On the Problem of Separating Variables in Multivariate Polynomial Ideals

Manfred Buchacher*
Manuel Kauers†
manfredi.buchacher@gmail.com
manuel.kauers@jku.at
Institute for Algebra
Johannes Kepler University, A4040 Linz, Austria

ABSTRACT

For a given ideal $I \subseteq \mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_m]$ in a polynomial ring with $n+m$ variables, we want to find all elements that can be written as $f - g$ for some $f \in \mathbb{K}[x_1, \dots, x_n]$ and some $g \in \mathbb{K}[y_1, \dots, y_m]$, i.e., all elements of I that contain no term involving at the same time one of the $x_1, \dots, x_n$ and one of the $y_1, \dots, y_m$. For principal ideals and for ideals of dimension zero, we give a algorithms that compute all these polynomials in a finite number of steps.

CCS CONCEPTS

• **Computing methodologies** → **Algebraic algorithms**.

KEYWORDS

Polynomial ideals; polynomial algebras; computer algebra; Gröbner bases

ACM Reference Format:
Manfred Buchacher* and Manuel Kauers†. 2024. On the Problem of Separating Variables in Multivariate Polynomial Ideals. In *International Symposium on Symbolic and Algebraic Computation (ISSAC '24), July 16–19, 2024, Raleigh, NC, USA.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3666000.3669680

1 INTRODUCTION

The problem under consideration is as follows. Given an ideal I of a polynomial ring $\mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_m]$, we want to know all elements of I that can be written in the form $f - g$ for some $f \in \mathbb{K}[x_1, \dots, x_n]$ and some $g \in \mathbb{K}[y_1, \dots, y_m]$. Such a polynomial $f - g$ is called *separated* because it contains no monomials that involve at the same time one of the $x_1, \dots, x_n$ and one of the $y_1, \dots, y_m$.

It is not hard to see that the pairs $(f, g) \in \mathbb{K}[x_1, \dots, x_n] \times \mathbb{K}[y_1, \dots, y_m]$ such that $f - g$ is a separated element of an ideal I of $\mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_m]$ form a unital $\mathbb{K}$-algebra with componentwise addition and multiplication. Indeed, $(1, 1)$ is clearly an element, and if (f, g), (f', g') are elements, then so are $(f + f', g + g')$ and (ff', gg'), the latter because $ff' - gg' = (f - g)f' + g(f' - g') \in I$. We denote the set of all these pairs (f, g) by $A(I)$ and call it the algebra of separated elements of I. Given a basis of the ideal I, we want to compute a set of generators of $A(I)$.

Equations with separated variables have been studied at least since the 1950s [5, 6, 10–15]. Early authors studied the algebraic curves defined by polynomials of the form $f(x) - g(y)$, and in particular the question under which circumstances such a polynomial is irreducible, and the structure of the corresponding function fields. Later, other aspects of the problem entered into the focus, for instance the problem of finding integer roots of polynomials with separated variables [4] or the relation of the separation problem to the problem of decomposing polynomials [2, 3, 7, 16].

The problem of finding separated polynomials in polynomial ideals has various applications. One application is the intersection of $\mathbb{K}$-algebras. For example, computing $\mathbb{K}[u_1, \dots, u_n] \cap \mathbb{K}[v_1, \dots, v_m]$ for given polynomials

$$u_1, \dots, u_n, v_1, \dots, v_m \in \mathbb{K}[t_1, \dots, t_k]$$

is equivalent to finding all the separated polynomials $f - g$ in the ideal

$$\langle x_1 - u_1, \dots, x_n - u_n, y_1 - v_1, \dots, y_m - v_m \rangle \cap \mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_m].$$

Our own motivation comes from a different direction. In a study of generating functions for lattice walk enumeration, Bousquet-Melou [8] finds the solution of a certain functional equation using an interesting elimination technique. She has certain power series $u_1, \dots, u_n$ in $\mathbb{K}[z][[t]]$ and certain power series $v_1, \dots, v_m$ in $\mathbb{K}[z^{-1}][[t]]$ and needs to combine them to a series that is free of z. To do so, she finds polynomials f and g such that $f(u_1, \dots, u_n) = g(v_1, \dots, v_m)$, and concludes that both sides of this equation belong to $\mathbb{K}[z][[t]] \cap \mathbb{K}[z^{-1}][[t]] = \mathbb{K}[[t]]$. We see the development of algorithmic tools for finding separated polynomials as a key step in turning Bousquet-Melou's technique into a general algorithm for solving functional equations.

For ideals I of a bivariate polynomial ring $\mathbb{K}[x, y]$, the problem is well understood. An algorithm for computing generators $I \cap (\mathbb{K}[x] + \mathbb{K}[y])$ was presented in [9]. Let us briefly sketch how this algorithm works.

Since every ideal $I \subseteq \mathbb{K}[x, y]$ is the intersection $I_0 \cap I_1$ of a 0-dimensional ideal I_0 and a principal ideal I_1, and because $A(I_0 \cap I_1) = A(I_0) \cap A(I_1)$, it is sufficient to solve the problem for such ideals, and to be able to intersect the corresponding algebras. The algebra of separated polynomials of I_0 can be determined by first computing

* M. Buchacher was supported by LIT-2022-11-YOU-214.
† M. Kauers was supported by the Austrian FWF grants PAT 9952223 and I6130-N.

ISSAC '24, July 16–19, 2024, Raleigh, NC, USA

ACM ISBN 979-8-4007-0696-7/24/07.
https://doi.org/10.1145/3666000.3669680

generators p, q of its elimination ideals. The elements of $\mathbb{K}[x] \cdot p + \mathbb{K}[y] \cdot q$ are clearly separated, however, they do not necessarily make up all of $I_0 \cap (\mathbb{K}[x] + \mathbb{K}[y])$. For finding the remaining ones it is sufficient to make an ansatz whose degrees are bounded by the degrees of p and q, reducing it, and solving a system of linear equations.

If I_1 is generated by some $p \in \mathbb{K}[x, y] \setminus (\mathbb{K}[x] \cup \mathbb{K}[y])$, then $A(I_1)$ is simple, i.e. generated by single element. Its generator corresponds to a separated polynomial $f - g$ that divides every other separated multiple of p. To determine $f - g$, it is sufficient to know the degrees of f and g. Finding $f - g$ then reduces to linear algebra. It turns out that there is always a grading on $\mathbb{K}[x, y]$ such that $\mathrm{lt}(f) - \mathrm{lt}(g)$ is the minimal separated multiple of the corresponding highest homogeneous component of p. The problem of finding a degree bound for the minimal separated multiple of p is thereby reduced to computing a separated multiple of a homogeneous polynomial. It can be shown that a homogeneous bivariate polynomial has a separated multiple if and only if it is, possibly up to a rescaling of the variables, a product of pairwise distinct cyclotomic polynomials. This can be checked by inspecting its roots.

Finally, the computation of the intersection of $A(I_0)$ and $A(I_1)$ is based on the fact that $A(I_0)$ has finite co-dimension as a $\mathbb{K}$-linear subspace of $\mathbb{K}[x] \times \mathbb{K}[y]$ and that $A(I_1)$ is generated by a single element of $\mathbb{K}[x] \times \mathbb{K}[y]$. Any element of $A(I_0 \cap I_1)$ is therefore a polynomial in the generator of $A(I_1)$, and (all) such polynomials can be found by (repeatedly) making an ansatz and solving a system of linear equations.

The present paper is about the separation problem for ideals I of $\mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_m]$ for arbitrary n and m. Our main result (Thm. 7 and Corollary 9 below) is a constructive proof that shows that $A(I)$ is simple when I is a principal ideal generated by an element of $\mathbb{K}[X, Y] \setminus (\mathbb{K}[X] \cup \mathbb{K}[Y])$. We show that the computation of its generator can be reduced to the bivariate problem. This generalizes the corresponding result from [9]. Observing that the case of 0-dimensional ideals can be treated in the same way as for bivariate polynomials, this then implies that we can proceed as in [9] to compute a finite set of generators for $A(I)$ whenever I is the intersection of a principal ideal and an ideal of dimension zero (Sect. 3). This implies in particular that $A(I)$ is finitely generated for such ideals.

However, in general $A(I)$ is not finitely generated, as shown in Example 5.1 of [9]. This indicates that an extension of the techniques from the case $n = m = 1$ to the case of arbitrary n and m is not straightforward, because there cannot be an algorithm that computes for every given ideal a complete list of generators of $A(I)$ in a finite number of steps. In Sect. 4, we propose two procedures for enumerating generators of $A(I)$. We do not know if there is a procedure that terminates whenever $A(I)$ is finitely generated.

Throughout the paper, $\mathbb{K}$ denotes a computable field of characteristic zero. It is assumed that there is a way to check for a given element of $\mathbb{K}$ whether it is a root of unity. This is a fair assumption when $\mathbb{K}$ is a number field or a rational function field over a number field. We write X for $x_1, \dots, x_n$ and Y for $y_1, \dots, y_m$ and consider the polynomial ring $\mathbb{K}[X, Y]$ in $n + m$ variables. When p is a polynomial in the variable v, we denote the coefficient of v^k in p by $[v^k]p$ for any $k \in \mathbb{N}$.

2 PRINCIPAL IDEALS

Consider a principal ideal $I = \langle p \rangle \subseteq \mathbb{K}[X, Y]$. If the generator belongs to $\mathbb{K}[X]$ or to $\mathbb{K}[Y]$, then the separation problem is not interesting. Let us exclude this case and assume that $p \in \mathbb{K}[X, Y] \setminus (\mathbb{K}[X] \cup \mathbb{K}[Y])$. Our goal is to obtain information about $A(I)$ using our understanding of the case $n = m = 1$. Consider the ring homomorphism

$$\phi\colon \mathbb{K}[X, Y] \to \mathbb{K}(X, Y)[s, t]$$

which maps each x_i to sx_i and each y_j to ty_j. The codomain is a bivariate polynomial ring. Therefore, if $P = \phi(p)$ and $\bar{I}$ is the ideal generated by P in $\mathbb{K}(X, Y)[s, t]$, we know that the algebra $A(\bar{I})$ is simple, and we can compute a generator $(F, G) \in \mathbb{K}(X, Y)[s] \times \mathbb{K}(X, Y)[t]$. If $A(\bar{I})$ is trivial, then so is $A(I)$, because ϕ maps any nontrivial element of $A(I)$ to a nontrivial element of $A(\bar{I})$. Suppose now that $A(\bar{I})$ is nontrivial, and let (F, G) be a generator. As every nonzero $\mathbb{K}(X, Y)$-multiple of a generator is again a generator, we may assume that (F, G) is such that F and G have no denominators and that $F - G$ has no factor in $\mathbb{K}[X, Y]$. Moreover, if (F, G) is a generator, then so is $(F + u, G + u)$ for every $u \in \mathbb{K}(X, Y)$, because $(1, 1)$ is an element of the algebra. We may therefore further assume that (F, G) is such that $[s^0]F = 0$. We can alternatively assume that $[t^0]G = 0$, but we cannot in general assume that $[s^0]F$ and $[t^0]G$ both are zero. However, we can achieve this situation by a change of variables, and it will be convenient to do so. The following lemma provides the justification.

Lemma 1. *Let $Q \in \mathbb{K}^{n+m}$, and let $h\colon \mathbb{K}[X, Y] \to \mathbb{K}[X, Y]$ be the translation by Q. Then h induces an isomorphism of $\mathbb{K}$-algebras between $A(I)$ and $h(A(I))$. In particular, $h(A(I)) = A(h(I))$ and a set of generators of $A(h(I))$ can be obtained from a set of generators of $A(I)$ by applying h to both components of each generator.*

Proof. Observe that h maps $\mathbb{K}[X]$ to $\mathbb{K}[X]$ and $\mathbb{K}[Y]$ to $\mathbb{K}[Y]$, and that h is invertible. Therefore,

$$(f, g) \in A(I) \quad \Longleftrightarrow \quad (h(f), h(g)) \in A(h(I))$$

for all $f \in \mathbb{K}[X]$ and all $g \in \mathbb{K}[Y]$. The claim follows. ∎

If Q is a point on which p vanishes, then $h(p)$ is a polynomial with no constant term. According to the lemma, it suffices to compute $A(\langle h(p) \rangle)$, so we may assume without loss of generality that $p(0) = 0$. We will then also have $P(0) = 0$, and then $(F - G)|_{s=0,t=0} = 0$, so $[s^0]F = [t^0]G$, as desired. If $\mathbb{K}$ is not algebraically closed, a point $Q \in \mathbb{K}^{n+m}$ for which $p(Q) = 0$ may not exist. We may have to replace $\mathbb{K}$ by some algebraic extension $\mathbb{K}(\alpha)$ in order to ensure the existence of a suitable Q. By the following lemma, such algebraic extensions of the coefficient field are harmless.

Lemma 2. *Let $I \subseteq \mathbb{K}[X, Y]$, let α be algebraic over $\mathbb{K}$, and let $J \subseteq \mathbb{K}(\alpha)[X, Y]$ be the ideal generated by I in $\mathbb{K}(\alpha)[X, Y]$. If $A(J)$ is generated by a single element as $\mathbb{K}(\alpha)$-algebra, then it has a generator with coefficients in $\mathbb{K}$, and this generator also generates $A(I)$ as $\mathbb{K}$-algebra.*

Proof. Let $p_1, \dots, p_\ell \in \mathbb{K}[X, Y] \subseteq \mathbb{K}(\alpha)[X, Y]$ be ideal generators of I and consider a generator (f, g) of $A(J)$. We may assume that (f,g) is not a $\mathbb{K}(\alpha)$-multiple of $(1,1)$, because otherwise $A(J)$ is trivial and there is nothing to show.

There are $q_1,\dots,q_\ell \in \mathbb{K}(\alpha)[X,Y]$ such that

$$f - g = q_1 p_1 + \dots + q_\ell p_\ell.$$

If α is of degree d, then $1,\alpha,\dots,\alpha^{d-1}$ is a $\mathbb{K}$-vector space basis of $\mathbb{K}(\alpha)$. Write $f-g=\sum_{i=0}^{d-1}(f_i-g_i)\alpha^i$ for certain $f_i\in\mathbb{K}[X]$ and $g_i\in\mathbb{K}[Y]$, and write $q_j=\sum_{i=0}^{d-1}q_{i,j}\alpha^i$ for certain $q_{i,j}\in\mathbb{K}[X,Y]$, so that

$$\sum_{i=0}^{d-1}(f_i-g_i)\alpha^i = \sum_{i=0}^{d-1}(q_{i,1}p_1+\dots+q_{i,\ell}p_\ell)\alpha^i.$$

Since $p_1,\dots,p_\ell$ are free of α, we can compare coefficients and find that $(f_i,g_i)\in A(J)$. As (f,g) is an algebra generator, each (f_i,g_i) can be expressed as a polynomial of (f,g) with coefficients in $\mathbb{K}(\alpha)$. As the degrees of nontrivial powers of (f,g) exceed those of (f,g), and therefore also those of (f_i,g_i), we have in fact $(f_i,g_i)=u_i(f,g)+v_i(1,1)$ for certain $u_i,v_i\in\mathbb{K}(\alpha)$. Since (f,g) is not a $\mathbb{K}(\alpha)$-multiple of $(1,1)$, at least one (f_i,g_i) is not a $\mathbb{K}(\alpha)$-multiple of $(1,1)$, and we can write (f,g) as a $\mathbb{K}(\alpha)$-linear combination of $(1,1)$ and this (f_i,g_i). Then (f_i,g_i) is a generator of $A(J)$ with coefficients in $\mathbb{K}$.

By $f_i-g_i=q_{i,1}p_1+\dots+q_{i,\ell}p_\ell$, we have $(f_i,g_i)\in A(I)$. Together with $A(I)\subseteq A(J)$, this implies that (f_i,g_i) is also a generator of $A(I)$. ■

Assuming that F,G are such that $[s^0]F=[t^0]G=0$, the question is now what a generator (F,G) of $A(\bar{I})$ implies about $A(I)$. Our answer to this question is Theorem 7, which says that if $A(I)$ is nontrivial, then a generator of $A(I)$ can be obtained from (F,G). In preparation for the proof of this theorem, we need a few lemmas.

Lemma 3. *Let $F\in\mathbb{K}[X,Y][s]$ be such that $[s^0]F=0$. Let the polynomials $u_0,\dots,u_k\in\mathbb{K}[X,Y]$ be such that $u_0+u_1F+\dots+u_kF^k$ has a factor p in $\mathbb{K}[X,Y]$. Suppose that p is not a common factor of $u_0,\dots,u_k$. Then $p\mid F$.*

Proof. Without loss of generality, we may assume that p is irreducible. (If it isn't, replace p by one of its irreducible factors.) We show that the assumption $p\nmid F$ implies that p is a common factor of $u_0,\dots,u_k$. Because of $[s^0]F=0$, the image of F in $(\mathbb{K}[X,Y]/\langle p\rangle)[s]$ is a polynomial of positive degree. Therefore, the images of $1,F,\dots,F^k$ in $(\mathbb{K}[X,Y]/\langle p\rangle)[s]$ are linearly independent over $\mathbb{K}[X,Y]/\langle p\rangle$. As the image of $u_0+u_1F+\dots+u_kF^k$ in $(\mathbb{K}[X,Y]/\langle p\rangle)[s]$ is assumed to be zero, the images of $u_0,\dots,u_k$ must be zero, which means $p\mid u_i$ for all i, as promised. ■

Lemma 4. *Let $(F,G)\in\mathbb{K}[X,Y][s]\times\mathbb{K}[X,Y][t]$ be such that $[s^0]F=[t^0]G=0$. Suppose that $F-G$ has no factor in $\mathbb{K}[X,Y]$. Let $u_0,\dots,u_k\in\mathbb{K}(X,Y)$ be such that*

$$u_0\binom{1}{1}+u_1\binom{F}{G}+\dots+u_k\binom{F^k}{G^k}\in\mathbb{K}[X,Y][s]\times\mathbb{K}[X,Y][t].$$

Then $u_0,\dots,u_k$ are in fact in $\mathbb{K}[X,Y]$.

Proof. Suppose otherwise and let $d\in\mathbb{K}[X,Y]$ be the least common denominator of $u_0,\dots,u_k$ and p be an irreducible factor of d. Then

$$p\mid du_0+du_1F+\dots+du_kF^k$$

and

$$p\mid du_0+du_1G+\dots+du_kG^k$$

and $p\nmid du_i$ for at least one i. By the previous lemma, this implies $p\mid F$ and $p\mid G$. But then $p\mid F-G$, in contradiction to the assumption. ■

Lemma 5. *Let $F\in\mathbb{K}[X,Y][s]$ be such that $[s^0]F=0$. Let k be a positive integer. Suppose that $[s^i]F^k$ is in $\mathbb{K}[X]$ for every $i>(k-1)\deg_s F$. Then $F\in\mathbb{K}[X][s]$.*

Proof. Write $F=c_1s+\dots+c_ds^d$ with $d=\deg_s F$ and $c_1,\dots,c_d\in\mathbb{K}[X,Y]$. We have $[s^{dk}]F^k=c_d^k$, which can only be in $\mathbb{K}[X]$ if c_d is. For $i=1,\dots,d-1$, the coefficient of s^{dk-i} in F^k is

$$kc_d^{k-1}c_{d-i}+p(c_{d-i+1},c_{d-i+2},\dots,c_d)$$

for a certain polynomial p. This follows from the multinomial theorem. By induction on i, it implies that also $c_1,c_2,\dots,c_{d-1}$ belong to $\mathbb{K}[X]$, as claimed. ■

Lemma 6. *Let $(F,G)\in\mathbb{K}[X,Y][s]\times\mathbb{K}[X,Y][t]$ be such that $[s^0]F=[t^0]G=0$. Suppose that $F-G$ has no factor in $\mathbb{K}[X,Y]$. Let $u_0,\dots,u_k\in\mathbb{K}[X,Y]$ be such that*

$$u_0\binom{1}{1}+u_1\binom{F}{G}+\dots+u_k\binom{F^k}{G^k}\in\mathbb{K}[X][s]\times\mathbb{K}[Y][t].$$

Then $F\in\mathbb{K}[X][s]$, $G\in\mathbb{K}[Y][s]$, and $u_0,\dots,u_k\in\mathbb{K}$.

Proof. The $\deg_s F$ highest order terms of F^k (w.r.t. s) exceed the highest order terms of the lower powers of F. (Note that the $u_0,\dots,u_k$ do not contain s.) Since $u_0+u_1F+\dots+u_kF^k$ belongs to $\mathbb{K}[X][s]$ by assumption, neither u_k nor the coefficients of the $\deg_s F$ highest order terms of F^k can contain Y. Therefore, by Lemma 5, F belongs to $\mathbb{K}[X][s]$.

As the s-degrees of the powers of F are pairwise distinct, it follows furthermore that none of the $u_0,\dots,u_k$ can contain any Y.

By the same reasoning, we get that G belongs to $\mathbb{K}[Y][t]$ and that none of the $u_0,\dots,u_k$ can contain any X, so in fact, we have $u_0,\dots,u_k\in\mathbb{K}$. ■

Theorem 7. *Let $p\in\mathbb{K}[X,Y]\setminus(\mathbb{K}[X]\cup\mathbb{K}[Y])$ be such that $p(0)=0$. Let $I=\langle p\rangle$, $P=\phi(p)$, and $\bar{I}=\langle P\rangle\subseteq\mathbb{K}(X,Y)[s,t]$. Suppose that $A(\bar{I})$ is not trivial and let $(F,G)\in\mathbb{K}(X,Y)[s]\times\mathbb{K}(X,Y)[t]$ be a generator such that F and G have no denominator, $F-G$ has no factor in $\mathbb{K}[X,Y]$, and $F|_{s=0}=G|_{t=0}=0$. Then $A(I)$ is nontrivial if and only if $F\in\mathbb{K}[X][s]$ and $G\in\mathbb{K}[Y][t]$ and $F|_{s=1}\neq G|_{t=1}$. In this case, $(F|_{s=1},G|_{t=1})$ is a generator of $A(I)$.*

Proof. "⇐": If F and G are as in the assumption, then $F-G$ is a $\mathbb{K}(X,Y)[s,t]$-multiple of P, say $F-G=QP$ for some $Q\in\mathbb{K}(X,Y)[s,t]$. Since P has no factor in $\mathbb{K}[X,Y]$ and $F-G$ has no denominator, it follows that Q has no denominator. Therefore, setting $s=1$ and $t=1$ shows that $F|_{s=1}-G|_{t=1}$ is a separated multiple of p and therefore an element of I. It follows that $A(I)$ contains $(F|_{s=1},G|_{t=1})$. It remains to show that this is not a $\mathbb{K}$-multiple of $(1,1)$. If it were, then $F|_{s=1}-G|_{t=1}=0$, which is excluded by assumption on F and G.

"⇒": If $A(I)$ is nontrivial, it contains some pair $(f,g) \in \mathbb{K}[X] \times \mathbb{K}[Y]$ that is not a $\mathbb{K}$-multiple of $(1,1)$. Then $(\phi(f), \phi(g))$ is a nontrivial element of $A(\bar{I})$. Then there are $u_0, \dots, u_k \in \mathbb{K}(X,Y)$ such that

$$\begin{pmatrix}\phi(f)\\ \phi(g)\end{pmatrix} = u_0 \begin{pmatrix}1\\1\end{pmatrix} + u_1 \begin{pmatrix}F\\G\end{pmatrix} + \cdots + u_k \begin{pmatrix}F^k\\G^k\end{pmatrix}.$$

The left hand side has no denominator in $\mathbb{K}[X,Y]$, because f and g are polynomials. Therefore, by Lemma 4, $u_0, \dots, u_k$ belong to $\mathbb{K}[X,Y]$. Next, by Lemma 6, it follows that $F \in \mathbb{K}[X][s]$, $G \in \mathbb{K}[Y][t]$, and $u_0, \dots, u_k \in \mathbb{K}$.

It remains to show that $F|_{s=1} \neq G|_{t=1}$. If they were equal, then they would be in $\mathbb{K}$, because $F|_{s=1}$ does not contain Y and $G|_{t=1}$ does not contain X. Then $(F|_{s=1}, G|_{t=1})$ would be a $\mathbb{K}$-multiple of $(1,1)$, and

$$u_0 \begin{pmatrix}1\\1\end{pmatrix} + u_1 \begin{pmatrix}F|_{s=1}\\G|_{t=1}\end{pmatrix} + \cdots + u_k \begin{pmatrix}(F|_{s=1})^k\\(G|_{t=1})^k\end{pmatrix}$$

would also be a $\mathbb{K}$-multiple of $(1,1)$. This is impossible, because (f,g) is assumed not to be a $\mathbb{K}$-multiple of $(1,1)$.

This completes the argument for the direction "⇒". In this argument, we have shown that every element of $A(I)$ can be written as a polynomial in $(F|_{s=1}, G|_{t=1})$. This construction also implies the additional claim about the generator of $A(I)$. ■

Example 8. *(1) If I is generated by $x_1^2+2x_1x_2+x_2^2+x_1y+x_2y+y^2$, then both $A(I)$ and $A(\bar{I})$ are nontrivial. They are generated by $((x_1+x_2)^3, y^3)$ and $((x_1+x_2)^3s^3, y^3t^3)$, respectively.*
(2) If I is generated by $x_1^2+x_1x_2+x_2^2+x_1y+x_2+y^2$, then $A(I)$ and $A(\bar{I})$ both are trivial.

There is no example where $A(\bar{I})$ is trivial but $A(I)$ is not, because ϕ maps nontrivial elements of $A(I)$ to nontrivial elements of $A(\bar{I})$. Conversely, we have also not found any example of a principal ideal I where $A(I)$ is trivial but $A(\bar{I})$ is not, and we suspect that no such example exists. However, as we will see in Example 22, there are such examples when I is not principal.

Corollary 9. *For every $p \in \mathbb{K}[X,Y] \setminus (\mathbb{K}[X] \cup \mathbb{K}[Y])$, the algebra $A(\langle p \rangle)$ is simple.*

Proof. We argue that all assumptions in Thm. 7 are "without loss of generality." First, by Lemmas 1 and 2, we can assume that $p(0)=0$. If $A(\langle p \rangle)$ is trivial, there is nothing to prove. If $A(\langle p \rangle)$ is not trivial, then so is $A(\langle P \rangle)$. If (F,G) is any generator of $A(\langle P \rangle)$, then so is every $\alpha(F,G)+\beta(1,1)$ for any choice $\alpha \in \mathbb{K}(X,Y) \setminus \{0\}$ and $\beta \in \mathbb{K}(X,Y)$. By a suitable choice of α and β, we can meet the assumptions imposed on (F,G) in Thm. 7. According to the theorem, then $(F|_{s=1}, G|_{t=1})$ is a generator of $A(I)$. ■

The assumption that p does not belong to $\mathbb{K}[X]$ or to $\mathbb{K}[Y]$ is necessary. For example, if $p \in \mathbb{K}[X]$, the algebra $A(I)$ consists of all $(f+c, c)$ where $f \in \mathbb{K}[X] \cdot p$ and $c \in \mathbb{K}$, and while this is a concise description of $A(I)$, such an algebra need not be finitely generated. To see this, consider $p = x_1x_2 \in \mathbb{K}[x_1,x_2]$. The x_2-degree of any nontrivial power of any nontrivial $\mathbb{K}[x_1,x_2]$-multiple of p will be at least 2, so every element $x_1^k x_2$ of the algebra can only be a $\mathbb{K}$-linear combination of generators. Because of $\dim_{\mathbb{K}} x_1x_2\mathbb{K}[x_1] = \infty$, there must be infinitely many generators.

We have just seen that the algebra $A(I)$ is simple whenever the ideal I is generated by a polynomial p of $\mathbb{K}[X,Y]$ that is not an element of $\mathbb{K}[X] \cup \mathbb{K}[Y]$. We now give a characterization of the generator of $A(I)$ in terms of certain divisibility relations. It is based on the following generalization of a theorem by Fried and MacRae [15]. For a proof we refer to [16]. See also [2].

Theorem 10. *Let $f, F \in \mathbb{K}[X]$ and $g, G \in \mathbb{K}[Y]$ be non-constant polynomials. The following are equivalent:*
(1) There exists $h \in \mathbb{K}[t]$ such that $F = h(f)$ and $G = h(g)$.
(2) $f-g$ divides $F-G$ in $\mathbb{K}[X,Y]$.

Let $F-G \in I \cap (\mathbb{K}[X] + \mathbb{K}[Y])$ such that $(F,G) \in A(I)$. If $A(I)$ is simple and generated by $(f,g) \in \mathbb{K}[X] \times \mathbb{K}[Y]$, then $(F,G) = (h(f), h(g))$ for some $h \in \mathbb{K}[t]$. The previous theorem implies that $f-g$ divides $F-G$ in $\mathbb{K}[X,Y]$. As a consequence of Corollary 9 and Theorem 10 we therefore have the following.

Corollary 11. *Let $p \in \mathbb{K}[X,Y]$. If p has a separated multiple, then it has one that divides any other of its separated multiples.*

If p has a separated multiple and the corresponding algebra is generated by (f,g), then $f-g$ is referred to as the *minimal separated multiple* of p. It is unique up to a multiplicative constant.

3 IDEALS OF DIMENSION ZERO

For ideals of dimension zero, the technique proposed in [9] for the case $n=m=1$ generalizes more or less literally to arbitrary n and m. We therefore give only an informal summary here and refer to [9] for a more formal discussion.

If $I \subseteq \mathbb{K}[X,Y]$ has dimension zero, then it contains a nonzero univariate polynomial for each of the variables. Denote these polynomials by $p_1, \dots, p_n, q_1, \dots, q_m$. Being univariate, these polynomials are in particular separated. This implies that $A(I)$ contains at least all pairs (p,q) where p is a $\mathbb{K}[X]$-linear combination of $p_1, \dots, p_n$ and q is a $\mathbb{K}[Y]$-linear combination of $q_1, \dots, q_m$. If (f,g) is any other element of $A(I)$, we can add an arbitrary $\mathbb{K}[X]$-linear combination of $p_1, \dots, p_n$ to f and an arbitrary $\mathbb{K}[Y]$-linear combination of $q_1, \dots, q_m$ to g and obtain another element of $A(I)$. It is therefore enough to search for elements (f,g) of $A(I)$ with $\deg_{x_i} f < \deg_{x_i} p_i$ and $\deg_{y_j} g < \deg_{y_j} q_j$ for all i and j. This restricts the search to a finite dimensional vector space. We can make an ansatz with undetermined coefficients for f and g, compute its normal form with respect to a Gröbner basis of I, equate its coefficients to zero and solve the resulting linear system for the unknown coefficients in $\mathbb{K}$. The solutions together with the $p_1, \dots, p_n$ and their X-multiples as well as the $q_1, \dots, q_m$ and their Y-multiples then form a set of generators of $A(I)$.

Example 12. *Let $I \subseteq \mathbb{K}[x_1,x_2,y_1,y_2]$ be the ideal generated by*

$$x_1+x_2+y_1+y_2,$$
$$x_1x_2+x_1y_1+x_1y_2+x_2y_1+x_2y_2+y_1y_2,$$
$$x_1x_2y_1+x_1x_2y_2+x_1y_1y_2+x_2y_1y_2,$$
$$x_1x_2y_1y_2-1.$$

Its elimination ideals are

$$I \cap \mathbb{K}[x_1,x_2] = \langle x_1^3+x_1^2x_2+x_1x_2^2+x_2^3, x_2^4+1\rangle,$$
$$I \cap \mathbb{K}[y_1,y_2] = \langle y_1^3+y_1^2y_2+y_1y_2^2+y_2^3, y_2^4+1\rangle.$$

Denoting the two generators of $I \cap \mathbb{K}[x_1, x_2]$ by p_1, p_2, respectively, polynomial division shows that this ideal is generated as a $\mathbb{K}$-algebra by $x_1^i x_2^j p_1$ for $i = 0, 1, 2$ and $j = 0, 1, 2, 3$ and $x_1^i x_2^j p_2$ for $i = 0, 1, 2, 3$ and $j = 0, 1, 2$. Similarly, we get a finite set of generators for the other elimination ideal.

It remains to check whether $A(I)$ contains any elements (p, q) where all terms in p have x_1-degree less than 3 and x_2-degree less than 4, and all terms in q have y_1-degree less than 3 and y_2-degree less than 4. It turns out that the following pairs form a basis of the $\mathbb{K}$-vector space of all these elements:

$$\begin{pmatrix} x_1^2 + x_2^2 \\ -y_1^2 - y_2^2 \end{pmatrix}, \begin{pmatrix} x_1 + x_2 \\ -y_1 - y_2 \end{pmatrix}, \begin{pmatrix} x_1 x_2 \\ y_1^2 + y_1 y_2 + y_2^2 \end{pmatrix}, \begin{pmatrix} x_1^2 x_2 + x_1 x_2^2 \\ -y_1^2 y_2 - y_1 y_2^2 \end{pmatrix}, \begin{pmatrix} x_1^2 x_2^2 \\ y_1^2 y_2^2 \end{pmatrix}.$$

These pairs together with the generators of the two elimination ideals form a finite set of generators of $A(I)$.

As a $\mathbb{K}$-linear subspace of $\mathbb{K}[X] \times \mathbb{K}[Y]$, the algebra $A(I)$ for an ideal I of dimension zero has finite co-dimension. From the algebra generators of $A(I)$ computed as described above, we can obtain a basis of a vector space V such that $V \oplus A(I) = \mathbb{K}[X] \times \mathbb{K}[Y]$, and for every $(f, g) \in \mathbb{K}[X] \times \mathbb{K}[Y]$ we can compute a pair $(\tilde{f}, \tilde{g}) \in V$ such that $(f, g) - (\tilde{f}, \tilde{g}) \in A(I)$. This amounts to Lemma 2.4 of [9].

In the case $n = m = 1$, every ideal can be written as the intersection of an ideal of dimension zero and a principal ideal. This is no longer true in the general case. However, if an ideal $I \subseteq \mathbb{K}[X, Y]$ happens to be the intersection of an ideal $I_0 \subseteq \mathbb{K}[X, Y]$ of dimension zero and a principal ideal $I_1 \subseteq \mathbb{K}[X, Y]$, then we can continue as in Sect. 4 of [9] and obtain a finite set of generators for $A(I)$.

Algorithm 4.3 of [9] relies on $A(I_0 \cap I_1) = A(I_0) \cap A(I_1)$ and uses that $A(I_0)$ has finite codimension and $A(I_1)$ is generated by a single element. It makes an ansatz for a polynomial in the generator of $A(I_1)$, then finds an equivalent element in V and forces that element to zero. This results in a system of linear equations for the coefficients of the ansatz, whose solutions give rise to elements of $A(I_0) \cap A(I_1)$. The search is repeated with an ansatz of larger and larger degree, but always excluding all monomials that are $\mathbb{N}$-linear combinations of degrees of generators found earlier. Since $(\mathbb{N}, +)$ is a noetherian monoid, after finitely many repetitions there are no monomials left and the list of generators is complete.

The correctness of this algorithm does not depend on the assumption $n = m = 1$ but extends literally to the case of arbitrary n and m. We can therefore record the following corollary to Thm. 7.

Corollary 13. *Let $I \subseteq \mathbb{K}[X, Y]$ be such that $I = I_0 \cap I_1$ for some ideal I_0 of dimension zero and some principal ideal I_1 whose generator is not in $\mathbb{K}[X] \cup \mathbb{K}[Y]$. Then $A(I)$ is finitely generated, and there is an algorithm for computing a finite set of generators.*

Example 14. *As a minimalistic example, consider the ideal $I = I_0 \cap I_1 \subseteq \mathbb{K}[x_1, x_2, y_1, y_2]$ with*

$$I_0 = \langle x_1 - 1, x_2 - 1, y_1 - 2, y_2 - 2 \rangle \quad \text{and} \quad I_1 = \langle x_1^2 + x_1 y_2 + y_2^2 \rangle.$$

The algebra $A(I_0)$ is generated by $(x_1 - 1, 0), (x_2 - 1, 0), (0, y_1 - 2), (0, y_2 - 2)$, and the algebra $A(I_1)$ is generated by $g = (x_1^3, y_2^3)$. We need to find all univariate polynomials p such that $p(g) \in A(I_0)$.

Modulo the $\mathbb{K}$-vector space $A(I_0)$, the element g itself is equivalent to $(0, 7)$, and the element g^2 is equivalent to $(0, 63)$. Therefore, $g^2 - 9g$ is an element of $A(I_0)$. This reduces the search to polynomials involving only odd powers of g. As the element g^3 is equivalent modulo $A(I_0)$ to $(0, 511)$, we find the additional element $g^3 - 73g$ of $A(I)$. Since $2\mathbb{N} + 3\mathbb{N} = \mathbb{N} \setminus \{0, 1\}$ and $A(I_0)$ does not contain any element of the form $\alpha g + \beta$, we can conclude that $A(I) = \mathbb{K}[g^2 - 9g, g^3 - 73g]$.

4 ARBITRARY IDEALS

For an arbitrary ideal I of $\mathbb{K}[X, Y]$, the algebra of separated polynomials is in general not finitely generated. It is therefore impossible to give an algorithm that computes a complete basis in a finite number of steps. The best we can hope for is a procedure that enumerates a set of generators and runs forever if $A(I)$ is not finitely generated, yet terminates if $A(I)$ is finitely generated. Unfortunately, we cannot offer such a procedure. However, if we drop the latter requirement, it is not hard to come up with an algorithmic solution.

For any fixed $d \in \mathbb{N}$, we can find all $(f, g) \in A(I)$ where f and g have total degree at most d by linear algebra, similar as in the case of zero dimensional ideals. Make an ansatz

$$f = \sum_{e_1 + \cdots + e_n \leq d} \alpha_{e_1, \ldots, e_n} x_1^{e_1} \cdots x_n^{e_n},$$
$$g = \sum_{e_1 + \cdots + e_m \leq d} \beta_{e_1, \ldots, e_m} y_1^{e_1} \cdots y_m^{e_m}$$

with undetermined coefficients $\alpha_{e_1, \ldots, e_n}, \beta_{e_1, \ldots, e_n}$ and compute the normal form of $f - g$ with respect to a Gröbner basis of I. The result will be a polynomial in X, Y whose coefficients are $\mathbb{K}$-linear combinations of the undetermined coefficients. Force these coefficients to zero and solve the resulting linear system. The result translates into a basis of the $\mathbb{K}$-vector space of all pairs $(f, g) \in A(I)$ with f and g of total degree at most d. By repeating this computation for $d = 1, 2, 3, \ldots$ indefinitely, we will get a set of generators of $A(I)$. In fact, these generators generate $A(I)$ not only as $\mathbb{K}$-algebra but even as $\mathbb{K}$-vector space. This is more than we want. We can eliminate some of the redundance in the output by discarding from the ansatz all terms that are powers of leading terms of generators that have been found in earlier iterations, but the approach nevertheless seems brutal as the size of the linear system will grow rapidly with increasing d.

An alternative procedure for enumerating algebra generators of $A(I)$ uses Gröbner bases instead of linear algebra. For this procedure, we reuse the idea of Sect. 2 and exploit the fact that we know how to compute a (finite) set of generators of $A(\bar{I})$ for every ideal $\bar{I}$ of a bivariate polynomial ring.

Like in Sect. 2, we consider the homomorphism

$$\phi\colon \mathbb{K}[X, Y] \to \mathbb{K}(X, Y)[s, t]$$

which maps each x_i to sx_i and each y_j to ty_j. Let $p_1, \ldots, p_\ell \in \mathbb{K}[X, Y]$ be generators of $I \subseteq \mathbb{K}[X, Y]$, let $P_i = \phi(p_i)$ for $i = 1, \ldots, \ell$, and let $\bar{I}$ be the ideal generated by $P_1, \ldots, P_\ell$ in $\mathbb{K}(X, Y)[s, t]$. The algebra $A(\bar{I})$ is finitely generated. Let $B_1, \ldots, B_u$ be a choice of generators. The homomorphism ϕ maps every element of $A(I)$ to an element of $A(\bar{I})$, and every such element can be written as a polynomial in $B_1, \ldots, B_u$ with coefficients in $\mathbb{K}(X, Y)$. Therefore, in order to find elements of $A(I)$, we search for elements of $\mathbb{K}(X, Y)[B_1, \ldots, B_u]$ that become elements of $A(I)$ after setting s and t to 1. This can be done effectively as soon as we can solve the following problem:

Problem 15. *Given: generators $p_1, \dots, p_\ell$ of I and some elements $(F_1, G_1), \dots, (F_k, G_k)$ of $A(\bar{I})$*

Find: a $\mathbb{K}$-vector space basis of the set of all elements of $A(I)$ that can be obtained from a $\mathbb{K}(X, Y)$-linear combination of $(F_1, G_1), \dots, (F_k, G_k)$ by setting s and t to 1.

With an algorithm for solving this problem, we can get a procedure that enumerates generators of $A(I)$. For $d = 1, 2, \dots$ in turn, the procedure calls the algorithm with all monomials in $B_1, \dots, B_u$ of degree at most d as $(F_1, G_1), \dots, (F_k, G_k)$.

In the remainder of this section, we discuss an algorithm for solving Problem 15. We first give a high-level description of the algorithm and prove that the approach is sound and complete. Afterwards, we show that each of the steps can be effectively computed.

Algorithm 16. *Input/Output: as specified in Problem 15*

1. *Compute a basis of the $\mathbb{K}[X, Y]$-module*
$$M := \operatorname{span}_{\mathbb{K}(X,Y)}(F_1 - G_1, \dots, F_k - G_k) \cap \underbrace{\langle \phi(p_1), \dots, \phi(p_\ell) \rangle}_{\subseteq \mathbb{K}[X,Y][s,t]}.$$
Write the elements $F - G$ of M in the form (F, G), so that M becomes a submodule of $\mathbb{K}[X, Y][s] \times \mathbb{K}[X, Y][t]$. (Include the pair $(1, 1)$ among the generators.)
2. *Compute bases of the $\mathbb{K}[X]$-module*
$$M_X := \{ (F, G) \in M : F \in \mathbb{K}[X][s] \}$$
and the $\mathbb{K}[Y]$-module
$$M_Y := \{ (F, G) \in M : G \in \mathbb{K}[Y][t] \}.$$
3. *Compute a basis of the $\mathbb{K}$-vector space $M_X \cap M_Y$.*
4. *Set $s = t = 1$ in the basis elements and return the result.*

Theorem 17. *Alg. 16 is sound and complete.*

Proof. *Soundness.* We show that every pair (f, g) in the output indeed belongs to $A(I)$. If (f, g) is an element of the output, then it is clear from Step 3 and the definition of M_X, M_Y that $f \in \mathbb{K}[X]$ and $g \in \mathbb{K}[Y]$. We need to show that $f - g \in I$. Let F, G be the polynomials from which f and g are obtained by setting s and t to 1. Then (F, G) is an element of M, therefore $F - G$ is an element of $\langle \phi(p_1), \dots, \phi(p_l) \rangle$, and therefore $f - g$ is an element of I.

Completeness. We show that if $(f, g) \in A(I)$ is such that the corresponding $(F, G) \in \mathbb{K}(X, Y)[s] \times \mathbb{K}(X, Y)[t]$ is a $\mathbb{K}(X, Y)$-linear combination of the elements $(F_1, G_1), \dots, (F_k, G_k)$, then it is a $\mathbb{K}$-linear combination of the output pairs. By assumption, $F - G \in \operatorname{span}_{\mathbb{K}(X,Y)}(F_1 - G_1, \dots, F_k - G_k)$. Also, since $f - g \in I$, we have $F - G \in \langle \phi(p_1), \dots, \phi(p_l) \rangle$. Therefore, (F, G) belongs to the module M computed in Step 1. Moreover, we have $F \in \mathbb{K}[X][s]$ and $G \in \mathbb{K}[Y][t]$ because $f \in \mathbb{K}[X]$ and $g \in \mathbb{K}[Y]$, so $(F, G) \in M_X \cap M_Y$. The claim follows. ∎

Step 4 of Alg. 16 is trivial, and Step 2 is a standard application of Gröbner bases. For example, in order to get a basis of M_X, it suffices to compute a Gröbner basis of M with respect to a TOP term order that eliminates Y, and to discard from it all elements which have a Y in the first component [1, Definition 3.5.2]. Steps 1 and 3 require more explanation.

For Step 1, we divide the problem into two substeps. First we compute a basis of the $\mathbb{K}[X, Y]$-module
$$N := \operatorname{span}_{\mathbb{K}(X,Y)}(F_1 - G_1, \dots, F_k - G_k) \cap \mathbb{K}[X, Y][s, t],$$
and then we obtain a basis of M by computing the intersection of this N with the ideal generated by $\phi(p_1), \dots, \phi(p_\ell)$ in $\mathbb{K}[X, Y][s, t]$. The two substeps are provided by the following lemmas.

Lemma 18. *For any given $q_1, \dots, q_k \in \mathbb{K}[X, Y][s, t]$, we can compute a basis of the $\mathbb{K}[X, Y]$-module*
$$\operatorname{span}_{\mathbb{K}(X,Y)}(q_1, \dots, q_k) \cap \mathbb{K}[X, Y][s, t].$$

Proof. As only finitely many monomials appear in $q_1, \dots, q_k$, we can view them as elements of a finitely generated $\mathbb{K}[X, Y]$-submodule of $\mathbb{K}[X, Y][s, t]$. We may identify this submodule with $\mathbb{K}[X, Y]^n$ for some n. In this identification, $\operatorname{span}_{\mathbb{K}(X,Y)}(q_1, \dots, q_k)$ is a certain subspace of $\mathbb{K}(X, Y)^n$. Let $A \in \mathbb{K}(X, Y)^{m \times n}$ be a matrix whose kernel is this subspace. Such a matrix exists and can be easily constructed by means of linear algebra. As multiplying A by a nonzero element of $\mathbb{K}(X, Y)$ does not change the kernel, we may assume that A belongs to $\mathbb{K}[X, Y]^{m \times n}$. Let $a_1, \dots, a_n \in \mathbb{K}[X, Y]^m$ be its columns. Then
$$\operatorname{span}_{\mathbb{K}(X,Y)}(q_1, \dots, q_k) \cap \mathbb{K}[X, Y]^n = \operatorname{Syz}(a_1, \dots, a_m).$$
The computation of a basis of the syzygy module is a standard application of Gröbner bases. ∎

Lemma 19. *Let N be a finitely generated $\mathbb{K}[X, Y]$-submodule of $\mathbb{K}[X, Y][s, t]$ and let J be an ideal of $\mathbb{K}[X, Y][s, t]$. Then $N \cap J$ is a finitely generated submodule of $\mathbb{K}[X, Y][s, t]$, and we can compute a basis of it from a module basis of N and an ideal basis of J.*

Proof. Let $n_1, \dots, n_r$ be module generators of N and $p_1, \dots, p_k$ be ideal generators of J. An element q of $\mathbb{K}[X, Y][s, t]$ belongs to $N \cap J$ if and only if there are $\alpha_1, \dots, \alpha_r \in \mathbb{K}[X, Y]$ and $\beta_1, \dots, \beta_k \in \mathbb{K}[X, Y][s, t]$ such that
$$\begin{aligned} q &= \alpha_1 n_1 + \dots + \alpha_r n_r \\ &= \beta_1 p_1 + \dots + \beta_k p_k. \end{aligned}$$
By taking the difference of these two representations of q, we see that the relevant tuples $(\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_k)$ are precisely the elements of
$$\operatorname{Syz}(n_1, \dots, n_r, -p_1, \dots, -p_k) \cap \mathbb{K}[X, Y]^r \times \mathbb{K}[X, Y][s, t]^k.$$
We can first compute a Gröbner basis of the syzygy module in $\mathbb{K}[X, Y][s, t]^{r+k}$, then discard the lower k coordinates, and then eliminate s and t. This yields a basis of the $\mathbb{K}[X, Y]$-module that contains a tuple $(\alpha_1, \dots, \alpha_r) \in \mathbb{K}[X, Y]^r$ if and only if $\alpha_1 n_1 + \dots + \alpha_r n_r \in N \cap J$. A basis of this module thus translates into a basis of $N \cap J$. ∎

We now turn to Step 3 of Alg. 16, where we have to compute the intersection of a finitely generated $\mathbb{K}[X]$-submodule M_X of $\mathbb{K}[X, Y][s, t]^2$ with a finitely generated $\mathbb{K}[Y]$-submodule M_Y of $\mathbb{K}[X, Y][s, t]^2$. The result is a $\mathbb{K}$-vector space, and the task is to compute a basis of this vector space.

Let $b_1, \ldots, b_u$ be a basis of M_X and $c_1, \ldots, c_v$ be a basis of M_Y. Like in the proof of Lemma 18, we seek $\alpha_1, \ldots, \alpha_u \in \mathbb{K}[X]$ and $\beta_1, \ldots, \beta_v \in \mathbb{K}[Y]$ such that

$$\alpha_1 b_1 + \cdots + \alpha_u b_u = \beta_1 c_1 + \cdots + \beta_v c_v. \tag{1}$$

If we can get hold of a finite set of monomials that contains all the monomials which can possibly appear in $\alpha_1, \ldots, \alpha_u, \beta_1, \ldots, \beta_v$, then we can find $\alpha_1, \ldots, \alpha_u, \beta_1, \ldots, \beta_v$ by making an ansatz with undetermined coefficients, plugging it into the above equation, comparing coefficients, and solving a linear system over $\mathbb{K}$. Every solution vector translates into a solution $(\alpha_1, \ldots, \alpha_u, \beta_1, \ldots, \beta_v) \in \mathbb{K}[X]^u \times \mathbb{K}[Y]^v$ of equation (1), and every such solution translates into an element $\alpha_1 b_1 + \cdots + \alpha_u b_u$ of the intersection $M_X \cap M_Y$. The following lemma tells us how to find the required monomials.

Lemma 20. *Let $(\alpha_1, \ldots, \alpha_u, \beta_1, \ldots, \beta_v) \in \mathbb{K}[X]^u \times \mathbb{K}[Y]^v$ be a solution of (1), let $i \in \{1, \ldots, v\}$, and let $\tau = y_1^{e_1} \cdots y_m^{e_m}$ be a monomial appearing in β_i. Let G be a Gröbner basis of*

$$\operatorname{Syz}(b_1, \ldots, b_u, -c_1, \ldots, -c_v) \subseteq \mathbb{K}[X, Y]^{u+v}$$

with respect to a TOP order that eliminates Y. Then there exists a monomial $\sigma = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ and an element $g \in G$ such that the first u components are free of Y and the $(u+i)$th component contains the monomial $\sigma\tau$.

Proof. A vector in $\mathbb{K}[X]^u \times \mathbb{K}[Y]^v$ is a solution of (1) if and only if it belongs to the syzygy module. The given solution q must therefore reduce to zero modulo G. By the choice of the term order, only elements of G whose first u components are free of Y will be used during the reduction. Call these elements $g_1, \ldots, g_\ell$. Again by the choice of the term order, these elements of G will only be multiplied by elements of $\mathbb{K}[X]$ during the reduction, i.e., we will have $q = q_1 g_1 + \cdots + q_\ell g_\ell$ for certain $q_1, \ldots, q_\ell \in \mathbb{K}[X]$. The $(u+i)$th component of q contains the monomial τ, so this monomial appears in a $\mathbb{K}[X]$-linear combination of the $(u+i)$th components of $g_1, \ldots, g_\ell$. As $\mathbb{K}[X]$-linear combinations cannot create new Y-monomials, some $\mathbb{K}[X]$-multiple of τ must already appear in at least one of the $g_1, \ldots, g_\ell$. ■

With the help of this lemma, we obtain for each $i \in \{1, \ldots, v\}$ a finite list of candidates of monomials that may appear in β_i. Applying the lemma again with the roles of X and Y exchanged, we can also obtain for each $i \in \{1, \ldots, u\}$ a finite list of candidates of monomials that may appear in α_i. This is all we need in order to complete Step 3 of Alg. 16.

Example 21. *Let us use Alg. 16 to search for a nontrivial element of $A(I)$ for the ideal*

$$I = \langle y_1^2 - x_2 y_2, x_2^2 - x_1 y_1, x_1^4 x_2 y_1 - x_2 y_1 y_2^4 \rangle.$$

The corresponding ideal $\bar{I}$ has dimension 0, and $A(\bar{I})$ contains $(s^6, 0)$ and $(0, t^6)$. Taking these elements as (F_1, G_1) and (F_2, G_2), we find in Step 1 that M is generated by the following vectors:

$$\begin{pmatrix} 0 \\ x_2 y_1^4 t^6 - x_1 y_1^3 y_2 t^6 \end{pmatrix}, \begin{pmatrix} x_2^4 y_1 s^6 - x_1 x_2^3 y_2 s^6 \\ 0 \end{pmatrix}, \begin{pmatrix} x_1^3 x_2^3 s^6 \\ y_1^3 y_2^3 t^6 \end{pmatrix},$$
$$\begin{pmatrix} x_2^6 y_2^6 s^6 \\ y_1^{12} t^6 \end{pmatrix}, \begin{pmatrix} x_2^7 y_2^5 s^6 \\ x_1 y_1^{11} t^6 \end{pmatrix}, \begin{pmatrix} x_2^8 y_2^4 s^6 \\ x_1^2 y_1^{10} t^6 \end{pmatrix}, \begin{pmatrix} x_2^9 y_2^3 s^6 \\ x_1^3 y_1^9 t^6 \end{pmatrix},$$
$$\begin{pmatrix} x_2^{10} y_2^2 s^6 \\ x_1^4 y_1^8 t^6 \end{pmatrix}, \begin{pmatrix} x_2^{11} y_2 s^6 \\ x_1^5 y_1^7 t^6 \end{pmatrix}, \begin{pmatrix} x_2^{12} s^6 \\ x_1^6 y_1^6 t^6 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

In Step 2, we find

$$M_X = \left\langle \begin{pmatrix} 0 \\ x_2 y_1^4 t^6 - x_1 y_1^3 y_2 t^6 \end{pmatrix}, \begin{pmatrix} x_1^3 x_2^3 s^6 \\ y_1^3 y_2^3 t^6 \end{pmatrix}, \begin{pmatrix} x_2^{12} s^6 \\ x_1^6 y_1^6 t^6 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\rangle$$

and

$$M_Y = \left\langle \begin{pmatrix} x_2^4 y_1 s^6 - x_1 x_2^3 y_2 s^6 \\ 0 \end{pmatrix}, \begin{pmatrix} x_1^3 x_2^3 s^6 \\ y_1^3 y_2^3 t^6 \end{pmatrix}, \begin{pmatrix} x_2^6 y_2^6 t^6 \\ y_1^{12} t^6 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\rangle$$

Step 3 yields

$$M_X \cap M_Y = \operatorname{span}_{\mathbb{K}} \left(\begin{pmatrix} x_1^3 x_2^3 s^6 \\ y_1^3 y_2^3 t^6 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right),$$

and the final result is $(x_1^3 x_2^3, y_1^3 y_2^3)$.

At the end of the day, Alg. 16 also has to solve a linear system, but it can be expected that the size of these linear systems grows more moderately than in the naive approach sketched at the beginning of the section. On the other hand, Alg. 16 achieves this size reduction via Gröbner basis computations, so it is not clear which of the two approaches is better. It is noteworthy however that the two approaches are not equivalent. For example, if $A(\bar{I})$ happens to be trivial, then $A(I)$ is trivial as well, and therefore detected by the reduction to the bivariate case. The approach based exclusively on linear algebra cannot detect that.

Unlike in the case of principal ideals, it is easy to find examples where $A(I)$ is trivial but $A(\bar{I})$ is not.

Example 22. *Consider the ideal $I \subseteq K[x_1, x_2, y_1, y_2]$ generated by $-x_1 + y_1 + x_1 x_2 y_2 - x_2 y_1 y_2$ and $-x_1 + y_1 + x_1^2 y_1 - x_1 y_1^2$. As its generating set is a Gröbner basis, it is clear that I cannot contain any separated polynomials, because in order to reduce a separated polynomial to zero, the Gröbner basis would need elements with a leading term only involving x_1, x_2 or only involving y_1, y_2. On the other hand, for the ideal $\bar{I} = \langle -sx_1 + ty_1 + s^2 t x_1 x_2 y_2 - st^2 x_2 y_1 y_2, -sx_1 + ty_1 + s^2 t x_1^2 y_1 - st^2 x_1 y_1^2 \rangle \subseteq \mathbb{K}(x_1, x_2, y_1, y_2)[s, t]$ we have $\bar{I} = \langle sx_1 - ty_1 \rangle$ and therefore $A(\bar{I})$ is different from $\mathbb{K}((1, 1))$.*

5 CONCLUSION

We made some progress on the problem of separating variables in multivariate polynomial ideals. While the algorithm for ideals of dimension zero generalizes smoothly from the bivariate case to the multivariate case, we did not find a straightforward generalization of the construction for principal ideals. Instead, we showed that it is possible to reduce the multivariate case to the bivariate case by merging variables. As a result, we obtain that the algebra of separated polynomials is simple for every principal ideal generated by a polynomial involving at least one variable from each of the two groups of variables. It follows furthermore that the algebra is finitely generated for every ideal that is the intersection of a principal ideal and an ideal of dimension zero. For arbitrary ideals, however, the algebra may not be finitely generated. In this case, we can enumerate generators of the algebra, but it remains open whether it is possible to arrange the enumeration in such a way that it terminates whenever the algebra happens to be finitely generated.

REFERENCES

[1] William W. Adams and Philippe Loustaunau. 1994. *An introduction to Gröbner bases*. Vol. 3. American Mathematical Society, Providence.

[2] Erhard Aichinger and Stefan Steinerberger. 2011. A proof of a theorem by Fried and MacRae and applications to the composition of polynomial functions. *Archiv der Mathematik* 97 (2011), 115–124.

[3] David R. Barton and Richard Zippel. 1985. Polynomial decompositon algorithms. *Journal of Symbolic Computation* 1, 2 (1985), 159–168.

[4] Yuri Bilu and Robert Tichy. 2000. The Diophantine equation $f(x) = g(y)$. *Acta Arithmetica* 95, 3 (2000), 261–288.

[5] Yuri F. Bilu. 1999. Quadratic Factors of $f(x) - g(y)$. *Acta Arithmetica* 90, 4 (1999), 341–355.

[6] Yuri F. Bilu and Robert Tichy. 2000. The diophantine equation $f(x) - g(y)$. *Acta Arithmetica* 95, 3 (2000), 261–288.

[7] Franz Binder. 1996. Fast computations in the lattice of polynomial rational function fields. In *Proceedings of ISSAC'96*. ACM, New York, 43–48.

[8] Mireille Bousquet-Melou. 2016. An elementary solution of Gessel's walks in the quadrant. *Advances in Mathematics* 303 (2016), 1171–1189.

[9] Manfred Buchacher, Manuel Kauers, and Gleb Pogudin. 2020. Separating Variables in Bivariate Polynomial Ideals. In *Proceedings of ISSAC'20*. ACM, New York, 54–61.

[10] J.W.S. Cassels. 1969. Factorization of polynomials in several variables. In *Proceedings of the 15th Scandinavian Congress Oslo*. 1–17.

[11] Pierrette Cassou-Nogues and Jean-Marc Couveignes. 1999. Factorisations explicites de $g(y) - h(z)$. *Acta Arithmetica* 87, 4 (1999), 291–317.

[12] H. Davenport, D. J. Lewis, and A. Schinzel. 1961. Equations of the form $f(x) = g(y)$. *The Quarterly Journal of Mathematics* 12, 1 (1961), 304–312.

[13] A. Ehrenfeucht. 1956. Kryterium absolutnej nierozkładalności wielomianów. *Commentationes Mathematicae* 2, 1 (1956), 167–169.

[14] Michael D. Fried. 1973. The field of definition of function fields and the problem in the reducibility of polynomials in two variables. *Illinois Journal of Mathematics* 17, 1 (1973), 128–146.

[15] Michael D. Fried and R. E. MacRae. 1969. On curves with separated variables. *Math. Ann.* 180 (1969), 220–226.

[16] Josef Schicho. 1995. A note on a theorem of Fried and MacRae. *Archiv der Mathematik* 65 (1995), 239–243.