2)^{<d+2>} \), \ldots.

A Lex-segment set \( L_d \) on \( \{x_0, \ldots, x_n\} \) is the \( |L_d| \) greatest monomials of degree \( d \) in \( \mathbb{k}[x_0, \ldots, x_n] \) with respect to the Lexicographical ordering. When \( L \) is a collection of Lex-segment sets, let \( I(L) \) denote the ideal generated by the elements in the Lex-segment sets. We call \( I(L) \) a Lex-segment ideal. When \( J \) is a monomial ideal, let \( |J^c_\leq d| \) denote the number of monomials outside \( J \) of degree \( d \). When writing \( \text{in}(I_{\leq d}) \) we mean the initial ideal of the ideal generated by \( I_{\leq d} \).

Let \( I \) be a homogeneous ideal generated in degree less than or equal to \( d \) and let \( L \) be a collection of Lex-segment sets with maximal degree \( d \). A property among Lex-segment ideals is that they have maximal co-growth (minimal growth), in the sense that

\[
|I(L)^c_{\leq d}| = |I(L)_{\leq d}|^{<d>},
\]

for instance, see [20], Proposition 4.11.

As the following theorem shows, the Gotzmann degree for \( S/I \) is related to the maximal degree of an element in a reduced Gröbner basis for \( I \). Although we believe that this result is not new, we have not been able to find it in the literature.

**Theorem 4.4** Let \( I \) be any graded ideal in \( \mathbb{k}[x_0, \ldots, x_n] \). The Gotzmann degree of \( \mathbb{k}[x_0, \ldots, x_n]/I \) is an upper bound for the degree of an element in a reduced Gröbner basis of \( I \).
Proof Let \( d \) be the Gotzmann degree of \( R = \mathbb{k}[x_0, \ldots, x_n]/I \). Let \( L \) be a collection of Lex-segment sets such that \( I(L)^c_d = \text{in}(I)^c_d \). Let \( d' \geq d \). Then
\[
\dim_k(R) = |I(L)^c_d| \geq |\text{in}(I)_{d'}| \geq |\text{in}(I)^c_{d'}| = \dim_k(R_{d'}).
\]

This implies that \( |\text{in}(I)_{d'}| = |\text{in}(I)^c_{d'}| \) for all \( d' \geq d \). Hence, \( \text{in}(I) \) is generated in degrees less than or equal to \( d \). It follows that there can not be any minimal Gröbner basis element of degree greater than \( d \).

\( \Box \)

### 4.2 The Gotzmann Degree of a Ring of Projective Dimension Zero

**Lemma 4.5** Let \( a \geq b \) be positive integers. It holds that \( \binom{a+1}{b+1} \geq \binom{a}{b} \) and \( \binom{a+1}{b+1} = \binom{a}{b} \) if and only if \( a = b \).

**Proof** Follows from \( \binom{a+1}{b+1} = \binom{a}{b+1} + \binom{a}{b} \) when \( a > b \).

\( \Box \)

**Proposition 4.6** Let \( R = S/I \) be a ring of projective dimension zero, and let \( t \) denote the maximal degree of a generator in a minimal generator set of \( I \). Let \( d \) denote the Gotzmann degree of \( R \) and let \( m = \dim_k(R_{t(R)}) \). Then \( d = \max(\text{ri}(R), m, t) \).

**Proof** Let \( Hf \) be the Hilbert function of \( R \). For \( d' \gg 0 \) it holds that \( Hf(d')^{<d'} = Hf(d') = m \). Write
\[
Hf(d') = \binom{n_i}{d'} + \binom{n_{i-1}}{d'-1} + \cdots + \binom{n_j}{j}
\]
for some \( n_i > \cdots > n_j \geq 1 \). We have
\[
Hf(d')^{<d'} = \binom{n_i + 1}{d' + 1} + \binom{n_{i-1} + 1}{d'} + \cdots + \binom{n_j + 1}{j + 1},
\]
so \( Hf(d') = Hf(d')^{<d'} \) only if \( d'_{-k} = \binom{n_{i-1} + 1}{d'_{-k}} = \binom{n_{i-1} + 1}{d'_{-k}} = \binom{n_{i-1} + 1}{d'_{-k}} = \binom{n_{i-1} + 1}{d'_{-k}} \) for \( k = i, \ldots, j \), i.e. \( n_k = d'_{-k} \) for \( k = i, \ldots, j \) by Lemma 4.5. From \( Hf(d')^{<d'} = m \) we deduce that
\[
Hf(d') = \binom{d'}{d'} + \cdots + \binom{d' - (m - 1)}{d' - (m - 1)}.
\]

Since \( Hf(d + 1) = Hf(d)^{<d'}, Hf(d + 2) = Hf(d + 1)^{<d+1'}, \ldots, Hf(d') = Hf(d' - 1)^{<d'-1} \), we get
\[
Hf(d) = \binom{d}{d} + \cdots + \binom{d - (m - 1)}{d - (m - 1)},
\]
and conclude that \( d \geq \text{ri}(R) \). Moreover \( d - (m - 1) \geq 1 \) implies that \( d \geq m \). That \( d \geq t \) is clear. Hence \( d \geq \max(\text{ri}(R), m, t) \). Finally, let \( d'' = \max(\text{ri}(R), m, t) \). Then \( Hf(d'') = m = \binom{d''}{d''} + \cdots + \binom{d'' - (m - 1)}{d'' - (m - 1)} \). Hence \( d \leq d'' \), finishing the proof.

\( \Box \)

### 5 Computing the Variety

In Sect. 4, we showed that we could stop the Gröbner basis computations after degree \( nz(R) + 1 \). Unfortunately, we have no good way of knowing that we have reached degree \( nz(R) \).

For instance, suppose that we are given an ideal by its generators and that we know that \( \dim_k(R_d) = \dim_k(R_{d+1}) \) for some \( d \). Not many conclusions can be made from this information. We do not even know the dimension—indeed—the rings \( \mathbb{k}[x, y, z]/(xy, yz, xz) \), \( \mathbb{k}[x, y, z]/(x^2, y^2, z^2) \) and \( \mathbb{k}[x, y, z]/(x^2, xy, xz) \) all have \( \mathbb{k} \)-dimension three in degree one and two. The first ring is of projective dimension zero and its regularity index is one. The second ring is artinian, while the third ring is of projective dimension one.
5.1 Extracting Information Without Knowledge of \(nz(R)\)

When \([f]R_d = R_{d+i}\), for some \([f] \in R_i\), we have the following two simple observations.

**Lemma 5.1** Let \(I\) be a graded ideal in \(S\) and suppose that there is an element \([f] \in R_i\) such that \([f]R_d = R_{d+i}\). Then \(R\) is either artinian or of projective dimension zero.

**Proof** The ring \(S/(I + (f))\) is artinian, hence \(S/I\) is of at most projective dimension zero. \(\square\)

**Lemma 5.2** Let \((f_1, \ldots, f_n) = I \subseteq \mathbb{k}[x_0, \ldots, x_n]\) and suppose that there is an element \([f] \in R_i\) such that \([f]R_d = R_{d+i}\). Then \(R\) is of projective dimension zero.

**Proof** The ring \(S/(I + (f))\) is artinian, hence \((f_1, \ldots, f_n, f)\) form a regular sequence and so do \((f_1, \ldots, f_n)\). It follows that \(S/I\) is of projective dimension zero. \(\square\)

Even if we know that \(R\) is of projective dimension zero, it is hard to tell whether or not the maximal ideal is associated. The following example shows that although \(\dim_k(R_d) = \dim_k(R_{d+1})\) and there is an element \(l\) such that \([l]R_d = R_{d+1}\), it does not hold that \(d \geq nz(R)\).

**Example 5.3** Let \(I = (x^2 - xz, xy - z^2, y^2 - z^2)\). Then \(\text{Hs}(R, t) = 1 + 3t + 3t^2 + t^3 + \cdots\) and \(nz(R) = 3\). We have \(I = (x - y, x - z)\cap(z^2, y^2, xy, x^2 - xz)\). Let \(V(I) = V((x - y, x - z)) = (1:1:1)\) and \(\sqrt{(z^2, y^2, xy, x^2 - xz)} = (x, y, z)\). We can choose \([lx, [y], [z]]\) or \([lzx, [yz], [z^2]]\) as \(k\)-bases in degree one and two respectively and thus, the map from \(R_1\) to \(R_2\) induced by multiplication by \([z]\) is surjective.

Fortunately, as Theorem 5.4 below shows, it is enough to find an \(l\) such that \([l]R_d = R_{d+1}\) if we are only interested in computing the variety. The theorem is similar to Theorem 3.13, where we have a one-to-one correspondence between eigenvectors and points. In Theorem 5.4, all points on the variety gives an eigenvector, but not vice versa.

**Theorem 5.4** Let \(I\) be any homogeneous ideal and let \(R = S/I\). Suppose that there exists an element \([l]S\) such that \([l]R_d = R_{d+1}\). Let \([\{f_1\}, \ldots, \{f_i\}]\) be a \(k\)-basis for \(R_{d+1}\). Let \([e_1], \ldots, [e_s]\) be such that \([e_i][l] = [f_i]\). Let \(A_0, \ldots, A_n\) be such that \(A_i\) corresponds to multiplication with \(x_i\) with respect to the bases \([e_1], \ldots, [e_s]\) and \([f_1], \ldots, [f_i]\).

Suppose that \(p \in V(I)\). Then \(e(p)^l = (e_1(p), \ldots, e_s(p))^l\) is a common eigenvector to the \(A_i\)’s. Let \(\lambda_i\) be the eigenvalue of \(A_i\) corresponding to \(e(p)^l\). Then \(p = (\lambda_0 : \lambda_1 : \cdots : \lambda_n)\).

**Proof** By the definition of the matrix \(A_j\) we have

\[x_j[l]e_k = a_{ki}^{(j)}[l]e_1 + \cdots + a_{kl}^{(j)}[l]e_s.\]

Thus, we get

\[x_j(p)e_k(p) = a_{ki}^{(j)}[l](p) \cdot e_1(p) + \cdots + a_{kl}^{(j)}[l](p) \cdot e_s(p),\]

or, written in matrix form,

\[x_j(p)e(p)^l = A_j[l](p)e(p)^l.\]

Now \(e(p)^l\) can not be the zero vector, since otherwise we would have \(p \in V(I + (e_1) + \cdots + (e_s))\), which is a contradiction since \(S/(I + (e_1) + \cdots + (e_s))\) is artinian. With the same argument, \(l(p)\) is non-zero.

Hence \(e(p)^l\) is an eigenvector of \(A_j\) with the eigenvalue \(\frac{x_j(p)}{l(p)}\). The theorem follows since

\[(\lambda_0 : \lambda_1 : \cdots : \lambda_n) = (x_0(p)/l(p) : x_1(p)/l(p) : \cdots : x_n(p)/l(p)) = (x_0(p) : x_1(p) : \cdots : x_n(p)).\]

\(\square\)
Example 5.5 Let $I = (y^2, z^2, xz, xy)$. Then $\dim_k(R_1) = 3$ and $\dim_k(R_2) = 2$. We choose $\{[x], [y], [z]\}$ and $\{[x^2], [yz]\}$ as $k$-bases in degrees one and two respectively. It is clear that $[x + z]R_1 = R_2$ and thus, by Lemma 5.1, we know that $I$ is of at most projective dimension zero. We have $[x + z][x] = [x^2]$ and $[x + z][y] = [yz]$, so with respect to the bases $\{[x], [y]\}$ and $\{[x + z][x], [x + z][y]\}$, we get

$$A_x = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad A_y = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad A_z = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

There are two common eigenvectors for these matrices—$(1, 0)$ and $(0, 1)$. The associated eigenvalues are $1, 0, 0$ and $0, 0, 1$ respectively. By Theorem 5.4, we know that $V(I) \subseteq \{(1: 0: 0), (0: 0: 1)\}$. We have $y^2((1: 0: 0)) = z^2((1: 0: 0)) = xz((1: 0: 0)) = xy((1: 0: 0)) = 0$, but $z^2((0: 0: 1)) \neq 0$, so $V(I) = \{(1: 0: 0)\}$. Thus, the second point was false.

Theorem 5.4 could also be used to compute the variety in Example 5.3 by setting up the multiplication matrices from degree one to two. We leave this computation as an exercise to the reader.

5.2 An Algorithm to Compute the Variety

So suppose that we want to compute the variety of an ideal $I$ which we suspect is of projective dimension zero. We propose the following algorithm.

Algorithm 5.6

K1 Compute the Gröbner basis elements of degree 1, 2 and so on until we reach a degree $d$ such that $|\text{in}(I)^i_d| \geq |\text{in}(I)^{i+1}_d|$ (this is the same as $\dim_k(R_d) \geq \dim_k(R_{d+1}) = t$).

K2 If $k$ contains less than $\dim_k(R_{d+1})$ elements, make a field extension $\overline{k}$ of $k$ such that $\overline{k}$ contains at least $\dim_k(R_d)$ elements. Set $k = \overline{k}$.

K3 Choose a linear form $[l]$ at random and check if $R_d[l] = R_{d+1}$. If it was not, choose another $l$. If we did not find such an element even after many tries, go back to stage K1 and compute more Gröbner basis elements.

K4 Choose a basis $\{[f_1], \ldots, [f_t]\} = [\text{in}(I)^t_{d+1}]$ for $R_{d+1}$ and let $e_1, \ldots, e_t$ be such that $[e_i][l] = [f_i]$.

K5 Compute the multiplication matrices with respect to the bases $\{[e_1], \ldots, [e_t]\}$ and $\{[f_1], \ldots, [f_t]\}$.

K6 Determine a set of common eigenvectors for these matrices and use Theorem 5.4 to determine a set $X$ with $|X| \leq t$ and $V(I) \subseteq X$.

K7 For each point in $X$, check if $p \in V(I)$ by evaluating $p$ on the generators of $I$.

We refer the reader to the book [29] for techniques to compute common eigenvectors using numerical methods.

6 Computations over Vanishing Ideals of Projective Points

In this section, we apply the theory of projective multiplication matrices to give an alternative version of the projective Buchberger–Möller algorithm. We also give an algorithm for computing projective separators.

6.1 An Alternative Buchberger–Möller Algorithm

Given a set of projective points $P = \{p_1, \ldots, p_m\}$ one can form the vanishing ideal $I(P)$, which consists of all polynomials vanishing on all of the points in $P$. The Hilbert series of $S/I(P)$ is well studied but not completely understood, cf. [13]. The most common way of computing Hilbert series of an ideal defined by projective points has been studied by means of the projective Buchberger–Möller algorithm [1, 24]. This algorithm computes a Gröbner basis of a vanishing ideal by choosing a $k$-basis for the $k$-spaces $R_0, R_1, \ldots, R_d$ until degree $\max(m, nz(R))$
and reducing potential Gröbner basis elements with respect to this basis. We will present a reduced version of the projective Buchberger–Möller algorithm which instead of computing the Gröbner basis of $P(I)$ computes $R_{\leq n\alpha}$, $l$ and the multiplication matrices. We show that the behavior of our method is asymptotically better than the classical Buchberger–Möller-algorithm.

Recall that we suppose that the representation of each projective point is fixed so that we can define evaluation of projective points in a unique way.

A nice way to compute normal forms with respect to vanishing ideals of projective points is by evaluation: Given a form $f$ of degree $d$ and a vector space basis $\{\{e_1\}, \ldots, \{e_m\}\}$ of $R_d$, we obtain the normal form $f(p_1) = \alpha_1 e_1 + \cdots + \alpha_m e_m$, where the $\alpha_i$’s are chosen to satisfy $f(p_1) = \alpha_1 e_1(p_1) + \cdots + \alpha_m e_m(p_1)$ for $i = 1, \ldots, m$. The normal form does not depend on the choice of representation of the points. Computing normal forms by means of evaluation is the key engine behind the graded Buchberger–Möller algorithm and the variation of the method given below.

When studying ideals of projective points, one can always assume that $n + 1 \leq m$. Indeed, we have the following lemma, which is a graded version of Lemma 5.2 in [22].

**Lemma 6.1** Let $E = \{x_{i0}, \ldots, x_{in}\}$ be any subset of the variables such that $E(P)$ and $\{x_0, \ldots, x_n\}(P)$ has same rank. Let $\pi$ be the natural projection from $P^n(k)$ to $P^n_1(k)$ defined by $\pi((a_0 : \cdots : a_n)) = (a_0 : \cdots : a_p)$. Then $q_1, \ldots, q_m$ are distinct where $q_i = \pi(p_i)$. Moreover, with $Q = \{q_1, \ldots, q_m\}$ and with $R = k[x_{i0}, \ldots, x_{in}]/I(Q)$, the graded algebras $\overline{R}$ and $R$ are isomorphic.

**Proof** Suppose that $x_i \notin E$. Then $x_i(P) = \alpha_1 x_{i1}(P) + \cdots + \alpha_p x_{ip}(P)$. Hence $x_i - \alpha_1 x_{i1} + \cdots + \alpha_p x_{ip} \in I$. Since $R_{\geq 1}$ is generated in degree one, it is clear that the elements in $E$ generates $R_{\geq 1}$. Since the evaluation on the $q_i$’s agrees on the elements in $k[x_{i0}, \ldots, x_{in}]$, it follows that $\overline{R}$ and $R$ are isomorphic as graded algebras. It is the clear that $q_1, \ldots, q_m$ are distinct.

**Remark** In a more subtle way, Lemma 6.1 actually follows directly from the projective Buchberger–Möller algorithm.

We now give a variant of the projective Buchberger–Möller algorithm for computing $R_{\leq n\alpha}$, $l$ and the multiplication matrices from the points. As for the Buchberger–Möller algorithm, this algorithm is based on the evaluation method to compute normal forms. But it differs from the Buchberger–Möller algorithm in the sense that it is focused on giving the multiplication tables with respect to the variables rather than giving a Gröbner basis for the ideal.

**Algorithm 6.3**

1. If $k$ contains to few elements, make a field extension $\overline{k}$ of $k$ such that $|\overline{k}| \geq |P|$. Set $k = \overline{k}$. Compute a non-zero divisor $l$ of degree one by using the method in Proposition 3.2.
2. Initiate the lists $B_0 = L_0 = [1]$ and Initials = [ ]. Let $d = 0$.
3. If rank$(B_d(P)) = |P|$, then nz$(R) = d$. Return $B_0, \ldots, B_d$ and $l$. Otherwise, increase $d$ by one, let $B_d = [ ]$ and let $L_d$ be the list of all monomials of degree $d$ which are not multiples of an element of Initials.
4. If $L_d$ is empty, go to step L3; otherwise choose the monomial $t = min \prec(L_d)$ with respect to a fixed monomial order and remove it from $L_d$.
5. If $t(P)$ can be written as a linear combination of the rows in $B_d(P)$, then add $t$ to the set Initials and continue with step L4. Else, append $t$ to $B_d$ and continue with step L4.

The correctness of the method is a direct consequence of the projective BM-algorithm, since the sets $B_0, \ldots, B_d$ are computed in the same way using the two methods. Thus Initials will generate $\text{in}(I_{\leq d})$, while $B_1$ will be the monomial complement of $\text{in}(I_i)$ for $i \leq d$. By using another selection method in step L4, it is possible to obtain a basis which is not necessarily the complement of an initial ideal. (It is an easy exercise to check that the termination of the algorithm does not depend on the selection method.)

We implicitly assume that we have used Lemma 6.1 so that $n \leq m$. This preprocessing can be done using $O(nm^2)$ arithmetic operations, since we test for linear dependence $n$ times. It is straightforward to lift the result in [21] and
show that the complexity of the algorithm is dominated by the arithmetic operations and not the monomial manipulations. The number of arithmetic operations for the step L1 is bounded by \( O(m^3) \) by an elementary analysis of the method in Proposition 3.2. For each degree \( d \) during the algorithm, we need to check linear dependence at most \( \min(m, n)m \) times. Thus, the arithmetic complexity of the method is at most proportional to \( O(r_i(R) \min(m, n)m^3) \).

Since \( R \) is Cohen–Macaulay, we have \( r_i(R) < m \). The original analysis [24] of the Buchberger–Möller algorithm reports the complexity \( O(mn^4) \). (Although it is possible to show that the performance is \( O(\min(m, n)m^3) \) by using arguments like those in [22].)

**Example 6.4** In Example 3.5 in [1], the point set \( P = \{(0 : 2 : 5), (0 : 1 : 2), (1 : 3 : 1), (2 : 3 : 4), (2 : 5 : 4), (1 : 4 : 3)\} \) is considered. The Gröbner basis with respect to the Degree Reverse Lexicographical ordering and \( x < y < z \) is generated in degree three and four and \( H_{s}(R, t) = 1 + 3t + 6t^2 + 6t^3 + \cdots \).

With our approach, we would first fix the coordinates \( P = \{(0, 2, 5), (0, 1, 2), (1, 3, 1), (4, 3, 4), (2, 5, 4), (1, 4, 3)\} \) and then compute \( L_0 = \{1\}, B_0 = \{1\} \) and \( L_1 = \{x, y, z\} \). Since \( \{x, y, z\}(P) \) has full rank, we will have \( B_1 = \{x, y, z\} \). Thus, Initials is empty and \( L_2 = \{z^2, yz, xz, y^2, xy, x^2\} \). It turns out that also \( \{z^2, yz, xz, y^2, xy, x^2\} \) \((P)\) has full rank, so \( B_2 = \{z^2, yz, xz, y^2, xy, x^2\} \). Since \( |P| = 6 \), the algorithm stops and we know that \( H_{s}(R, t) = 1 + 3t + 6t^2 + 6t^3 + \cdots \). It is immediate that \( y(p_i) \neq 0 \) for \( i = 1, \ldots, 6 \), so \( B_3 = \{y^2, y^2z, yz, y^3, y^3z, y^2z^2, y^2z^3\} \) can be used as a \( k \)-basis in degree three, and in general

\[
B_d = \{y^{d-2}z^2, y^{d-1}z^2, xy^{d-2}z, xy^{d-1}, x^2y^{d-2}\}.
\]

Say that we want to compute the normal form of \( x^6 + z^6 \). If we do it by evaluation, we solve the linear equations

\[
(\alpha_1 y^4 z^2 + \alpha_2 y^2 z^3 + \alpha_3 y^3 z + \alpha_4 y^5 + \alpha_5 x y^5 + \alpha_6 x^2 y^4)(p_i)
\]

for \( i = 1, \ldots, 6 \) which is equivalent to perform Gaussian elimination on a \( (6 \times 6) \)-matrix. As result, we get

\[
Nf(x^6 + z^6, B) = \frac{2083926583}{23522400}y^6 - \frac{1160325231}{470448000}xy^5 - \frac{811541583}{26136000}y^5z
- \frac{327280970021}{940896000}x^2y^4 + \frac{1752785233}{117612000}y^4z^2 + \frac{127511218609}{313632000}xy^4z.
\]

We could also use the multiplication matrices. Notice that \( A_x, A_y \) and \( A_z \) share the six linear independent eigenvectors

\[
(z^2(p_i), yz(p_i), xz(p_i), y^2(p_i), xy(p_i), x^2(p_i))^T.
\]

Thus, if we let \( T = B_2(p_i)^T \), we have \( A_x = TD_xT^{-1}, A_y = TD_yT^{-1} \) and \( A_z = TD_zT^{-1} \), where \( D_x = \text{diag}(0, 0, 1/3, 4/3, 2/5, 1/4), D_y = \text{diag}(1, 1, 1, 1, 1, 1) \) and \( D_z = \text{diag}(5/2, 2, 1/3, 4/3, 4/5, 1) \).

So to compute the normal form of \( x^6 + z^6 \), we can start by computing

\[
Nf(x^2, B) = x^2 = (0, 0, 0, 0, 0, 1) \cdot (z^2, yz, xz, y^2, xy, x^2)
\]

and

\[
Nf(z^2, B) = z_2 = (1, 0, 0, 0, 0, 0) \cdot (z^2, yz, xz, y^2, xy, x^2).
\]

We have \( Nf(x^6 + z^6, B) = Nf(x^6, B) + Nf(z^6, B) \), where

\[
Nf(x^6, B) = (0, 0, 0, 0, 0, 1)A_x^4(y^4z^2, y^5z, xy^4z, y^6, xy^5, x^2y^4)^T
= (0, 0, 0, 0, 0, 1)TD_x^4T^{-1}(y^4z^2, y^5z, xy^4z, y^6, xy^5, x^2y^4)^T
\]

and

\[
Nf(z^6, B) = (1, 0, 0, 0, 0, 0)A_z^4(y^4z^2, y^5z, xy^4z, y^6, xy^5, x^2y^4)^T
= (1, 0, 0, 0, 0, 0)TD_z^4T^{-1}(y^4z^2, y^5z, xy^4z, y^6, xy^5, x^2y^4)^T.
\]

Of course, this gives the same result as before.
6.2 An Note on Computing Separators

A family of separators with respect to a set of affine points \( P = \{p_1, \ldots, p_m\} \), is a set \( \{f_1, \ldots, f_m\} \) of polynomial functions such that \( f_i(p_i) = 1 \) and \( f_j(p_j) = 0 \) if \( i \neq j \). It is easy to see that the separators forms a \( k \)-basis for \( k[x_1, \ldots, x_n]/I(P) \).

When the points are projective, we say that \( \{f_1, \ldots, f_m\} \) is a set of separators if \( f_i(p_i) \neq 0 \) and \( f_i(p_j) = 0 \) when \( i \neq j \). When all separators are of the same degree \( d \), they constitute a \( k \)-basis for \( R_d \). If \( k \) contains at least \( m \) elements such that there exists a non-zero divisor \( \ell \), we can construct a separator-\( k \)-basis for \( R_{d+1} \) as \( f_1^\ell, \ldots, f_m^\ell \).

In [22], two methods for computing separators with respect to a collection of affine points are discussed. It is possible to lift this method to the projective setting. Both methods perform the same number of arithmetic operations. We will illustrate one of the methods by an example. In \( \mathbb{P}^2 \), consider \( p_1 = (1, 2, 0, 1, 1) \), \( p_2 = (1, 0, 1, 1, 2) \), \( p_3 = (1, 2, 0, 3, 3) \), \( p_4 = (0, 0, 2, 0, 4) \), \( p_5 = (0, 0, 2, 1, 5) \) and \( p_6 = (2, 1, 3, 1, 6) \). We associate the following table to this point set

\[
\begin{bmatrix}
1 & 1 & 1 & 0 & 0 & 2 \\
2 & 0 & 2 & 0 & 0 & 1 \\
0 & 1 & 0 & 2 & 2 & 3 \\
1 & 1 & 3 & 0 & 1 & 1 \\
1 & 2 & 3 & 4 & 5 & 6
\end{bmatrix}
\]

The sets on the right hand side are also described by an example: The set \( \{1, 3\} \) on the second row shows that \( p_1 \) and \( p_3 \) agree on the first two coordinates. When computing such a table from a point set, one obtains a matrix \( c_{ij} \), where \( c_{ij} \) is the first position where \( p_i \) and \( p_j \) differ.

This matrix is used to compute the separators and it is clear that

\[ Q_i = \prod_{i \neq j} \frac{x_{c_{ij}} - p_{j c_{ij}}}{p_{i c_{ij}} - p_{j c_{ij}}} \]

satisfies \( Q_i(p_j) = 0 \) if \( i \neq j \) and \( Q_i(p_i) = 1 \).

It is shown in [22] that at most \( nm + m^2 \) arithmetic comparisons are used to compute the matrix \( c_{ij} \). (In fact a slightly improved upper bound is given.)

We will now show how to make use of the matrix \( c_{ij} \) to compute projective separators. If we let \( S_{ij}(p_i) \neq 0 \) and \( S_{ij}(p_j) = 0 \), then \( Q_1, \ldots, Q_m \) is a set of projective separators for \( p_1, \ldots, p_m \), where

\[ Q_i = \prod_{j \neq i} S_{ij}. \]

Suppose that each point \( p_i \) is normalized in the sense that the first non-zero position equals one. It is then clear that we can use the affine method to compute the matrix \( (c_{ij}) \) with respect to the points.

We will now give an explicit algorithm to compute each \( S_{ij} \). To simplify notation, let \( h = c_{ij} \).

- If \( p_{ih} = 0 \), then \( p_{jh} \neq 0 \). Let \( h' \) be the least position such that \( p_{ih'} = 1 \) and let \( S_{ij} = p_{jh}x_{h'} - p_{jh}x_h \).
- Else, if \( p_{ih} \neq 0 \) but \( p_{jh} = 0 \), then let \( S_{ij} = x_h \).
- Finally, suppose that \( p_{ih} \neq 0 \) and \( p_{jh} \neq 0 \). Since \( p_i \) and \( p_j \) agrees on all coordinates less than \( h \) and \( p_{ih} \neq p_{jh} \), there is a \( h' \leq h \) such that \( p_{ih'} = p_{jh'} = 1 \). Thus, let \( S_{ij} = p_{jh}x_{h'} - p_{jh'}x_h = p_{jh}x_{h'} - x_h \).

Notice that we can choose the index \( h' \) occurring in the two situations as the first entry where \( p_i \) equals one. It is clear that we can determine the first non-zero index of each point using at most \( nm \) arithmetic comparisons. We have proved the following proposition.

**Proposition 6.5** Let \( P = \{p_1, \ldots, p_m\} \) be a set of distinct projective points. Then we can compute a set of separators of degree \( m - 1 \) with respect to \( P \) using at most \( nm + m^2 \) arithmetic operations.
Example 6.6 Let $p_1 = (1 : 2 : 0 : 1 : 1 : 0 : 3 : 5), p_2 = (1 : 0 : 1 : 1 : 2 : 0 : 3 : 5), p_3 = (1 : 2 : 0 : 3 : 3 : 1 : 2 : 0)$ and let $p_4 = (0 : 1 : 1 : 0 : 2 : 0 : 1 : 0)$. We will show how to compute $Q_1$. We have $c_{12} = 2$ and $p_{12} = 2$ and $p_{22} = 0$. Thus, $S_{12} = x_2$. We have $c_{13} = 4$ and $p_{14} = 1$ and $p_{54} = 3$. Since $p_{11} = p_{31} = 1$, we let $S_{13} = p_{34}x_1 - x_4 = 3x_1 - x_4$. We have $c_{14} = 1$ and $p_{41} = 0$, so $S_{14} = x_1$. Hence $Q_1 = x_2(3x_1 - x_4)x_1$.

7 Discussion

To summarize, this paper has been dealing with the relation between points on the variety of an ideal of projective dimension zero and the projective multiplication matrices.

It would of course also be possible to compute a projective variety $V(I)$ by splitting the problem into one affine piece $I + (x_0 + 1)$ and one projective piece $I + (x_0)$. We can give two arguments that our approach is important. The first argument is theoretical—although our method relies on classical results in the affine setting, the method we present is new, and might turn out to be able to generalize to rings of arbitrary projective dimension. The second is computational. Being able to use the grading is known to be a powerful tool when performing computations, see for instance [6]. And we have a strong criteria in Theorem 5.4 which does not have a counterpart in the affine setting.

Acknowledgments The author would like to thank Clas Löfwall for suggesting the study of ideals of projective dimension zero. He also pointed out that Theorem 3.12 holds for an arbitrary field. The author is also grateful to two anonymous referees for pointing out missing references and criticism related to the terminology and the presentation.

References

1. Abbott, J., Bigatti, A., Kreuzer, M., Robbiano, L.: Computing ideals of points. J. Symb. Comput. 30(4), 341–356 (2000)
2. Abbott, J., Kreuzer, M., Robbiano, L.: Computing Zero-Dimensional Schemes. J. Symb. Comp. 39(1), 31–49 (2005)
3. Alonso, M.E., Mora, T., Niesi, G., Raimondo, M.: An algorithm for computing analytic branches of space curves at singular points. In: Proceedings 1992 International Workshop on Mathematics Mechanization, International Academic Publishers, Pekin, pp. 135–166 (1992)
4. Auzinger, W., Stetter, H.J.: An elimination algorithm for the computation of all zeros of a system of multivariate polynomial equations. I.S.N.M. 86, 11–30, Birkhäuser (1988)
5. Atiyah, M.F., Macdonald, I.G.: Introduction to commutative algebra. Addison-Wesley Publishing Co, Reading (1969)
6. Björck, G., Fröberg, F.: A faster way to count the solutions of inhomogeneous systems of algebraic equations, with applications to cyclic n-roots. J. Symb. Comput. 12(3), 329–336 (1991)
7. Buchberger, B., Möller, M.: The construction of multivariate polynomials with preassigned zeroes. Computer Algebra (Marseille, 1982), Lecture Notes in Comput. Sci. 144, 24–31 (1982)
8. Coppersmith, D., Winograd, S.: Matrix multiplication via arithmetic progressions. J. Symb. Comput. 4(3), 251–280 (1990)
9. Corless, R.M.: Editor’s corner: Gröbner bases and matrix eigenproblems. SIGSAM Bull. 30(4), 26–32 (1996)
10. Corless, R.M., Gutermann, K., Kotsireas, I.S.: Using symmetries in the eigenvalue method for polynomial systems. J. Symb. Comput. 44(11), 1536–1550 (2009)
11. Corless, R.M., Gianni, P.M., Trager, B.M.: A reordered Schur factorization method for zero-dimensional polynomial systems with multiple roots. In: Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation, pp. 133–140 (1997)
12. Faugère, J.C., Gianni, P., Lazard, D., Mora, T.: Efficient computation of zero-dimensional Gröbner bases by change of ordering. J. Symb. Comp. 16(4), 329–344 (1993)
13. Geramita, A.V., Maroscia, P., Roberts, L.: The Hilbert function of a reduced k-algebra. J. London Math. Soc. (2) 28(3), 443–452 (1983)
14. Gotzmann, G.: Eine Bedingung für die Flachheit und das Hilbertpolynomial eines graduierter Ringes. Math. Z. 158(1), 61–70 (1978)
15. Gröbner, W.: Algebraische Geometrie. Vol. 2, Bibliographisches Institut Mannheim, Mannheim (1970)
16. Kreuzer, M.: Computing Hilbert-Kunz functions of 1-dimensional graded rings. Universitatis Iagellonicae Acta Mathematica 45, 81–95 (2007)
17. Kreuzer, M., Robbiano, L.: Computational Commutative Algebra 2. Springer, Heidelberg (2005)
18. Lazard, D.: Algèbre linéaire sur $K[X_1, \ldots, X_n]$ et élimination. Bull. Soc. Math. France 105, 165–190 (1977)
19. Lazard, D.: Resolution des systemes d’équations algebriques. Theoret. Comput. Sci. 15, 77–110 (1981)
20. Lundqvist, S.: An algorithm to determine the Hilbert series for graded associative algebras. Research Reports in Mathematics, vol. 3, pp. 1–19. Stockholm University (2005)
21. Lundqvist, S.: Complexity of comparing monomials and two improvements of the Buchberger–Möller algorithm. MMISC, Lecture Notes in Comput. Sci. 5393, 105–125 (2008)
22. Lundqvist, S.: Vector space bases associated to vanishing ideals of points. J. Pure Appl. Alg. 214(4), 309–321 (2010)
23. Lundqvist, S.: Non-vanishing forms in projective space over finite fields. J. Comm. Alg. 2(4), 435–443 (2010)
24. Marinari, M.G., Möller, H.M., Mora, T.: Gröbner bases of ideals defined by functionals with an application to ideals of projective points. Appl. Algebra Eng. Commun. Comput. 4(2), 103–145 (1993)
25. Möller, H.M., Stetter, H.: Multivariate polynomial equations with multiple zeros solved by matrix eigenproblems. Numer. Math. 70(3), 311–329 (1995)
26. Möller, H.M., Tenberg, R.: Multivariate polynomial system solving using intersection of eigenspaces. J. Symb. Comput. 32(5), 513–531 (2001)
27. Mourrain, B.: Isolated points, duality and residues. J. Pure Appl. Alg. 117, 118, 469–493 (1997)
28. Robbiano, L.: Introduction to the theory of Hilbert functions. Queen’s Papers in Pure and Appl. Math. 85, B1–B26 (1990)
29. Stetter, H.: Numerical Polynomial Algebra, xv+472 pp. SIAM, Philadelphia (2004)